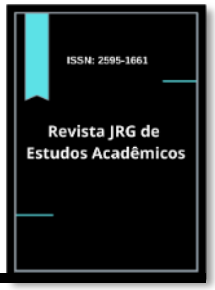
B1 ISSN: 2595-1661

ARTIGO DE REVISÃO

Listas de conteúdos disponíveis em Portal de Periódicos CAPES

Revista JRG de Estudos Acadêmicos

Página da revista:
https://revistajrg.com/index.php/jrg



A legislação brasileira e os crimes virtuais no Estado do Tocantins entre os anos de 2021 e 2023

Brazilian legislation and virtual crimes in the state of Tocantins between 2021 and 2023

DOI: 10.55892/jrg.v7i15.1663
ARK: 57118/JRG.v7i15.1663

Recebido: 16/11/2024 | Aceito: 23/11/2024 | Publicado *on-line*: 27/11/2024

Eva Barros dos Santos Macedo[1]
https://orcid.org/0009-0009-8102-2028
http://lattes.cnpq.br/9520306055549948
Faculdade Serra do Carmo, TO, Brasil
E-mail: evasantosmacedo09@gmail.com

Enio Walcácer de Oliveira Filho[2]
https://orcid.org/0000-0002-9137-2330
http://lattes.cnpq.br/6875090942782476
Faculdade Serra do Carmo, TO, Brasil
E-mail: ewalcacer@gmail.com

Resumo

O presente estudo apresenta uma análise acerca dos números de registro de crimes cibernéticos ocorridos no Tocantins entre os anos de 2021 e 2023. Apresenta um recorte legislativo de leis que contemplam crimes de natureza virtual, bem como as suas esferas de atuação. Além de promover reflexão no que tange a compreender as dificuldades de atuação da legislação nos cibercrimes. Para tanto, constituiu o método indutivo, contemplando a pesquisa exploratória baseada em dados e revisões bibliográfica e legislativas que permitiram concluir a ineficácia legislativa aliada às dificuldades de atuação de profissionais como a principal causa da ineficiência punitiva.

Palavras-chave: Internet; Crimes virtuais; Tocantins.

[1] Graduanda em Direito pela Faculdade Serra do Carmo.
[2] Mestre em Prestação Jurisdicional e Direitos Humanos, Especialista em Ciências Criminais e também em Direito e Processo Administrativo. Graduado em Direito e em Comunicação Social com habilitação em Jornalismo, todos os cursos pela Universidade Federal do Tocantins (UFT). Professor de Direito Processual Penal, escritor e pesquisador em Direito e Processo Penal e Direitos Humanos. Delegado da Polícia Civil do Tocantins.

Abstract
The present study presents an analysis of the registration numbers of cybercrimes occurring in Tocantins between the years 2021 and 2023. It presents a legislative outline of laws that cover crimes of a virtual nature, as well as their spheres of action. In addition to promoting reflection in terms of understanding the difficulties of legislation in cybercrimes. To this end, the inductive method was adopted, including exploratory research based on data and bibliographical and legislative reviews that made it possible to conclude that legislative ineffectiveness combined with the difficulties experienced by professionals as the main cause of punitive inefficiency.

Keywords: *Internet; Virtual crimes; Tocantins.*

1. Introdução

Criada em 1969, pelo projeto do Departamento de Defesa dos Estados Unidos, a internet é uma rede que estabelece conexão entre uma ampla quantidade de aparelhos eletrônicos em torno do mundo. Destaca-se que inicialmente era utilizada restritamente pelos militares para promover comunicação entre eles, uma vez que o cenário era de guerra. Hodiernamente, no entanto, com o avanço tecnológico e a expansão da globalização, o acesso às redes de navegação tornou-se amplamente disponível e acessível para praticamente todas as classes sociais.

Diante desse cenário, o espaço virtual se converteu em um ambiente passível de práticas delitivas, uma vez possibilitado o acesso aos dados de usuários, bem como a aglomeração da diversidade de ideologias que por vezes resultam em crimes de ofensa à honra. Assim, com a evolução tecnológica e a consequente globalização surgem os crimes virtuais, tanto como uma consequência do desenvolvimento das sociedades na forma de se relacionarem, como pela facilidade delitiva oferecida pela internet.

Os crimes virtuais são atos ilícitos praticados no espaço virtual com o intuito de roubar, ofender, denegrir, prejudicar, abusar psicologicamente ou fisicamente a outrem, estes são observados desde 1990 quando a internet se mostrava um sistema de comunicação pouco seguro e *hackers* já eram capazes de invadir os sistemas. No Brasil, os primeiros crimes virtuais são datados de junho de 1996, quando foi descoberta uma invasão em sites relacionados ao governo, como o oficial do Supremo Tribunal Federal.

