DIREITO DIGITAL NO COMBATE A CRIMES CIBERNÉTICOS

ARTIGO ORIGINAL

OLIVEIRA, Elenilcio Dauto de[1], ALEXANDRE, Weliton do Nascimento[2]

OLIVEIRA, Elenilcio Dauto de. ALEXANDRE, Weliton do Nascimento. **Direito digital no combate a crimes cibernéticos.** Revista Científica Multidisciplinar Núcleo do Conhecimento. Ano 08, Ed. 12, Vol. 03, pp. 64-98. Dezembro de 2023. ISSN: 2448-0959, Link de acesso: https://www.nucleodoconhecimento.com.br/lei/combate-a-crimes-ciberneticos, DOI: 10.32749/nucleodoconhecimento.com.br/lei/combate-a-crimes-ciberneticos

RESUMO

O presente trabalho tem a finalidade de demonstrar por meios de fontes formais e não formais do direito digital, trazendo uma alusão histórica e evolutiva do direito na luta ao combate a crimes cibernéticos. Abordaremos, também, quais os avanços jurídicos em relação aos delinquentes virtuais. A internet é um campo fértil em que golpistas reais e sem precedentes têm angariado seus interesses, assim buscaremos explicar por meio de legislações e entendimentos doutrinários, quais as consequências aos violadores da incolumidade da pessoa humana na esfera cibernética, como o judiciário tem alçado êxito e se comportado desde os surgimentos do direito digital até os dias contemporâneos.

Palavras-chave: Direito digital, Cibercriminalidade, Combate, Legislação.

1. INTRODUÇÃO

É evidente que a evolução tecnológica tem dado azo a mudanças de paradigmas no desenvolvimento social. “A tecnologia move o mundo” assim dizia, Steve Jobs, um dos maiores propulsores do desenvolvimento inovador mundial. Além dos avanços da sociedade, a ascensão da ciência artificial trouxe infortúnios aos controles de limitações no ambiente digital.

Em virtude desse panorama e aproveitando-se das facilidades pela falta limites ao acesso global das redes interconectadas, criminosos espargem suas malhas tracejadas de armadilhas e farsas com o fim de lograr seus intentos maliciosos. Todavia, isto não significa ineficácia da internet ao contexto social, que diante deste processo evolutivo traz inúmeros benefícios ao trabalho, à educação e ao lazer.

Desta forma, entre vantagens e desvantagens surgem barreiras e desafios a serem superados, para isto, emergiu o direito digital com a necessidade/obrigatoriedade de ditar normas e proteger usuários no espaço virtual contra ataques indesejados.

Assim, com o surgimento do direito digital afloram uma nova perspectiva sobre aspectos sociais, democrático, tecnológicos e criminais, e isto não se restringe a esfera computacional, mas a um progresso plenamente interconectados e indispensáveis ao ramo jurídico.

Portanto, o presente artigo abordará uma análise teórica do histórico evolutivo e a aplicação prática do direito ao mundo tecnológico, ainda neste mesmo corolário, discorreremos a sistemática de alguns dispositivos legais no combate aos crimes cibernéticos e suas espécies.

2. CONCEITO DE DIREITO DIGITAL

O direito digital assenta-se sobre o ramo do direito público e privado que estuda a ciência do direito e a ciência computacional. O grupo Iberdrola diz que as novas tecnologias estão inovando o modo que o direito está sendo exercido e desta forma as leis vem se adaptando ao desenvolvimento da nova cidadania digital, permitindo e regulamentando o acesso à informação de forma segura e transparente, dentro de um progresso inovador constante (Grupo Iberdrola, 2022).

O direito digital abrange todos os ramos do direito.

> O Direito Digital consiste na evolução do próprio Direito, abrangendo todos os princípios fundamentais e institutos que

RC: 150720
Disponível em: https://www.nucleodoconhecimento.com.br/lei/combate-a-crimes-ciberneticos

> estão vigentes e são aplicados até hoje, assim como introduzindo novos institutos e elementos para o pensamento jurídico, em todas as suas áreas (Direito Civil, Direito Autoral, Direito Comercial, Direito Contratual, Direito Econômico, Direito Financeiro, Direito Tributário, Direito Penal, Direito Internacional etc.) (Pinheiro,2021, p. 49).

Klaus Schwab um dos maiores expoentes do fator informacional fez menção as tecnológicas como impulsão aos desembaraços globais, por meio da (inteligência artificial, robôs autônomos, *big* data, internet das coisas, *machine learning*, computação em nuvem etc.) são resultantes da transformação digital, também chamada de indústria 4.0 (SCHWAB, 2016).

O filósofo e sociólogo polonês Zygmunt Bauman expressa sobre a volatilidade tecnológica em um conceito fundamental de que nada é constante, tudo se transforma com o tempo, por isso, vivemos em uma modernidade líquida (Bauman, 2001).

Com estas concepções, agregamos que a linearidade do mundo circunscreve no tempo e no espaço com uma velocidade incalculável nos contornos virtuais, e assim, temos que nos adaptar a essas novas configurações.

3. HISTÓRICO DA INTERNET NO MUNDO

É relevante destacar, que a grande transformação tecnológica surgiu no início do século XIX, através da chamada “revolução industrial” que desencadeou uma onda de conquistas rumo a um mundo contemporâneo interconectado. E os primeiros relatos da origem desta evolução foram a fabricação das máquinas a vapor na Grã-Bretanha (Basan, 2021).

Detalhes desta revolução é demonstrada pelo renomado fundador do fórum econômico mundial, doutor Klaus Schwab,

> A primeira revolução industrial ocorreu aproximadamente entre 1760 e 1840. Provocada pela construção das ferrovias

RC: 150720
Disponível em: https://www.nucleodoconhecimento.com.br/lei/combate-a-crimes-ciberneticos

> e pela invenção da máquina a vapor, ela deu início à produção mecânica. A segunda revolução industrial, iniciada no final do século XIX, entrou no século XX e, pelo advento da eletricidade e da linha de montagem, possibilitou a produção em massa (Schwab, 2016, p.18).

A segunda onda evolutiva advém da revolução francesa, em 1789 com surgimento do Estado liberal e não mais submissão ao Estado Absolutista, deste fator emana a sociedade industrial, dando força a novas pesquisas e descobertas (Basan, 2021).

Em momento posterior e diante do absenteísmo do poder absolutista estatal a sociedade avança e as leis tornam-se escritas, suscitando assim, o início do constitucionalismo clássico o qual consagrou os direitos fundamentais como a propriedade, liberdade e privacidade.

Diante desta evolução trabalhadores lutaram por uma participação mais ativa no processo social fundada na ideia de igualdade, assim conquistaram o direito ao voto e as manifestações populares, obrigando o Estado a cumprir prestações sociais e elaborar políticas de defesa e direitos.

Avante na luta pelos direitos e já no período pós-segunda guerra mundial um novo ideal de evolução é agregado ao sistema jurídico, quando República da Alemanha em 1949 criou o instituto “Dignidade da Pessoa Humana”, para tutelar direitos e impor aos legisladores e aos particulares limites normativos (Basan, 2021).

Os relatos primórdios da internet, surgiram nos Estados Unidos, que após anos de pesquisas o Departamento de Defesa Norte-Americano interligou um sistema de rede computador para aperfeiçoamento das táticas militares (Basan, 2021).

Vejamos a abordagem do autor Longhi sobre o tema,

> [...] convenciona-se que as utilizações da Internet ocorreram no âmbito militar. Tal ferramenta fora útil às estratégias de conquista de território e telecomunicações na corrida indireta armamentista e espacial entre os Estados Unidos e a extinta

RC: 150720
Disponível em: https://www.nucleodoconhecimento.com.br/lei/combate-a-crimes-ciberneticos

> União Soviética, durante a Guerra Fria, em meados da década de 1960 (Longhi *et al*., 2020, p.136).

A terceira onda desta revolução só eclodiu na década 1970 com o crescimento da produção industrial e o avanço das tecnologias (Basan, 2021).

> A terceira revolução industrial começou na década de 1960. Ela costuma ser chamada de revolução digital ou do computador, pois foi impulsionada pelo desenvolvimento dos semicondutores, da computação em mainframe (década de 1960), da computação pessoal (década de 1970 e 1980) e da internet (década de 1990), (Schwab, 2016, p.18-19).

Arthur Pinheiro Basan, detalha que: “a virada fundamental, nos anos 70, demonstra o início de uma nova fase na automação da produção industrial: robótica, linhas de produção flexíveis, máquinas industriais com controles digitais etc” (Basan, 2021, p.55).