No ano 1987, a lei nº 7.646, foi introduzida na legislação como a primeira, no Brasil, que tratou do espaço cibernético, esta foi revogada pela lei nº 9.609 de 1998 também dispondo sobre a proteção intelectual na programação de computadores, sua comercialização e outras providências. Posteriormente, outras leis foram introduzidas à legislação, mas considera-se que, em sua maioria, os crimes virtuais já estão tipificados no Código Penal, por se tratarem de crimes comuns praticados no ciberespaço. O que faz com que haja uma vasta possibilidade de cibercrimes.

Questiona-se, como enfoque deste trabalho: as legislações penais brasileiras atuais são suficientes para prevenir e reprimir o cometimento de crimes no ciberespaço?

Para responder à questão este artigo faz uma análise qualitativa de leis existentes no Brasil que visam a regulamentação do uso da internet, bem como as suas disposições acerca da proteção e das garantias no que tange ao ambiente virtual. Como filtro de inclusão de análise, a ênfase estará nas leis 12.737 de 2012 e

12.965 de 2014, tanto por serem as mais recentes sobre o assunto, como pelo conteúdo jurídico que apresentam.

Para que seja feita a análise das leis, é feita uma revisão de literatura sobre a temática, para abalizamento da análise, pautada em estudiosos da temática, tanto do direito quanto da área da tecnologia, permitindo entender como o uso da tecnologia pela sociedade civil, como uma rede de conexão, também possibilita o surgimento de um novo tipo de fenômeno criminal.

O estudo também permite um aporte reflexivo sobre as dificuldades enfrentadas pelos profissionais que atuam nessa área, sendo um campo aberto onde não existe uma delimitação fronteiriça como no mundo real, e as regulamentações tradicionais dos Estados esbarram na conexão global permitida no ciberespaço.

De maneira mais específica, o trabalho debruça-se sobre o cenário de acontecimento destes crimes no Estado do Tocantins, analisando os crimes mais recorrentemente investigados no âmbito da polícia civil do Estado, e a efetividade dessa atuação, bem como elementos que podem ser identificados na análise desse fenômeno criminal.

A relevância do tema é antevista em face a complexidade do mesmo, e a relevância que adquiriram o ciberespaço na atualidade não apenas Tocantinense, mas mundial, em vista da inexistência de fronteiras no mundo virtual e a dependência tecnológica percebida na sociedade atual.

2. Metodologia

O objetivo da presente pesquisa é, sob a ótica indutiva, verificar a efetividade legislativa na regulamentação da internet por meio da observação do fenômeno no Tocantins, de forma quantitativa, analisando a tipologia criminal e a efetividade do combate a tais delitos.

Assim, a metodologia utilizada para desenvolver o presente estudo detém um escopo qualitativo, na análise do conjunto legislativo pertinente, bem como quantitativo, na análise dos crimes ocorridos no meio virtual no Estado do Tocantins, entre os anos de 2021 e 2023, buscando-se o método indutivo para as conclusões acerca do fenômeno. Ainda, como complementação de base teórica, é feita uma revisão de literatura sobre o tema.

3. Da internet aos crimes virtuais

Pode-se afirmar que a internet teve seu surgimento em setembro 1969 através da Arpanet, uma rede de computadores montada pela ARPA (Advanced Research Projects Agency) que se tratava de uma subdivisão do Departamento de Defesa dos Estados Unidos que tinha a missão de mobilizar recursos de pesquisa com o objetivo de alcançar superioridade tecnológica militar em relação à União Soviética. Essa rede de computadores buscava manter a comunicação e o armazenamento de dados confidenciais do país, sendo montada em pontos estratégicos e todos interligados, de tal maneira que mesmo que houvesse ataque em um desses pontos a comunicação não seria perdida (Sousa e Volpe 2015).

Após o fim da Guerra Fria, essa rede foi muito utilizada pelas universidades, onde os estudantes poderiam trocar de forma ágil o resultado de seus estudos e pesquisas. Posteriormente, na década de 80, ocorreu a transição da Arpanet para o que se convencionou chamar de “internet”. Contudo, só por volta de 1990 que a Arpanet foi desativada de vez pelo Departamento de Defesa, sendo substituída pelos backbones da NSFNET e foi criado um sistema de hipertexto com o auxílio do CER.

A partir disso, a internet teve uma grande popularização, principalmente pelo que se conhece por “WWW” (World Wide Web). Em relação a isso, Castell explicita:

> O que permitiu à Internet abarcar o mundo todo foi o desenvolvimento da www. Esta é uma aplicação de compartilhamento de informação desenvolvida em 1990 por um programador inglês, Tim Berners-Lee, que trabalhava no CERN, o Laboratório Europeu para a Física de Partículas baseado em Genebra. Embora o próprio BernersLee não tivesse consciência disso (Berners-Lee, 1999, p.5), seu trabalho continuava uma longa tradição de ideias e projetos técnicos que, meio século antes, buscara a possibilidade de associar fontes de informação através da computação interativa. (Castell, pág. 16, 2003)

A partir desse momento a internet teve uma grande expansão pelo mundo, em razão do surgimento de novos navegadores como a internet Explorer, Mozilla Firefox, Google Chrome, Opera, dentre outros (Barroso, Silva 2022). Consequentemente o número de usuários aumentaram, que resultou na proliferação de sites, chats e as redes sociais. Surge porquanto, um esboço do que se tornaria a internet, uma importante ferramenta com redes sociais e navegadores que interligam o mundo todo, se tornando indispensáveis no dia a dia.

Como toda forma de tecnologia, a internet está em constante aprimoramento, não sendo um meio em que se pode garantir, na totalidade, a sua segurança. Nos anos 1960, quando do início da rede, começaram a surgir os primeiros infratores das regras e protocolos de rede, buscando desvendar falhas para uso no que foi o princípio de um tipo de guerra cibernética. A prática de busca por violações era feita para atos de sabotagem, espionagem, abusos gerais, e eram de difícil detecção nos primeiros anos dos sistemas conectados.

Em razão de tais violações, foram criadas, na década de 1970, nos EUA, as nomenclaturas *Hacker e Cracker* para designar pessoas que identificavam falhas e violavam computadores por meio da rede de conexão. Os *hackers* eram designados como aqueles que descobriam as vulnerabilidades, sem utilizar delas para benefício próprio ou de terceiros, apenas para alertar sobre falhas e aprimoramento de sistemas. Os *crackers,* por sua vez, eram aqueles que exploravam as falhas para benefícios pessoais ou de terceiros e para prejuízo de outros (Souza, 2015).

Para uma melhor compreensão Saldanha explica:

> O HACKER, espécie, é a pessoa que possui extremo conhecimento em TI (tecnologia da informação) e TC (tecnologia da comunicação), utilizando sua capacidade para explorar vulnerabilidades e aperfeiçoar sistemas. Tudo no intuito de buscar melhoria de software, de sistemas e de redes de uma forma legalizada. Em tese, não possuem motivação econômica. Diferentemente ocorre com os CRACKERS. Estes, também possuem um grande conhecimento em TI e TC. Porém, utilizam sua capacidade para fins ilícitos visando a obtenção de proveito pessoal, podendo, ainda, serem chamados de Ciberpiratas ou Black Hat. Possuem motivação econômica, comportamento malicioso e integram o crime organizado. (s.p). (Saldanha 2011 *apud* Souza; Volpe 2015)

É possível dizer, assim, que os *crackers* eram os criminosos originais, aqueles que atuavam à margem dos protocolos existentes para causar danos e se beneficiar de falhas, mesmo antes de qualquer legislação sobre o tema. Pode-se dizer que é um termo que abrange os criminosos, em uma analogia ao direito penal, em regra atuando de forma anônima por meio de protocolos e sistemas que garantiam a dificuldade de seu rastreamento.

Com a profusão de sistemas e aparelhos conectados à internet - smartphones, tablets, eletrodomésticos eletrônicos, televisões, além dos tradicionais computadores, as possibilidades de uso da rede para os benefícios da sociedade evoluiu, mas da mesma medida evoluíram as possibilidades de uso das vulnerabilidades das redes, e dos equipamentos a ela conectados, sendo o ciberespaço um terreno onde ano após ano vem aumentando a quantidade de cometimento de crimes.

3.1 O ciberespaço e a conceituação do crime virtual

Antes de entender o que é crime virtual, tem-se que ter a exata compreensão do que é o mundo virtual, ou o ciberespaço. A obra distópica de William Gibson, Neuromancer, tratou pela primeira vez da nomenclatura que daria conta desse espaço que, à época, estava sendo criado um espaço que não era propriamente físico, mas que permitia a interação, e hoje permite negócios, interações, conexões, enfim, toda a sorte de ações humanas (e não humanas). Para ele o ciberespaço é "[...] uma alucinação consensual, vivida diariamente por bilhões de operadores legítimos, em todas as nações, por crianças a que se estão a ensinar conceitos matemáticos." (GIBSON, 2004, p. 65)

Mas essa alucinação, bom frisar, é real, e hoje regula as relações humanas em vários graus e sentidos, logo, a chama-se o ciberespaço de virtual

> [...] porque está construída principalmente através de processos virtuais de comunicação de base eletrônica. É real (e não imaginária) porque é a nossa realidade fundamental, a base material com que vivemos a nossa existência, construímos os nossos sistemas de representação, fazemos o nosso trabalho, nos relacionamos com os outros, obtemos informação, formamos a nossa opinião, atuamos politicamente e alimentamos os nossos sonhos. (Silva e Conceição, 2013, p. 140)

Ou seja, o ciberespaço é também um mundo real, se for uma loucura coletiva, como argumentava Gibson, é uma loucura com consequências sólidas nas vidas cotidianas, pois grande parte do sistema atual é fundado com base nesse mundo virtual – bancos, processos jurídicos, documentos, dinheiro, relacionamentos, dados de localização, sistemas governamentais, etc.