Ao final da década 1980 essa tecnologia já alcançava as universidades e laboratórios de pesquisas. Em 1993, o sistema informativo já estava bem desenvolvido, podendo ser utilizado por empresas e por particulares por meio de linhas telefônicas (Teixeira, 2022).

Porém, o grande ápice tecnológico foi a criação da rede mundial de computadores, interligando várias máquinas para se comunicarem entre si, sendo, portanto, este sistema introduzido no Brasil somente a partir de 1995 (Teixeira, 2022).

4. EVOLUÇÃO DO DIREITO DIGITAL NO BRASIL

Podemos relatar que dentre o processo de evolução, a internet tem se destacado e com a exposição de tantos recursos tecnológicos decorrente deste evento inovador prosperam também as ações maliciosas na rede digital brasileira, o primeiro delito ao qual se tem relatos foi a inserção de dados falsos, mais conhecido como (peculato informático), sendo este inserido no rol dos crimes digitais pela Lei 9.983/2000 (Saber Direito, 2022).

Diante da preocupação estatal, em 2001, estatuiu-se a Medida Provisória 2.200-2/2001 que instituiu a ICP- Brasil responsável por certificações digitais e infraestrutura de chave pública. Esta medida vincula-se ao seu cerne garantir a assinatura eletrônica por meio de autenticidade, integridade e validade jurídica, originando assim novos métodos de transações eletrônicas (Brasil, 2001).

Em uma análise mais otimizada pode se vislumbrar que esta medida instituiu políticas de segurança ao sistema operacional, ainda favoreceu a cooperação de políticas externas, como por exemplo, negociação e homologação de tratados e acordos bilaterais.

Pinheiro (2021, p.156) afirma que

> A assinatura eletrônica é, portanto, uma chave privada, ou seja, um código pessoal e irreproduzível que evita os riscos de fraude e falsificação. Para o Direito Digital, uma chave criptográfica significa que o conteúdo transmitido só pode ser lido pelo receptor que possua a mesma chave e é reconhecida com a mesma validade da assinatura tradicional.

Em 2006, emana a Lei 11.419/06 alterando a dinâmica processual, ocorrendo a transladação meios físicos para os meios eletrônicos, e criando assinaturas digitais por meio de certificados (token) facilitando a tramitação dos arquivos (Brasil, 2006).

> Esse tema da informatização do processo judicial (ou processo eletrônico) tem como consequência a modernização do Poder Judiciário. Embora o processo sem papel tenha surgido antes do advento da lei em questão, isso passou a ser tratado de forma mais enfática a partir da vigência da Lei n. 11.419/2006 (Teixeira, 2022, p. 492).

Outro marco histórico e revolucionário do direito digital ocorreu em 2008, quando foi sancionada a primeira legislação sobre combate a pornografia infantil na internet. A lei 11.829/2008 trouxe em seu teor o objetivo de coibir práticas de atos que atentem contra a dignidade sexual das crianças e dos adolescentes (Brasil, 2008).

Em 2012, com a edição a lei 12.737/2012 trouxe gradação de pena para exploradores de vulnerabilidades alheia por meios de dispositivos informáticos, conhecida como Lei dos Crimes Cibernéticos ou Carolina Dieckmann (Brasil, 2012).

Com a ascensão da informatização, os mercados e-commerce passaram a ter dificuldades em atender demandas pelo grande volume de vendas dos produtos, deixando os consumidores inconformados pela demora na entrega dos itens adquiridos pela internet. De modo a amparar o consumidor inclui-se nas normas nacionais o decreto 7.962 de 2013, o qual traz regras sobre o compras e vendas no comércio eletrônico (Brasil, 2013).

Para agregar mais respaldo e corrobora com a sistemática informativa a lei 12.965/14, conceituada com Marco Civil da Internet, exalou princípios, garantias e direitos assegurando a necessidade de estabelecer diretrizes para resguardar a liberdade de expressão, à privacidade, à proteção de dados pessoais e ao direito de acesso no domínio digital (Brasil,2014).

Barreto e Brasil (2016) aduzem que, o projeto Macro Civil da Internet traz uma visão não incriminadora, mas sim garantidora de direitos com ênfase nas liberdades no espaço virtual.

Em 2015 o Código de Processo Civil (CPC) ampliou a confluência probatória possibilitando a formulação de diligências digitais, com isso reforçou outros dispositivos normativos como a Lei de Acesso à Informação (LAI) e a Lei Geral de Proteção de Dados (LGPD) na busca por indícios factível atreláveis ao processo (Brasil, 2015a).

Dentre várias provas que podem ser confrontadas na seara digital podemos destacar as informações produzidas em sistema de dados das empresas, como os dados de redes sociais, ferramentas de geoprocessamento e biometria. Desta forma subentende-se que o valor probante por meios informáticos é uma derivação de vários dispositivos legais, e depende de conversão à forma impressa, as quais

pode ser anexada com outros meios de provas para solucionar um litígio (Lopes *et al.,* 2021).

Ainda em 2015 criou-se a lei 13.185/15, que combate a intimidação e ameaças, *cyberbullying* (assédio moral na internet), visando reprimir as agressões repetitivas sejam psicológicas, sejam físicas, que causar humilhação ou difamação sem motivos (Brasil, 2015b).

Dentre as nuances de mudanças e evoluções, 2017 foi o ano da famigerada reforma trabalhista trazida pela lei 13.647/17 a qual elenca em suas disposições a possibilidade de empresas contratarem funcionários na modalidade de teletrabalho e home office, facilitando a acessibilidade das pessoas ao mercado de trabalho pelos mecanismos digitais.

Na definição de Tarcisio Teixeira

> Teletrabalho é uma modalidade de trabalho realizada a distância (ou home office), ou seja, fora das dependências (estabelecimento ou residência) do empregador, em que se utilizam ferramentas da Tecnologia da Informação (meios telemáticos e informatizados), principalmente com canais de comunicação on-line via internet para se comunicar com a empresa e/ou colegas de trabalho, clientes, fornecedores etc. (Teixeira, 2020, p. 199).

Outra lei que veio com muita força de reestruturação do contexto normativo foi a Lei Geral de Proteção de Dados (LGPD), regendo os direitos no ciberespaço e trazendo como fonte primordial o tratamento de dados pessoais.

Expressam os autores Fernandes e Carvalho (2018), que a Lei Geral de Proteção de Dados assegura salvaguardar direitos relativos à pessoa titular dos dados preservados, disciplina também, os modos de operações a serem seguidos pelos agentes de tratamento e a obrigatoriedade de reparação dos danos causados por irregularidade ou pela não observância aos preceitos da LGPD.

Outro ponto de destaque ao mundo digital foi dado pela introdução da lei 13.718 /2018, que alterou o Código Penal inserindo o artigo 218-C, tipificando-o em um rol de ações que incidem em crime contra as vulnerabilidades de infantis e adolescentes na internet. Este mesmo dispositivo prevê pena de reclusão aos propagadores de conteúdos proibidos e explícitos com menores, além disso, esta mesma lei prevê agravantes no caso de Pornografia de Vingança, que nos conceitos doutrinários vem da denominação inglesa (*revenge porn*), que é uma forma de *cybervingança* ou vingança digital, muito frequente nas redes sociais em situação de pós relacionamentos afetivos (Teixeira, 2022).

5. CRIMES CIBERNÉTICOS

Não é recente as práticas de violências provenientes da tecnologia, a ilustre filósofa escritora - Hannah Arendt - a qual vivenciou muitos tipos de violências no período do holocausto, já demonstrava sua preocupação com aumento das mudanças tecnológicas desde a década de 1960, isto fica evidente quando em sua façanha literária “Sobre a Violência” ela discorre sobre hostilidades, guerras e progresso tecnológicos.

Entre suas reflexões Hannah fez apontamentos sobre a tecnologia: “A violência multiplica, com os instrumentos que a tecnologia fornece de maneira cada vez mais exponencial, o vigor individual” (Arendt, 1994, p.9).

Após estes apontamentos, iremos aprofundar ao estudo do crime cibernético em si, os quais trazem em sua essência os mesmos fatos típicos que os crimes comuns, no entanto, são praticados contra ou com a utilização dos sistemas eletrônicos.

Vejamos o que diz a (OECD), *Organization for Economic Cooperation and Development:* Este organismo de cooperação e desenvolvimento define que, crime de informática são atos de vontade típicos e antiéticos, podendo seus efeitos ser

gerados por manipulação, falsificação, sabotagem e outras formas de acesso não autorizado na rede universal de comunicação (Aras, 2015).