Pois bem, dentro desse espaço real chamado mundo virtual, assim como acontecem nas relações no mundo não virtual, ou concreto, ocorrem também crimes. A doutrina brasileira de direito penal nomeia de forma diversas os crimes que ocorrem no meio virtual ou por intermédio de dispositivos conectados a ele - crimes da informática, cibercrime, crimes eletrônicos – são alguns dos nomes dados aos crimes que ocorrem no ciberespaço ou por intermédio dele (Kunrath, 2017, p.45).

O que se nota é que, conceitualmente falando, não se trata apenas de crimes que ocorrem *dentro do espaço virtual*, mas sim aqueles que se relacionam a esse espaço, por meio de dispositivos quaisquer que se conectam à rede da internet ou a utilizam como meio para a sua consecução.

Ao conceituar o que chama de *cibercrime*, Rosa explica ser

> A conduta atente contra o estado natural dos dados e recursos oferecidos por um sistema de processamento de dados, seja pela compilação, armazenamento ou transmissão de dados, na sua forma, compreendida

> pelos elementos que compõem um sistema de tratamento, transmissão ou armazenagem de dados, ou seja, ainda, na forma mais rudimentar; 2. O Crime de Informática é todo aquele procedimento que atenta contra os dados, que faz na forma em que estejam armazenados, compilados, transmissíveis ou em transmissão; 3. Assim, o Crime de Informática pressupõe does elementos indissolúveis: contra os dados que estejam preparados às operações do computador e, também, através do computador, utilizando-se software e hardware, para perpetrá-los; 4. A expressão crimes de informática, entendida como tal, é toda a ação típica, antijurídica e culpável, contra ou pela utilização de processamento automático e/ou eletrônico de dados ou sua transmissão; 5. Nos 10 crimes de informática, a ação típica se realiza contra ou pela utilização de processamento automático de dados ou a sua transmissão. Ou seja, a utilização de um sistema de informática para atentar contra um bem ou interesse juridicamente protegido, pertença ele à ordem econômica, à integridade corporal, à liberdade individual, à privacidade, à honra, ao patrimônio público ou privado, à Administração Pública, etc. (Bispo; Pinto, *apud* Rosa, 2002, p. 53).

Quanto à classificação, os cibercrimes subdividem-se em dois tipos: os Crimes Virtuais Próprios e os Crimes Virtuais Impróprios. Nos crimes próprios o sistema informático é utilizado como objeto e meio do crime praticado, ou seja, são aqueles que só podem ser praticados no meio virtual, vez que o bem jurídico protegido é a inviolabilidade das informações. Já os crimes impróprios, são aqueles praticados no meio informativo que visam “produzir resultado naturalístico, que ofenda o mundo físico ou o espaço “real”, ameaçando ou lesando outros bens, não-computacionais ou diversos da informática” (Jesus, 2003 *apud* Carneiro, 2012).

3.2 A internet no Brasil e os primeiros crimes virtuais

Segundo Eduardo Vieira (2003), a internet no Brasil teve seu marco inicial em 1988, quando a Fundação de Amparo à Pesquisa do Estado de São Paulo (Fapesp) realizou a primeira conexão com um dos maiores centros de pesquisa científica dos Estados Unidos, o Fermilab. Posteriormente, a Universidade Federal do Rio de Janeiro e o Laboratório Nacional de Computação Científica também se conectaram a universidades norte-americanas. A princípio, as conexões a rede eram voltadas exclusivamente para o setor acadêmico, sendo disponibilizadas para o público em geral anos depois.

O ano de 1996 marcou um verdadeiro "boom" da internet no Brasil. Esse crescimento acelerado foi impulsionado pela melhoria dos serviços oferecidos pela Embratel e, principalmente, pelo desenvolvimento natural do mercado (Vieira, 2023). Durante esse período, houve uma expansão significativa no número de usuários, provedores e na variedade de serviços disponibilizados pela rede.

Uma evidência clara de que a Internet já estava em plena expansão no Brasil ocorreu em 14 de dezembro de 1996, quando Gilberto Gil lançou uma música diretamente pela rede. Na ocasião, ele realizou uma apresentação ao vivo, em versão acústica, e interagiu com internautas, compartilhando suas experiências e perspectivas sobre a internet.

As literaturas que versam sobre os crimes virtuais e informáticos no país tiveram seus primeiros indícios no início do século XX, em meados de 1960, onde as primeiras aparições de crimes dessa modalidade surgiram, ou foram identificados, sendo relacionados em sua grande maioria com sabotagem e manipulação de grandes sistemas de computadores. Não significa que eram desconhecidos os crackers no Brasil, mas sim que as consequências criminais de determinadas condutas praticadas nas redes foram identificadas apenas nesse período.

No fim dos anos 80 e início dos anos 90, quando a internet começou a se expandir, a figura do *cracker* já se fazia presente, com o surgimento de crimes como invasão de sistemas e furto de software. Em 18 de junho de 1996, foi registrada, inclusive, uma invasão em sites ligados ao Supremo Tribunal Federal (Dantas, 2015).

Mas foi apenas no final dos anos 90, início dos anos 2000, que ocorreu uma maior disseminação dos variados tipos de crimes virtuais, entre eles a pirataria, pedofilia, invasão de sistemas e propagação de vírus (Santos *et al*., 2023).

Nas últimas décadas, com a ampla disseminação da internet, o Brasil intensificou suas preocupações sobre o impacto dessa tecnologia, o que levou à inclusão, na Constituição Federal de 1988, de disposições que conferem ao Estado responsabilidades também no campo da informática, abrindo-se o leque de proteção do Estado também ao ciberespaço brasileiro.

Atualmente, com a proliferação de dispositivos e pessoas conectadas à internet, os crimes previstos de forma tradicional, em um mundo ainda não conectado, mostram-se insuficientes para o combate ao fenômeno criminal que se potencializa na rede da internet no Brasil, mostrando a necessidade premente de uma legislação que preveja e permita a responsabilização criminal para condutas praticadas no meio virtual ou por meio dele.

Deve-se lembrar que o mundo virtual não é bem delimitado, não há fronteiras, sendo essencialmente uma rede mundial de dispositivos e pessoas conectadas, o que potencializa as dificuldades de controle de tudo que ocorre na rede. Mas tal dificuldade não pode ser óbice para a regulamentação, naquilo que for possível, dentro das legislações nacionais, como é o caso do Brasil. Consoante ao que defende Ramón J. Moles, “o ciberespaço não dispõe de fronteiras territoriais, mas de normas ou técnicas, que regulam sistemas de acesso e que não pertencem ao mundo jurídico. Assim, não vigora o conceito de soberania e nem de competência territorial” (Moles, 2000, *apud* Conte, 2008).

Mas, ressalta-se, ainda que não exista soberania ou competência nacional sobre os sistemas de acesso, não pode o Estado se escusar de responsabilizar ou limitar condutas que sejam praticadas por pessoas que estejam em território nacional, fazendo uso da rede, e que estejam sob sua jurisdição, pois assim fosse criar-se-ia um espaço sem lei onde tudo seria possível.

4.Um recorte legislativo sobre os crimes virtuais

É certo que há diversos obstáculos que dificultam a persecução de crimes cometidos no ciberespaço ou por meio dele, exigindo, portanto, um reajuste das categorias tradicionais que tratam do combate a crimes convencionais que ocorrem no mundo concreto. A garantia da segurança das redes, por parte do Brasil, é um imperativo estatal, como garantidor dos direitos que asseguram aos seus cidadãos, seja no mundo concreto ou virtual.

Para assegurar o uso das redes no Brasil, a primeira legislação que tratou o ciberespaço foi a lei nº 7.646 de 1987, posteriormente revogada pela lei nº 9.609/1998 que ainda se encontra em vigor. Esta traz importantes dispositivos sobre a proteção da propriedade intelectual e dos programas de computador, bem como outras considerações. A legislação trata apenas do resguardo a um escopo de direitos, os *da autoria*, apresentando em seu capítulo V, intitulado de “Das infrações e das penalidades”, o que muitos doutrinadores consideram a primeira tipificação associada a crimes cibernéticos.

Certamente que a legislação se mostrava insuficiente para as possibilidades de violações que permite o ciberespaço, sendo evidenciados dia após dia em noticiários

no Brasil e no mundo, desde violações a pessoas, individualmente, até a soberania nacional, como a espionagem de políticos e do próprio governo. Diante desse cenário de expansão de violações no ciberespaço, surgiu o Marco Civil da Internet no Brasil, lei nº 12.965 de 2014, trazendo previsões que estabelecem princípios, garantias e deveres no uso da internet no Brasil.

Em aprimoramento da lei, no ano de 2016, surgiu a sua regulamentação, por meio do Decreto nº 8.771 com o objetivo de suprir algumas lacunas, como a proteção de registros e dados e a neutralidade da rede. Nas palavras de Rogério Greco:

> O referido diploma legal foi regulamentado pelo Decreto nº 8.771, de 11 de maio de 2016, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela Administração Pública e estabelecer parâmetros para fiscalização e apuração de infrações. (Greco, 2024, pág. 430)

A primeira lei específica sobre crimes virtuais elaborada no ordenamento jurídico brasileiro foi a lei nº 12.737/2012, popularmente chamada de lei Carolina Dieckmann, em mais um exemplo de avanço legislativo brasileiro por casuísmos, e não por projetos e estudos. A lei foi criada em 2012 quando a atriz Carolina Dieckmann foi vítima de um crime virtual, após ter tido o endereço eletrônico invadido e fotos de cunho íntimo expostas nas redes de comunicação e informação.