O crescente número de delitos cibernéticos é alarmante e de acordo com, Patricia Peck Pinheiro, uma pesquisa de estatística feita pela Polícia Federal dos Estados Unidos (FBI), concluíram que os crimes cibernéticos chegaram a US$ 3,5 bilhões de prejuízos em 2019 (Pinheiro, 2021).

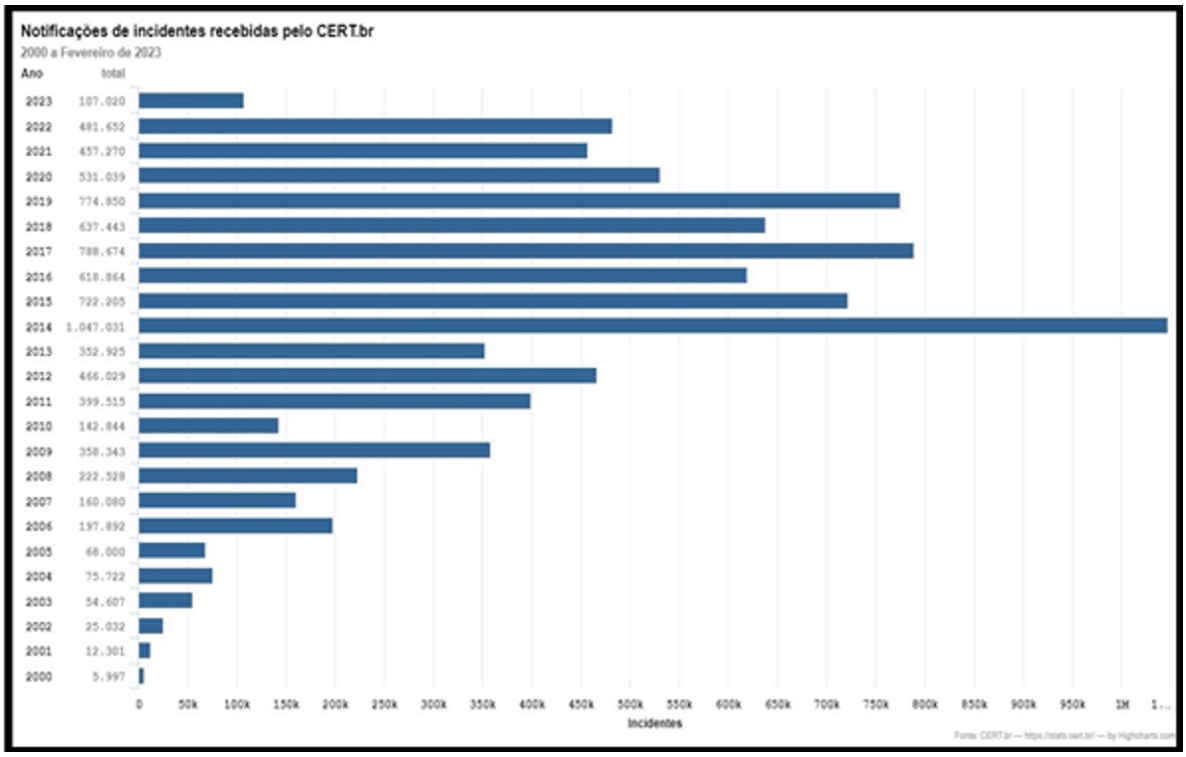
No Brasil, temos mais 152 milhões de usuários de internet, isso corresponde a 81% da população, e com este vasto campo de acesso por usuários conectados isto proporciona facilidades aos criminosos para agirem diuturnamente, desenvolvendo programas de sites falsos, links de sorteios, mensagens com vírus, estelionato virtual, *fake News* e outras formas de ataques (Silva, 2022).

> Segundo pesquisas atuais, crescem os crimes virtuais, e estes, em breve, irão ultrapassar os crimes físicos. Sendo assim, podemos vislumbrar a importância que a computação forense terá para a sociedade, pois é por meio dessa ciência que será possível descortinar os fatos e punir os infratores (Pinheiro, 2016, p. 278).

Para melhor compreensão observe no Gráfico 1. a ascensão dos ataques de *cybercrimes,* comprovada pelo Centro de Estudos Resposta e Tratamento de Incidentes de Segurança no Brasil (Cert.Br, 2023).

RC: 150720
Disponível em: https://www.nucleodoconhecimento.com.br/lei/combate-a-crimes-ciberneticos

Gráfico 1 - Total de Incidentes Reportados ao CERT.BR por Ano



Fonte: Cert.Br. (2023).

Baptista Junior e Dian analisam o gráfico até o ano de (2020) e destacam que: é evidente o crescimento dos incidentes com segurança da informação, que segundo Cert.br a amostragem são indicativos da majoração de mais de 33600% nos índices de ataques reportados (Baptista Junior e Dian, 2021).

6. CRIMES VIRTUAIS QUE AFETAM SENTIMENTOS ALHEIO

Estas modalidades afetam não só os contornos físicos, mas também psicológicos das vítimas, e ainda podem ter caráter pejorativo em relação ao fator pecuniário e neste mesmo teor podemos afirmar que são crimes que atacam as liberdades fundamentais por violar o vigor privado.

6.1 ESTELIONATO SENTIMENTAL/ EMOCIONAL

O termo, Estelionato Sentimental, surgiu em um processo que aconteceu em Brasília no ano de 2015. O juiz da 7ª Vara Cível de Brasília condenou o réu a ressarcir todos os prejuízos causados a sua ex-namorada, pelos danos materiais.

Sustentou o magistrado que,

> Embora a aceitação de ajuda financeira no curso do relacionamento amoroso não possa ser considerada como conduta ilícita, certo é que o abuso desse direito, mediante o desrespeito dos deveres que decorrem da boa-fé objetiva (dentre os quais a lealdade, decorrente da criação por parte do réu da legítima expectativa de que compensaria a autora dos valores por ela despendidos, quando da sua estabilização financeira), traduz-se em ilicitude, emergindo daí o dever de indenizar"(Processo n. 0012574- 32.2013.8.07.0001) (Santos, 2015, [n.p.]).

Ex positis, o juiz condenou o réu ao pagamento de cento e um mil e quinhentos reais a sua ex-namorada como forma de ressarcimento a diversas contas que ela teria pagado durante o relacionamento de dois anos, incluindo roupas, sapatos e pagamentos de contas telefônicas etc. Nesta vertente criminosa a lesão ocorre não somente aos bens jurídicos materiais, mas também psicológicos.

O crime de estelionato emocional na modalidade eletrônica está previsto na legislação penal como uma qualificadora, agravante do induzimento a erro mediante fraude.

Vejam o que diz a Legislação Penal,

> Art. 171 § 2º-A. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos e multa, se a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo (Brasil, 1940).

É uma modalidade de *cyberdelito* em que utilizam a internet como ferramenta para sua concretização, o agente manipula, induz, engana a vítima que voluntariamente acredita no artifício errôneo (Bezerra *et al*., 2020).

6.2 *STALKING / CYBERSTALKING*

Stalking (perseguição) é uma das mais novas caracterização criminosa inserida na lei brasileira, sua maior incidência ocorre no mundo virtual, este crime pode acontecer por ressentimento, rejeição ou por latentes predadores, podendo estes serem pessoas conhecidas da vítima ou não.

O autor Cleyton da Silva Bezerra define *stalking,*

> O "*STALKING*" deriva do termo "*stalk*", que numa tradução livre seria algo como "perseguição furtiva", embora seja traduzido em adaptação livre para "ato de perseguir alguém, de forma continuada e reiterada, ameaçando sua integridade e psicológica, com restrição à liberdade de locomoção ou invasão à liberdade ou privacidade de outra pessoa (Bezerra *et al.,* 2020, p. 87).

Por conseguinte, as consequências para as vítimas destas delinquências são, medo de sair de casa, bloqueio das contas, mudanças de rotinas etc.

À vista disso, por ser um crime eminentemente virtual, o direito digital buscou criminalizar as condutas de perseguição e opressões reiteradas a alguém e fez isso através de lei incriminadora 14.132/2021 inserido ao CP o Art. 147-A, aduzindo que a perseguição se configura por qualquer meio, inclusive digital, quando o autor compromete as liberdades e ainda ameaça à integridade física ou psicológica de outra pessoa. A pena para quem for condenado por *stalking* vai de 6 (seis) meses a 2 (dois) anos de prisão e multa (Brasil, 2021).

Julgado de um caso prático em que um homem é condenado por crime de *stalking* (perseguição) a uma Juíza da vara do trabalho: O caso ocorreu em Osasco na cidade de São Paulo, onde o reclamante inconformado com a decisão judicial

RC: 150720
Disponível em: https://www.nucleodoconhecimento.com.br/lei/combate-a-crimes-ciberneticos

desfavorável iniciou uma perseguição virtual contra à juíza prolatora da sentença, dando ensejo neste caso ao crime de *stalking*.

No evento em tese, o coator foi processado, julgado e condenado, o excelso julgador entendeu que o opressor estava ameaçando a integridade da magistrada, e fundamentou que, embora a inafastabilidade de jurisdição seja imprescindível ao exercício jurisdicional, o excesso deste configura abuso de direitos, além do mais, para reiterar a decisão sustentou que crime de perseguição foi inserido no Código Penal pela Lei nº 14.132/2021 (artigo 147-A) e exige que essa coação seja reiterada e por qualquer meio. Assim, tem-se que o fato delitivo pode ser praticado por intermédio de meios digitais, o que se costuma denominar '*cyberstalking'*, disse o magistrado (Kopp, 2022).

6.3 *CATFISHING* / FALSA IDENTIDADE

Conhecido como crime de "Falsa Identidade", o qual tem como objetivo enganar e seduzir pessoas que buscam por um relacionamento em sites ou em redes sociais. Assim destacam Castro e Zaganelli (2020, p. 314) sobre *Catfishing*: […] O ato de criação de um perfil falso na internet, seja utilizando informações de outras pessoas ou dados inteiramente inventados, corresponde a criar uma falsa identidade.

Esta modalidade de crime tem previsão legal no Art. 307 do Código Penal, diz que, quem atribui perfil falso para auferir vantagens em proveito alheio pode ser condenado em até um ano de prisão, se não constituir crime mais grave (Castro; Zaganelli, 2020).

7. CRIMES DIGITAIS QUE ATENTAM CONTRA A HONRA E O ESTADO DEMOCRÁTICO

7.1 LIBERDADE DA EXPRESSÃO E DISCURSO DE ÓDIO NAS REDES SOCIAIS

A liberdade de expressão é assegurada por regras de diretos internacionais que destina a garantir ao estado democrático a livre expressão intelectual, artística, científica e a comunicação.

Embora previsto no texto constitucional, essas liberdades não são genéricas, além da vedação ao anonimato, incorre em crime quem profere palavras de ódio ou de ofensas em redes sociais.

Sobre o discurso de ódio diz o autor Estevam que,

> O discurso do ódio consiste na divulgação de mensagens que difundem e estimulam o ódio racial, a xenofobia, a homofobia e outras formas de ódio baseadas na intolerância e que confrontam os limites éticos de convivência com o objetivo de justificar a privação de direitos (Estevam *et al.,* 2019 [n.p.]).

Além disso, a Constituição Federal em seu Art.5º XLI repudia atos atentatórios contra direitos e liberdade fundamentais (Brasil, 1988),

> É cediço que a prática do discurso de ódio não está limitada a tecnologias da informação. A manifestação do preconceito pode também ser exteriorizada através de jornais, livros e revistas impressos, além de, por óbvio, da forma mais tradicional de linguagem: a fala. Todavia, o uso da internet para disseminar o ódio social de alguns contra determinados grupos, em sua maioria vulneráveis, parece favorecer a perpetuação do preconceito e intolerância, em especial de negros, homossexuais e mulheres, uma vez que possibilita que a mensagem odiosa chegue, rapidamente, a milhões de pessoas, trazendo consequências tão ou mais gravosas do que a discriminação praticada no mundo “real” (Jesus; Milagre, 2016, p.43, *apud* Escobar 2019).

Desta forma, os aprazados dispositivos confeccionam que liberdade de expressão, embora decorra do exercício de cidadania, palavras não podem ser verbalizadas indiscriminadamente nas mídias sociais, há, portanto, margens para sua a utilização, como por exemplo, vedação ao anonimato, proibições a discussões odiosas, pejorativas ou criminosas, sendo consequentemente, passíveis de responsabilização civis e penais os autores de tais atos (Pinheiro, 2021).

7.2 MISOGINIA VIRTUAL

Misoginia são fatores perduram no tempo desde a antiguidade clássica em que o patriarcalismo tratava as mulheres como objetos desprovidos de qualquer autonomia, são estigmas, aversões que homens tinham em relação ao sexo feminino, em razão das condições sociais, domésticas, raça, política, trabalho etc.

No entanto, na idade contemporânea essa realidade é outra, mas ainda há resquícios destes preconceitos em nossa sociedade, principalmente nas redes sociais, os quais devem ser punidos severamente na forma da lei (Austen, 2012).

No Brasil esta modalidade transgressão é configurada pela lei 13.642/2018, chamada de Lei Lola, que alterou o artigo 1º da lei 10.446/2002, atribuindo a Polícia Federal competência para investigar atos infringentes a dignidade da mulher (Brasil, 2018a).

Assim declara o Art. 1º, VII. da lei 10.446/2002 alterada pela Lei Lola

> quando houver repercussão interestadual ou internacional que exija repressão uniforme, poderá o Departamento de Polícia Federal do Ministério da Justiça, sem prejuízo da responsabilidade dos órgãos de segurança pública arrolados no art. 144 da Constituição Federal, em especial das Polícias Militares e Civis dos Estados, proceder à investigação, dentre outras, das seguintes infrações penais:
>
> quaisquer crimes praticados por meio da rede mundial de computadores que difundam conteúdo misógino, definidos

> como aqueles que propagam o ódio ou a aversão às mulheres (Brasil, 2002).

Isto posto, entende-se que a misoginia pode ultrapassar fronteiras globais que além de ferir a honra da mulher, pode atingir outras esferas da dignidade da pessoa humana, como a raça, a cor e até mesmo a coexistência social (Bailey, 2022).

7.3 PROPAGAÇÃO DE *FAKE NEWS*

Nos últimos anos a disseminação de *Fake News* (Notícias Falsas) não são novidades no mundo digital, com a constante popularização das redes sociais e os avanços digitais tem facilitado a propalação de notícias fictícias, podendo, entretanto, nos casos de desrespeitos aos princípios éticos e morais da ordem democrática caracterizar ofensa à liberdade de comunicação e expressão.

Estevam (2019), diz que *fake News* são inverdades fundadas sem base concreta a qual induz pessoas a erros ou distorções de entendimentos e pensamentos reais dos fatos, seja visando lucros ou não.

Faustino (2019) relata que não basta termos acesso à liberdade de informações, mas estas devem ser verdadeiras e ainda afirma que a garantia à informação decorre do direito de expressão.

Embora não haja tipificação direta de lei ao crime de *Fake News*, no congresso está em trâmite projetos tendentes a combater desinformações nas redes sociais, como é o caso do projeto de lei 2630/2020, o qual não tem como finalidade reprimir a liberdade de expressão, mas regulamentar o funcionamento e a transparência de acesso a informações nas redes sociais.

Diante da exorbitante quantidade de notícias falsas espalhadas sobretudo em época de eleições, o Código Eleitoral nos termos do Art. 323 fixou pena de detenção de dois meses a um ano e multa, para quem difunde dados falsos no período eleitoral (Brasil,1965).

A tipificação de *Fake News* também pode ser vista por interpretação analógica aos crimes contra a honra da lei penal.

Dispõe a lei 2848/1940 (código penal)

> Art. 138 -Caluniar alguém, imputando-lhe falsamente fato definido como crime: Pena - detenção, de seis meses a dois anos, e multa.
>
> Art. 139 - Difamar alguém, imputando-lhe fato ofensivo à sua reputação: Pena - detenção, de três meses a um ano, e multa
>
> Art. 140 - Injuriar alguém, ofendendo- lhe a dignidade ou o decoro: Pena - detenção, de um a seis meses, ou multa (Brasil, 1940).

As consequências por espalhamento de *fake* também conhecido como *hoax* (boatos) na internet na visão dos organizadores Cleyton e Giovani em sua obra "Combate às *Fakes News*" revelam que: Os efeitos das *fake News* são desastrosos, tanto para o profanador quanto para o receptor dos insultos, de tal forma que essas notícias podem destruir a vida de uma pessoa ou levar ao caos social (Bezerra, *et al*., 2019).

Para ilustrarmos bem essas consequências, relembraremos o escândalo das eleições estadunidenses em 2016, no manifesto em questão a empresa norte americana "*Cambridge Analytica*" foi acusada desviar dados pessoais de usuários do *Facebook* e do *Twitter* para favorecer o concorrente presidencial, Donald Trump, nas decisões das eleições americanas.