A época a legislação brasileira não possuía nenhuma tipificação legal sobre crimes dessa natureza jurídica, sendo um avanço em termos de limitação de conduta no ciberespaço, como bem explica Ferreira (2022), foi a "[...] partir da promulgação desse instrumento legal, a internet, outrora campo livre para a ação de criminosos, passou a ser mais bem monitorada e fiscalizada, fazendo com que fosse maior a repressão a crimes como a prática de crimes."

Ocorre que, em 2012, a internet no Brasil já havia completado 16 anos desde seu "boom" (ocorrido por volta de 1996), mostrando mais uma vez o atraso do legislador frente a problemas que já vinham sendo evidenciados no país e no resto do mundo. Foi necessário um crime, como muitos outros que vinham acontecendo, atingir a uma pessoa que tivesse acesso às mídias, e que fosse conhecida para que o Congresso saísse de sua inércia, sendo então criada a lei nº 12.737.

A referida lei trouxe a previsão de crimes informáticos, além de ter provocado algumas mudanças no Código Penal acrescentando os artigos 154-A e 154-B na Sessão IV intitulado de "Crimes contra a inviolabilidade dos segredos". Em 28 de maio de 2021, com a promulgação da lei nº 14.155/2021, os artigos foram ajustados para expandir o alcance da modalidade fundamental e elevar o rigor punitivo, prevendo penas mais severas.

Os artigos mencionados dispõem:

> 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:
> Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa.
> § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.
> § 2º Aumenta-se a pena de 1/3 (um terço) a 2/3 (dois terços) se da invasão resulta prejuízo econômico.

> § 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:
> Pena – reclusão, de 2 (dois) a 5 (cinco) anos, e multa.
> § 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.
> § 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:
> I - Presidente da República, governadores e prefeitos;
> II - Presidente do Supremo Tribunal Federal;
> III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou
> IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.
> **Ação penal**
> 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 (Brasil, 2021).

A lei 12.737/2012, com o rompimento da inércia anterior, evidentemente representa um marco importante para a legislação brasileira, dando mais segurança aos milhões de usuários do ciberespaço no Brasil, sendo o começo de um caminho de regulamentação de condutas no espaço virtual como acontece com o espaço concreto.

Mas a lei é eficaz? Eis outro questionamento importante, pois vê-se foi criada mediante um populismo midiático, uma pressão criada por conta de uma pessoa com espaço nos meios de comunicação e conhecida, sendo feita às pressas, e talvez sem o estudo necessário do fenômeno em si. Neste aspecto explicam Reis e Viana (2021) que

> muitos estudiosos, doutrinadores e advogados especialistas no tema a reconhecem como fraca e ineficaz, como se a mesma tivesse sido feita às pressas apenas ocasionando a falsa sensação de segurança perante os crimes virtuais, onde os seus dispositivos podem gerar dupla interpretação, além de serem amplos e confusos o quê facilitaria o enquadramento de condutas triviais e utilizações mais amplas para a defesa dos criminosos, tendo ainda penas não inibidoras, ou seja, não tão incisivas a ponto de fazer com que os meliantes cometessem novamente crimes.

Sem entrar no mérito da suficiência da pena para prevenção geral e para a prevenção especial positiva, cabe entender se os mecanismos criados são eficazes para a tutela dos bens jurídicos violados, dada a dificuldade que se têm, quando, por exemplo, do vazamento de fotos íntimas, de se retirar isso das redes, posto a falta de fronteiras e limites do ciberespaço.

Mas para além dos crimes tipificados na lei, há uma profusão de outros crimes que podem acontecer no ciberespaço ou por seu intermédio, indo além do que se prevê na Lei 12.737/2012, e tais crimes tendem a um aumento, visto as possibilidades crescentes dos tipos de crimes que podem ocorrer no meio virtual.

Sobre essa evolução Almeida e Oliveira, no mesmo sentido, defendem que

> (...) os criminosos estão se tornando cada vez mais experientes em tecnologia, às vezes até mais do que as agências de investigações dos crimes cibernéticos. A aplicação da lei deve acompanhar os avanços tecnológicos para ficar a par das atividades criminosas online. Os Estados também precisam trabalhar muito para recrutar indivíduos com experiência em tecnologia que possam ajudá-los em seus esforços de investigação (Almeida; Oliveira, 2022, *on line*)

O que se vê é a incipiência legislativa na atualidade brasileira, incapaz de abarcar os crimes que podem ser cometidos com a rede ou por intermédio dela, sendo a lei 12.737/2012 uma legislação criada às pressas para agradar, de forma simbólica, um reclame midiático pontual e casuísta, não sendo amparada por estudos que demonstrassem as necessidades reais de tutela a bens jurídicos no ciberespaço. Ainda assim é um ponto de partida, que deve ser usado para o aprimoramento em debates com especialistas que possibilitem um avanço, mais do que necessário, de tutela para esse meio específico que é o mundo virtual.