As denúncias feita pelo jornal, *The New York Times*, colocou a prova a legalidade da decisão eleitoral, que foram duramente criticadas, aumentando assim, as preocupações externas em estabelecer novas políticas coercitivas para as empresas operadoras e controladoras de dados pessoais, no Brasil essa preocupação se materializou com a edição da Lei Geral de Proteção de Dados, com o desígnio resguardar a personalidade individual (BBC News, 2018).

8. CRIMES CONTRA A DIGNIDADE SEXUAL NO CIBERESPAÇO

São delitos que causam muita repulsa social, pois, dada a hostilidade e o potencial lesivo desta modalidade criminosa que muitas vezes são irreversíveis para as vítimas, houve assim uma preocupação maior do estado em tutelar a dignidade sexual na escala cibernética, e fez isto através de vários dispositivos incriminador os quais serão analisados posteriormente.

8.1 PORNOGRAFIA INFANTIL

Por tamanha hediondez, sem dúvidas, a pornografia infantil é, de longe, o delito de maior repercussão e o mais repulsivo para a sociedade em geral. Por isso, sua tipificação decorre de vários preceitos normativos, Lei penal (2848/1940); lei de combate aos crimes de pornografia infantil na internet (11.829/2008); Estatuto da criança e do adolescente (lei 8.069/1990) e inserção da pornografia infantil no rol dos delitos hediondos pela lei 7.220/2014.

Crime de produção de pornografia infantil caracteriza-se

> [...] qualquer forma de pornografia envolvendo criança ou adolescente (artigo 240 do Estatuto da Criança e do Adolescente — pena de quatro a oito anos). Também pratica esse crime quem agencia de qualquer forma ou participa das cenas de pornografia infantil (artigo 240, §1º, do Estatuto da Criança e do Adolescente). A pena para esse delito é aumentada em 1/3 (um terço) em diversos casos em que o crime é mais grave (artigo 240, §2º, do Estatuto da Criança e do Adolescente), (Botelho *et al*., 2013, p.202).

A lei penal também estabelece sua rigidez, em relação ao crime contra a dignidade sexual infantil na internet

> Art. 218-C do Código Penal: oferecer, trocar, disponibilizar, transmitir, vender ou expor à venda, distribuir, publicar ou divulgar, por qualquer meio - inclusive por meio de comunicação de massa ou sistema de informática ou telemática, fotografia, vídeo ou outro registo audiovisual que

> contenha cenas de estupro ou de estupro de vulnerável ou que faça apologia ou induza a sua prática, ou, sem o consentimento da vítima, cena de sexo, nudez ou pornografia:
>
> Pena - reclusão, de 1 (um) a 5 (cinco) anos, se o fato não constitui crime mais grave (Brasil,1940).

Embora a Polícia Federal no âmbito de suas competências e cooperação internacional tem mostrado um excelente trabalho no combate a violências. Não obstante, em se tratando de pornografia infantil na internet há muito a ser feito, e por isso o poder legiferante ao editar normas de direito digital tem demostrado suas preocupações em relação à criança e ao adolescente, isso fica indubitável com a publicação das leis que incriminam ações que atacam a dignidade sexual das crianças e adolescentes inclusive em meios digitas (Bezerra, *et al*., 2020).

8.2 PORNOGRAFIA DE VINGANÇA/ *REVENGE PORN*

Pornografia de vingança são crimes praticados por motivos diversos, mas o motivo preponderante é o inconformismo pelo término do relacionamento, assim começam expor na internet a intimidade do ex-cônjuge como forma de vingança (Cassanti, 2014).

O legislador constitucional ao formular as diretrizes de direitos fundamentais zelou pela tutela da intimidade, assegurando indenizações decorrente de sua violabilidade, podendo o cônjuge ou companheiro lesado invocar a tutela do estado em detrimento de sua dignidade íntima (Brasil,1988).

> Usualmente essa violência é cometida por um ex-companheiro ou alguém do círculo social da mulher. Consiste na divulgação de conteúdo íntimo da mulher, podendo ser vídeos ou fotos, que contenham nudez ou relações sexuais, sem o consentimento da mesma com objetivo de se vingar, normalmente após o término do relacionamento amoroso (Faraj, 2021, p.20).

Revenge Porn, é o termo inglês para pornografia de vingança, são atos que extrapolam os contornos da vida intima, são publicações por sentimentos vingativos e retaliações

> dados da organização *Safernet* indicam um preocupante aumento de casos registrados. Em 2014, 1.225 pedidos de orientação psicológica chegaram à entidade. Destes, 224 eram relacionados à questão de vazamento de fotos íntimas (18%) – um aumento de 119,8% em relação a 2013. 81% dos pedidos por orientação foram feitos por mulheres. O número ainda se concentra em mulheres com até 25 anos (53%), sendo que um em cada quatro casos envolveu adolescentes (Lana, 2019, p.12).

No Brasil o combate a pornografia de vingança se concretiza pela lei 13.718/2018 a qual inseriu ao CP o artigo 218 - C, sendo que a disponibilização, divulgação, exposição, em quaisquer meios de comunicação incide em pena de reclusão, de 1(um) a 5 (cinco) anos, além das majorantes se constituírem crimes mais grave (Brasil, 2018b).

8.3 PEDOFILIA VIRTUAL

A “Lei Maior” tutela a crianças e adolescentes, garantindo sua proteção e os cuidados necessários ao seu desenvolvimento, estas garantias são de competência, tanto da família, quanto da sociedade e também do governo.

Para externalizar esta preocupação, Constituição Federal de 1988 trouxe de forma expressa quais são os responsáveis garantir esta proteção

> Art. 227 - É dever da família, da sociedade e do Estado assegurar à criança e ao adolescente, com absoluta prioridade, o direito à vida, à saúde, à alimentação, à educação, ao lazer, à profissionalização, à cultura, à dignidade, ao respeito, à liberdade e à convivência familiar e comunitária, além de colocá-los a salvo de toda forma de negligência, discriminação, exploração, violência, crueldade e opressão.

RC: 150720
Disponível em: https://www.nucleodoconhecimento.com.br/lei/combate-a-crimes-ciberneticos

> § 4.º A lei punirá severamente o abuso, a violência e a exploração sexual da criança e do adolescente (Brasil, 1988).

Para concretizar a ideia expressa na CF outras leis ampliaram a proteção aos incapazes, sendo elas: Estatuto da Criança e do Adolescente - Lei 8.069/1990, com alterações pela Lei 11.829/2008,

> Art. 5º Nenhuma criança ou adolescente será objeto de qualquer forma de negligência, discriminação, exploração, violência, crueldade e opressão, punido na forma da lei qualquer atentado, por ação ou omissão, aos seus direitos fundamentais (BRASIL, 1990).
>
> [...]
>
> Art. 240. Produzir, reproduzir, dirigir, fotografar, filmar ou registrar, por qualquer meio, cena de sexo explícito ou pornográfica, envolvendo criança ou adolescente: Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa.
>
> Art. 241-E. Para efeito dos crimes previstos nesta Lei, a expressão "cena de sexo explícito ou pornográfica" compreende qualquer situação que envolva criança ou adolescente em atividades sexuais explícitas, reais ou simuladas, ou exibição dos órgãos genitais de uma criança ou adolescente para fins primordialmente sexuais (Brasil, 2008).

Com a facilidade de entretenimento e comodidade sugestionáveis na internet estimulam os predadores que aproveitam de oportunidade e falhas para satisfazer seus desejos ou aferir lucros no espaço virtual. Segundo especialistas, a Pornografia Infantil na Internet é a segunda forma de crime organizado mais lucrativa, perdendo apenas para o narcotráfico, crianças são feitas de objetos lucrativos por essas redes de pedofilia (Breier, 2014, *apud* Pereira; Teza, 2015).

Para ilustrarmos um alerta sobre pedofilia virtual podemos citar o caso apresentado recentemente na novela "Travessia" exibida pela emissora, Rede Globo de Televisão, no episódio em questão um *deepfeke* (tecnologia que muda o rosto e voz em vídeo chamada) apresenta-se a uma jovem a qual faz amizades íntimas, no entanto, mal sabia ela que estava se expondo a um predador pedófilo camuflado

por um software que muda a face. Embora a dramatização pareça apenas uma cena comum de novela, isto já é realidade no mundo real (Souza e Helder, 2023).

9. TIPOS DE ATAQUES CIBERCRIMINOSOS

Os crimes eletrônicos podem ser praticados por qualquer pessoa física ou jurídica, todavia, os criminosos mais conhecidos são os hackers e os *crackers*, pois estes são especialistas com amplo conhecimento digital.

Newton De Lucca estabelece a distinção entre *hackers* e *crakers*

> As palavras, na verdade, não são sinônimas. Os hackers são especialistas em informática, capazes de invadir computadores alheios, mas, também, de impedir invasões dos outros. Não existe, necessariamente, uma conotação pejorativa para os hackers que podem prestar serviço de extrema valia. Já os crackers, ao revés, atuam de forma claramente dolosa, isto é, com a intenção de prejudicar alguém ou de tirar proveito ou partido para si da informação obtida". Títulos e contratos eletrônicos – o advento da informática e seu impacto no mundo jurídico (De Lucca *et al*., 2005, p. 71).

9.1 *HACKERS*

Hackeadores são especialistas que utilizam métodos avançados, (*phishing*, spam, *ransomware, spyware, trojan*), de invasão aos sistemas telemáticos alheios.

Modalidades de *hackers*, segundo Pinheiro (2021)

Hackers Mercenários: são profissionais espião que acessam a rede mundial de computadores de forma remota para obterem acessos a dados de corporações e do governo. Lembrando também que estes profissionais podem ser de utilidade licita ao fortalecimento de segurança de grandes empresas.

RC: 150720
Disponível em: https://www.nucleodoconhecimento.com.br/lei/combate-a-crimes-ciberneticos

Hackers Heróis: são grupos que disseminam crimes coletivos em busca de status, e utilizam-se das redes sociais para publicarem seus feitos vandálicos, como exemplo os pichadores de muros.

Pesquisa da empresa *Attrition* revela que,

> O Brasil é o país que está em primeiro lugar quanto aos ataques de delinquentes virtuais realizados no mundo com 3,56%, à frente dos Estados Unidos com 2,65%. Essa organização diz que uma possível explicação para isso é o fato de que os hackers americanos possuem maior prática, não deixando pistas e impedindo o rastreamento do crime, diminuindo o registro de ataques (Teixeira, 2022, p. 66).

A ação desses invasores é considerada crime de acordo com o Código Penal, as mudanças legislativas pela Lei n. 12.737/2012 introduziu o Art. 154-A ao CP. Pois, Trata-se de invasores que exploram vulnerabilidades alheias a dispositivos informáticos, com finalidade de obter vantagens ilícitas. No entanto os hackers nem sempre atuam em atividade dolosa, podem ser usados para atividades lícitas (Teixeira, 2022).

9.2 *CRACKERS*

A magnitude tecnológica abre alas aos verdadeiros criminosos da rede mundial, os crackers tem um conhecimento muito mais amplo em tecnologia, por isso, não é mais novidade nem tampouco recentes matérias concernentes a invasões de crackers a grandes empresas nacionais e internacionais até mesmo a site do governo (Jesus; Milagre, 2016).

Estes espiões com elevado conhecimento tecnológico atuam exclusivamente de forma dolosa em detrimento de proveito alheio.

> Em 2013, o país perderia U$$ 8 bilhões com ataques de crackers, roubos de senhas, clonagens de cartões, pirataria virtual, além de espionagem governamental e industrial, entre outros crimes cibernéticos. Crimes de informática custaram

> U$$ 500 bilhões para a economia mundial em 2013 (Jesus; Milagre, 2016, [n.p.]).

Crackers são especialistas que têm alvos específicos, sendo estes na maioria das vezes empresas que operam online e bancos, entre as vítimas brasileiras destes ataques quem ostenta os maiores ranking são empresas.

> Segundo a pesquisa da empresa ISS – *Internet Security Systems* (Sistemas de Segurança de Internet) realizada com 100 empresas brasileiras, entre elas 30 bancos, apenas 2,75% possuíam software para detectar invasores on-line. “O risco é eminente, o sistema é altamente vulnerável. Hoje, na internet, existem programas para invadir todos os tipos de sistema”, diz Leonardo Scudere, presidente da ISS no Mercosul (Teixeira, 2022, p. 66).

Assim podemos afirmar que estes, digamos expert da tecnologia, são dotados de auto saber informacional, no entanto utilizam a internet a contrário sensu do ideal comum, ferindo assim as normas e causando altos prejuízos alheios.

10. MÉTODOS DE INVASÃO A DISPOSITIVOS ELETRÔNICOS

São ferramentas de software que os agentes maliciosos utilizam com o escopo de executarem suas ações, dentre várias atividades ardilosas as que mais se destacam são as de *phishing* e *spywares.*

10.1 *PHISHING*

Phishing (pescaria), é uma das técnicas de invasão a dispositivos informáticos muito utilizado na engenharia social, vários métodos são utilizados, como por exemplo, envios de e-mail fraudulentos na tentativa de capturar dados pessoais, senhas de cartões de créditos e outros dados.

A autora Patricia Peck expõe exemplos que criminosos adotam para executar a técnica de *phishing*,

RC: 150720
Disponível em: https://www.nucleodoconhecimento.com.br/lei/combate-a-crimes-ciberneticos

> Normalmente a fraude por *Phishing Scan* ocorre da seguinte forma: (1) um código malicioso é enviado por e-mail para as vítimas, (2) as quais, não analisando a veracidade do conteúdo nem o remetente da mensagem, acessam a informação, executam o arquivo e, consequentemente, (3) o computador do usuário é infectado, (4) comprometendo suas informações confidenciais, tais como senhas, dados pessoais etc., (5) essas informações são transmitidas para o fraudador, (6) que as utiliza para acessar, por exemplo, (7) o Internet *Banking* da vítima e desviar dinheiro para outra conta (Pinheiro, 2021, p. 138).

Os invasores dissimulam a ilegitimidade dos arquivos enviados às vítimas, passando-se por grandes empresas de modo a atrair curiosos, que por sua vez, são instigados tanto pela qualidade dos produtos, quanto pelas ofertas de grandes lucros, assim, clicam em links, preenche formulários ou baixam aplicativos, por conseguinte, os cibercriminosos iniciam suas operações nas tentativas de coletarem as informações pessoais para cometerem suas delinquências (Cassanti, 2014).

> [...] O Brasil destaca-se como quarto principal alvo dos crackers em ataques de phishing (pescaria de senhas) no mundo, figurando entre os cinco países que mais tiveram empresas hackeadas. Algo em torno de 38 milhões de usuários lesados (Jesus; Milagre, 2016, [n.p.]).

Desta forma, com o aumento desta modalidade de delitos de invasão informática, surge a necessidade de criminalizar os exploradores dessas fragilidades alheias. Embora sua incidência maior seja na seara digital, a criminalização do *phishing* emerge no 155, § 4º, inciso II, do Código Penal Brasileiro, que se trata de invasão a dispositivos informáticos, cuja pena podendo chegar a quatro anos, além de multa.

10.2 *SPYWARES*

Spywares (espião) são softwares maliciosos em forma de aplicativos que altera a funcionamento do computador para explorar arquivos e capturas senhas, entretanto os ataques não se restringem a isso, podendo chegar a casos extremos como

RC: 150720
Disponível em: https://www.nucleodoconhecimento.com.br/lei/combate-a-crimes-ciberneticos

espionagens através da câmera do aparelho celular ou computadores (Cassanti, 2014).

Damásio de Jesus define claramente a intenção dos *spywares*,

> Código ou programa malicioso instalado ou injetado normalmente em aplicativos baixados de fontes duvidosas, que tem a função de coletar informações do usuário de um computador e enviá-las ao destinatário. Informações comumente coletadas são hábitos de consumo, informações de navegação, dentre outros. Alguns permitem o controle da máquina pelo atacante. Também podem estar inseridos dentro de adwares, softwares não autorizados que exibem propagandas no computador da vítima. Assim como os famosos cookies, também se prezam a coletar informações sobre um usuário de um serviço web (Jesus; Milagre, 2016, p. 34-35).

Nesta modalidade de invasão os transgressores tem consubstanciado seus escopos de forma sorrateira e isso lhes facilitam a captura de dados e senhas digitais, tornando assim, este delito em elevado grau de dificuldade para combatê-lo, razões pelas quais subjaz em seus modos operandi sagazes e ardilosos, assim, incumbe aos operadores do poder normativo a ponderação sobre tais aspectos e mais políticas repressivas.

11. CONSIDERAÇÕES FINAIS

A missão de combater crimes cibernéticos não tem sido tarefa fácil, pois, diante da dinâmica progressiva tecnologia atual é evidente que se intensifica também a massiva disparidade criminosa. Entretanto, não podemos deixar de mencionar também que internet tem seus aspectos positivos a qual viabiliza muitos recursos e facilidades nas atividades e operações desenvolvidas, o promissor vultoso espaço virtual também pode ser objeto de estudo e ferramentas de combate a violências e ameaças a direitos.