5.Crimes virtuais no Tocantins segundo dados da Secretaria da Segurança Pública

Para entender o panorama dos crimes virtuais no Brasil, para o escopo deste trabalho, busca-se entender o panorama desses crimes no Estado do Tocantins, para traçar premissas gerais pelo método indutivo.

Os dados obtidos foram fornecidos pela Secretaria da Segurança Pública do Tocantins, que disponibiliza registros de boletins de ocorrência registrados nas Delegacias de Polícia Civil do Tocantins, por meio do sistema SINESP/MJSP.

No quadro há a indicação da natureza do delito, sendo listados os principais crimes praticados em âmbito virtual no Estado entre os anos de 2021 e 2023.

	Grupo Natureza	2021	2022	2023
1	ESTELIONATO	1.563	2.531	3.307
2	AMEAÇA	239	477	618
3	DIFAMAÇÃO	163	230	255
4	OUTROS FATOS ATÍPICOS	140	251	302
5	INJÚRIA COMETIDA OFENDENDO A DIGNIDADE OU DECORO	107	150	172
6	FURTO	81	53	70
7	CONFLITOS DIVERSOS – OUTROS	69	340	185
8	FRAUDE ELETRÔNICA COMETIDA COM A UTILIZAÇÃO DE INFORMAÇÕES FORNECIDAS PELA VÍTIMA OU POR TERCEIRO	69	412	643
9	CALÚNIA	55	78	111
10	FURTO QUALIFICADO COM ABUSO DE CONFIANÇA OU MEDIANTE FRAUDE, ESCALADA OU DESTREZA	49	53	56
11	INVASÃO DE DISPOSITIVO INFORMÁTICO	48	110	123
12	ESTELIONATO COMETIDO CONTRA IDOSO OU VULNERÁVEL	36	54	35
13	FALSA IDENTIDADE	31	129	76
14	OUTRAS FRAUDES	17	73	6
15	PERSEGUIÇÃO (STALKING)	15	32	66
16	EXTORSÃO	14	45	56

17	INJÚRIA REAL	14	25	16
18	FALSIDADE IDEOLÓGICA	13	18	23
19	PERTUBAÇÃO DO TRABALHO OU DO SOSSEGO ALHEIO	10	9	5
20	APROPRIAÇÃO INDÉBITA	9	11	24
21	DIFAMAÇÃO COMETIDA OU DIVULGADA EM QUAISQUER DAS REDES SOCIAIS DA REDE MUNDIAL DE COMPUTADORES/DIFAMAÇÃO COMETIDA CONTRA FUNCIÓNARIO PÚBLICO , EM RAZÃO DE SUAS FUNÇÕES	14	55	66
22	DIVULGAÇÃO DE CENA DE ESTUPRO OU DE CENA DE ESTUPRO DE VULNERÁVEL, DE CENA DE SEXO OU DE PORNOGRAFIA	6	20	13
23	FURTO QUALIFICADO SE COMETIDO POR MEIO DE DISPOSITIVO ELETRÔNICO OU INFORMÁTICO	6	59	72
24	DIFAMAÇÃO, INJÚRIA E CALÚNIA COMETIDA NA PRESENÇA DE VÁRIAS PESSOAS, OU POR MEIO QUE FACILITE A DIVULGAÇÃO DA CALÚNIA, DA DIFAMAÇÃO OU INJÚRIA	10	7	15
25	INVADIR DISPOSITIVO INFORMATICO RESULTANDO PREJUÍZO ECÔNOMICO	5	8	8
26	ESTUPRO	2	2	3
TOTAL		**4806**	**7254**	**8349**

Fonte: Secretaria da Segurança Pública do Tocantins (SSP-TO, 2024)

Conforme observa-se no quadro fixado, o Estado do Tocantins registra uma grande diversidade de crimes virtuais, sendo que alguns tipos de ocorrência aumentaram expressivamente nesse período, enquanto outros apresentaram redução. Essa variação revela mudanças no comportamento criminoso virtual, refletindo tanto o impacto das medidas de segurança implementadas quanto as mudanças nas práticas dos criminosos.

Entre os crimes que mais cresceram no período estão as fraudes eletrônicas, o estelionato e as ameaças virtuais. Esses crimes tiveram um aumento significativo, com destaque para a fraude eletrônica, que saltou de 69 ocorrências em 2021 para 643 em 2023. Esse aumento pode ser atribuído a golpes que utilizam informações pessoais das vítimas, muitas vezes obtidas por meio de redes sociais, phishing e manipulação psicológica, como em falsas campanhas de doação ou sorteios (Santos *et al.*, 2023). Esse crime causa impacto econômico direto, envolvendo transações fraudulentas que retiram quantias significativas das vítimas, muitas vezes causando prejuízos irreparáveis.