Diante dos embasamentos teóricos estudados, observamos que há uma procuração crucial do Estado em resguardar a liberdades cidadãos e a defesa do estado democrático. A vista disso, o poder estatal tem trabalhado por meios de regulação de normas e políticas de combates com o objetivo de inibir os criminosos de agirem livremente nas redes digitais.

Em outra análise, discorremos sobre alguns crimes virtuais em espécie e dentre eles os que mais causam danos às vítimas e à sociedade, seja por ferir a dignidade moral ou sexual, seja por auferir proveito financeiro ou por atos de mero capricho em satisfazerem suas vontades de delinquir.

Em uma análise mais sintetizada, podemos inferir que os crimes virtuais andam à frente do poder legislativo, posto que, embora este tenha empreendido esforços para edição de normas e regulamentos no sentido de combatê-los, parece-nos que não são suficientes, tendo ainda, muito o que ser deliberado e sancionado.

É irrefutável que os crimes cibernéticos tenham deixado seus rastros de prejuízos tanto aos cofres públicos quanto, aos particulares, portanto, políticas de combates devem ser estudadas e instituída neste enfrentamento, além disso, campanhas de esclarecimentos e elucidações sobre os perigos que circundam as redes digitais.

Diante desta explanação, o propósito da presente pesquisa foi colaborar para um caráter educativo, atrelado aos deveres de impor medidas de combate, por meio de políticas públicas e ações repressivas uniformes mais intensas, com o indispensável apoio de cooperações nacionais e estrangeiras.

Assim sendo, com a gradatividade incontrolável de crimes na internet a expectativa é que sejam instituídos órgãos de justiça especializados em direito digital que atuem com a finalidade exclusiva evitar e combater ações criminosas cibernéticas.

REFERÊNCIAS

ARAS, Vladimir. Crimes de informática. Uma nova criminalidade. **Informática Jurídica**, 2015. Disponível em: https://www.informatica juridica.com/author/vladimiraras/. Acesso em: 5 abr. 2023.

ARENDT, Hannah. **Sobre a violência**. Tradução: André Duarte. 3.ed. Rio de Janeiro, RJ: Relume Dumará, 1994.

AUSTEN, Jane *et al*. **Misoginia**: interdição e preconceito contra a mulher na Antiguidade Clássica: Unaspress, 2012. 216 / 212 p.

BAILEY, Moya. **Misoginoir transformada**: a resistência digital da mulher preta. Tradução: Camila Javanauskas. New York University Press: 2022. 272p. ISBN 978-65-86460-61-2.

BAPTISTA JUNIOR, José Henrique; DIAN, Maurício de Oliveira. A crescente importância da segurança de informação, sobretudo durante a pandemia. **Revista Interface Tecnológica**. Taquaritinga – São Paulo - Brasil, ano 2021, v. 18, n. 1, p. 56-67, 30 jul. 2021.

BARRETO, Alesandro Gonçalves; BRASIL, Beatriz Silveira. **Manual da investigação cibernética à luz do macro civil da internet**. Rio de Janeiro-RJ: Brasport, 2016. 293 p. ISBN 978-85-7452-816-8.

BASAN, Arthur Pinheiro. **Publicidade digital e proteção de dados pessoais**: o direito ao sossego. Indaiatuba, SP: Foco, 2021. 404 p. ISBN 978-65-5515-203-6.

BAUMAN, Zygmunt. **Modernidade Líquida**. Tradução: Plínio Dentzien. Rio de Janeiro: Zahar, 2001. 258 p. ISBN 85-7110-598-7.

BBC NEWS**. Entenda o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira de autoridades: Vazamento sem precedentes expôs dados de 50 milhões de usuários e mergulhou empresa em nova crise, pouco tempo depois de comoção sobre disseminação de notícias falsas**. G1, globo.com, 2018. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/entenda-o-escandalo-de-uso-politico-de-dados-que-derrubou-valor-do-facebook-e-o-colocou-na-mira-de-autoridades.ghtml. Acesso em: 8 maio 2023.

BEZERRA, Clayton da Silva *et al*. **Combate ao Crime Cibernético**: Doutrina e Prática – A visão do delegado de polícia. Rio de Janeiro: Mallet, 2020. 269 p. ISBN 978-85-92842-00-0.

BEZERRA, Clayton da Silva *et al*. (org.). **Combate às Fake News**: (A visão do delegado de polícia). São Paulo: Posteridade, 2019. 266 p. ISBN 978-85-53020-10-2.

BOTELHO, Rosana Camargo de Arruda *et al.* **Violência sexual contra crianças e adolescentes:** novos olhares sobre diferentes formas de violações. São Paulo: 2013. 370 p. Disponível em: https://www.mpba.mp.br/sites/default/files/biblioteca/crianca-e-adolescente/violencia sexual/cartilhas/violencia_sexual_contra_criancas_adolescentes_cartilha_abmp_childhood.pdf. Acesso em: 18 abr. 2023.

BRASIL. Constituição (1988). Constituição da República Federativa do Brasil de 1988. **Diário Oficial da União**. Brasília, 05 de out. de 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 11 abr. 2023.

BRASIL. Decreto nº 7.962, de 15 de março de 2013. Regulamenta a Lei nº 8.078, de 11 de setembro de 1990, para dispor sobre a contratação no comércio eletrônico. **Diário Oficial da União**. Brasília, 15 mar. 2013. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/decreto/d7962.htm. Acesso em: 10 mar. 2023.

BRASIL. Decreto-Lei 2.848, de 07 de dezembro de 1940. Código Penal. **Diário Oficial da União**. Brasília, 07 de dez. de 1940. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm. Acesso em: 30 abr. 2023.

BRASIL. Lei nº 4.737, de 15 de julho de 1965. Institui o Código eleitoral. **Diário Oficial da União**. Brasília, 15 de jul. de 1965. Disponível em: http://www.planalto.gov.br/ccivil_03/Leis/L4737.htm. Acesso em: 11 mar. 2023.

BRASIL. Lei nº 8.069, de 13 de julho de 1990. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. **Diário Oficial da União**, Brasília, 13 de jul. de 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: 30 abril. 2023.

BRASIL. Lei nº 10.446, de 8 de maio de 2002. Dispõe sobre infrações penais de repercussão interestadual ou internacional que exigem repressão uniforme, para os fins do disposto no inciso I do § 1o do art. 144 da Constituição. **Diário Oficial da União**. Brasília, 08 de maio de 2002.Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/2002/L10446.htm. Acesso em: 20 maio 2023.

BRASIL. Lei nº 11.419, de 19 de dezembro de 2006. Dispõe sobre a informatização do processo judicial; altera a Lei nº 5.869, de 11 de janeiro de 1973 – Código de Processo Civil; e dá outras providências. **Diário Oficial da União.** Brasília, 19 de dez. de 2006. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/l11419.htm. Acesso em: 9 mar. 2023.

BRASIL. Lei nº 11.829, de 25 de novembro de 2008. Altera a Lei no 8.069, de 13 de julho de 1990 - Estatuto da Criança e do Adolescente, para aprimorar o combate à produção, venda e distribuição de pornografia infantil, bem como criminalizar a aquisição e a posse de tal material e outras condutas relacionadas à pedofilia na internet. **Diário Oficial da União**. Brasília, 25 de nov. de 2008. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/lei/l11829.htm. Acesso em: 10 mar. 2023.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. **Diário Oficial da União**. Brasília, 30 de nov. de 2012. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 30 nov. 2012.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **Diário Oficial da União**. Brasília, 23 de abr. de 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 10 mar. 2023.

BRASIL. Lei nº 13.105, de 16 de março de 2015. Código de Processo Civil. **Diário Oficial da União**. Brasília, 16 de mar. de 2015a. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm. Acesso em: 10 mar. 2023.

BRASIL. Lei nº 13.185, de 6 de novembro de 2015. Institui o Programa de Combate à Intimidação Sistemática (Bullying). **Diário Oficial da União**. Brasília, 06 de nov. de 2015b. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13185.htm. Acesso em: 25 mar. 2023.

BRASIL. Lei nº 13.642, de 3 de abril de 2018. Altera a Lei nº 10.446, de 8 de maio de 2002, para acrescentar atribuição à Polícia Federal no que concerne à investigação de crimes praticados por meio da rede mundial de computadores que difundam conteúdo misógino, definidos como aqueles que propagam o ódio ou a aversão às mulheres. **Diário Oficial da União**. Brasília, 03 de abr. de 2018a. Disponível em http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13642.htm. Acesso em: 17 abr. 2023.

BRASIL. Lei nº 13.718, de 24 de setembro de 2018. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tipificar os crimes de importunação

sexual e de divulgação de cena de estupro, tornar pública incondicionada a natureza da ação penal dos crimes contra a liberdade sexual e dos crimes sexuais contra vulnerável, estabelecer causas de aumento de pena para esses crimes e definir como causas de aumento de pena o estupro coletivo e o estupro corretivo; e revoga dispositivo do Decreto-Lei nº 3.688, de 3 de outubro de 1941 (Lei das Contravenções Penais). **Diário Oficial da União**. Brasília, 24 de set. de 2018b. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13718.htm. Acesso em: 25 abr. 2023.

BRASIL. Lei nº 14.132, de 31 de março de 2021. Acrescenta o art. 147-A ao Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para prever o crime de perseguição; e revoga o art. 65 do Decreto-Lei nº 3.688, de 3 de outubro de 1941 (Lei das Contravenções Penais). **Diário Oficial da União**. Brasília, 31 de mar. de 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14132.htm. Acesso em: 10 abr. 2023.

BRASIL. Medida provisória nº 2.200-2, de 24 de agosto de 2001. Institui a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências. **Diário Oficial da União**. Brasília, 24 de ago. de 2001. Disponível em: https://www.planalto.gov.br/ccivil_03/mpv/antigas_2001/2200-2.htm. Acesso em: 16 mar. 2023.

CASTRO, Anaflavia Cera Daltro de; ZAGANELLI, Margareth Vetis. Catfishing: Crime de falsa identidade. **Revista de Estudos Jurídicos da UNESP**, Franca, v. 24, n. 40, p. 305-324, jul./dez. 2020. Disponível em: https://seer.franca.unesp.br/index.php/estudosjuridicosunesp/article/view/3099. Acesso em: 11 abr. 2023.

CASSANTI, Moisés de Oliveira. **Crimes virtuais, vítimas reais**. Tijuca Rio de Janeiro-RJ: Brasport, 2014. 162 p.

CERT.br. **Estatísticas dos Incidentes Reportados ao CERT.br**. Cert.br, 2023. Disponível em: https://www.cert.br/stats/incidentes/. Acesso em: 05 de mar. 2023.

DE LUCCA, Newton et al. **Direito & internet:** aspectos jurídicos relevantes. 2.ed., São Paulo: Quartier Latin, p. 179-207. 2005.

ESCOBAR, Patricia Elena Santos. **Misoginia e internet**: A manifestação do ódio contra mulheres no ambiente virtual e as possíveis implicações da Lei nº 13.642/2018. 2019. 74 f. TCC (Graduação em Direito) - Departamento de Ciências Jurídicas, Universidade Federal da Paraíba, Santa Rita, 2019. Disponível em: https://repositorio.ufpb.br/jspui/handle/123456789/14671?locale=pt_BR. Acesso em: 27 abr. 2023.

ESTEVAM, Marcelo Henrique de Sousa *et al*. **Estudos essenciais de direito digital**. Uberlândia: LAECC, 2019. 450 p. ISBN 978-65-80358-03-8. ebook.

FAUSTINO, André. **Fake News**: A Liberdade de Expressão nas Redes Sociais na Sociedade da Informação. São Caetano do Sul, SP -: LURA, 2019. ISBN 978-65-80430-25-3. Disponível em: www.luraeditorial.com.br. Acesso em: 15 abr. 2023.

FARAJ, Estela Freitas. **Direito digital**: Crimes cibernéticos contra a mulher. 2021. Trabalho de Conclusão de Curso (Bacharel em Direito) – Centro Universitário UNIFAAT, Atibaia/São Paulo, 2021. Disponível em: http://186.251.225.226:8080/handle/123456789/353. Acesso em: 25 abr. 2023.

FERNANDES, Ricardo Vieira de Carvalho; CARVALHO, Angelo Gamba Prata. **Tecnologia Jurídica & Direito Digital**: II congresso internacional de direito, governo e tecnologia. Fórum, Belo Horizonte, 2018.

GRUPO IBERDROLA. **Direitos digitais, imprescindíveis na era da Internet**. Iberdrola 2023. Disponível em: https://www.iberdrola.com/inovacao/o-que-sao-direitos-digitais. Acesso em: 15 mar. 2023.

JESUS, Damásio; MILAGRE. José Antonio. **Manual de crimes informáticos**. São Paulo: Saraiva, 2016.

KOPP, Daniele. **Homem é condenado por Cyberstalking após perseguir juíza**. Canal de ciências criminais, 8 dez. 2022. Disponível em:

https://canalcienciascriminais.com.br/homem-condenado-juiza-cyberstalking/. Acesso em: 12 jun. 2023.

LANA, Alice de Perdigão. **Mulheres expostas**: revenge porn, gênero e o Marco Civil da Internet. Curitiba: GEDAI/UFPR, 2019. ISBN 978-85-67141-27-5. ebook.

LOPES, Alan Moreira, *et al*. **Direito digital teoria e prática**. São Paulo: Tirant lo Blanch, 2021.

LONGHI, João Victor Rozatti *et al*. **Fundamentos do direito digital**. Uberlândia: LAECC, 2020. 480 p. ISBN 978-65-99099-21-2. ebook.

PEREIRA, Amanda Santa Helena; TEZA, Amanda. **A pedofilia virtual**: como conferir proteção integral aos direitos de crianças e adolescentes na rede? eGov UFSC, 29 out, 2018. Disponível em: https://egov.ufsc.br/portal/conteudo/pedofilia-virtual-como-conferir-prote%C3%A7%C3%A3o-integral-aos-direitos-de-crian%C3%A7-e-adolescentes-na. Acesso em: 30 abr. 2023.

PINHEIRO, Patrícia Peck. **Direito digital**. 6.ed., São Paulo: Saraiva, 2016.

PINHEIRO, Patricia Peck. **Direito digital**. 7.ed., São Paulo: Saraiva, 2021.

SABER DIREITO. Direito Digital - Aula 1. **Rádio e TV Justiça.** Brasília, 2022. 1 vídeo (55:19). Publicado pela: Rádio e TV Justiça. Disponível em: https://www.youtube.com/watch?v=AsLuIgccshM. Acesso em: 03 mar. 2023.

SANTOS, Fabio Celestino dos. **Estelionato sentimental - Quando o amor paga a conta**. Meu Artigo, 2022. Disponível em: https://meuartigo.brasilescola.uol.com.br/atualidades/estelionato-sentimentalquando-amor-paga-conta.htm. Acesso em: 6 abr. 2023.

SCHWAB, Klaus. **A quarta revolução industrial**. Tradução: Daniel Moreira Miranda. São Paulo: Edipro, 2016. 176 p. ISBN 978-85-7283-978-5

SILVA, Gilsimar Pinheiro. **Crimes digitais**: evolução dos crimes e a aplicação do direito. Orientador: Islamara da Costa. 2021. Trabalho de conclusão de curso (Bacharel em Direito) - Faculdade de Direito na Universidade Potiguar, Potiguar/RN, 2021. Disponível em: https://repositorio.animaeducacao.com.br/handle/ANIMA/22552. Acesso em: 27 abr. 2022.

SOUZA, Vivian; HELDER, Darlan. '**Deepfake ao vivo':** tecnologia que muda rosto e voz em videochamada, como na novela 'Travessia', já existe na vida real. G1. Globo.com, 2023. Disponível em: https://g1.globo.com/tecnologia/noticia/2023/04/01/deepfake-ao-vivo-tecnologia-que muda-rosto-e-voz-em-videochamada-como-na-novela-travessia-ja-existe-na-vida real. ghtml. Acesso em 30 abr. 2023.

TEIXEIRA, Tarcisio. **Direito Digital e processo eletrônico**. 6.ed., São Paulo: SaraivaJur, 2022.

TEIXEIRA, Tarcisio. **Direito digital e processo eletrônico**. 5.ed., São Paulo: Saraiva, 2020.

Enviado: 12 de setembro de 2023.

Aprovado: 21 de novembro, 2023.

[1] Graduado em Serviço Jurídico Cartorário e Notariais pela UNISA (2022). Acadêmico do 9º período do curso de Direito Centro Universitário São Lucas Ji-Paraná. ORCID: 0009-0005-9481-3268.
[2] Orientador. Especialista em Direito Processual Civil, Pós-graduando em Docência no Ensino Superior, ambos pela Faculdade FAVENI (2022), Bacharel em Direito pelo Centro Universitário São Lucas Ji-Paraná (2021). ORCID: 0009-0005-9146-2749.