Cabe ressaltar que para tais crimes não há uma legislação específica, sendo utilizado para a sua reprimenda as legislações clássicas, independendo o meio virtual para a sua consumação.

O estelionato, que saltou de 1.563 ocorrências em 2021 para 3.307 em 2023, confirma a crescente sofisticação dos golpistas virtuais. Esse crime, muitas vezes praticado por meio de falsos investimentos ou de promessas de retorno financeiro garantido, expõe a vulnerabilidade dos usuários frente a esquemas que exploram a falta de informação financeira ou a confiança dos internautas em plataformas digitais. Os danos econômicos gerados são significativos, uma vez que esses crimes atingem desde transações bancárias até o roubo de senhas e informações pessoais,

comprometendo contas e gerando prejuízos que afetam as vítimas por longos períodos (Costa, Bezerra 2024).

Outro dado alarmante é o aumento das ameaças virtuais, que passaram de 239 ocorrências em 2021 para 618 em 2023. Esse tipo de crime não gera apenas danos econômicos, mas atinge diretamente a saúde mental das vítimas. A facilidade de difundir mensagens ofensivas, incitação ao ódio e até mesmo ameaças de violência física cria um clima de hostilidade no ambiente digital, e isso tem um impacto psicológico negativo tanto nas vítimas quanto nos usuários em geral, que se sentem intimidados a interagir livremente em redes sociais ou outras plataformas.

Outrossim, em que pese o crime de invasão de dispositivo informático não tenha crescido na mesma proporção que fraudes eletrônicas, estelionato e ameaças virtuais, ele também segue uma tendência ascendente. Em 2021, foram registradas 48 ocorrências, subindo para 123 em 2023. A ascensão desse crime, que envolve o acesso não autorizado aos dispositivos alheios, com o objetivo de roubar informações, manipular dados ou até mesmo instalar programas maliciosos, cuja tipificação adveio da lei nº 12.737/2012 (lei Carolina Dieckmann), evidencia a vulnerabilidade dos dispositivos conectados à internet e a falta de proteção adequada, ao passo que criminosos aprimoram continuamente suas técnicas de invasão.

Por outro lado, alguns crimes virtuais apresentaram uma redução ao longo do período analisado, com destaque para o furto, que possuía 81 registros em 2021 e caiu para 70 em 2023, e para a perturbação do trabalho ou do sossego alheio, que registrou 10 ocorrências em 2021 e apenas 5 em 2023. No entanto, essa redução não é altamente significativa e, especificamente no caso do furto, observa-se um aumento no furto qualificado, que cresceu expressivamente, sugerindo que não houve uma real redução na prática do crime, mas sim uma mudança na forma de execução.

Assim, com base na análise dos registros de boletins no Estado do Tocantins entre os anos de 2021 e 2023, é evidente que a maioria dos crimes praticados em ambientes virtuais aumentaram consideravelmente. Esse crescimento expressivo reflete a expansão do uso da tecnologia e das redes digitais, que, apesar de proporcionarem maior conectividade e facilidades ao cotidiano, acabam por também representar uma ampliação dos riscos e vulnerabilidades. O ambiente virtual, pela sua natureza de anonimato e dificuldade de rastreamento, mostra-se propício à prática de delitos, exigindo medidas preventivas cada vez mais robustas e a implementação de políticas públicas eficazes para coibir tais condutas e proteger os usuários de forma eficiente.

6. Considerações Finais

Como se nota, por meio dos dados do Tocantins, usando como premissa indutiva que refletem a realidade nacional, é que os crimes que ocorrem no ciberespaço, em geral, estão acontecendo cada vez com mais frequência. Há, conforme os dados analisados, uma crescente notificação de crimes cometidos no ciberespaço, sendo que, no Tocantins, entre os anos de 2021 e 2022 houve um aumento de 50,93% dos crimes ocorridos no ciberespaço, sendo que entre os anos de 2022 e 2023 o aumento foi de 15,5%, em um total acumulado de aumento, entre os anos 2021 e 2023 de 73,7% de aumento, extremamente considerável.

Quanto ao aumento dos números, diversos fatores devem ser considerados, para o escopo deste trabalho o que se denota é que a crescente implica em considerar que as penas ou mesmo a efetividade da punição está sendo baixa para os crimes ocorridos no ciberespaço, não sendo capaz de coibir o cometimento de novos crimes, que vem aumentando exponencialmente ano a ano. Há a possibilidade de que a

prevenção geral dos crimes não seja o suficiente para dissuadir os criminosos, ou seja, que não esteja sendo percebida as consequências de praticar um delito no ciberespaço para se evitar delinquir nesse meio virtual. Há ainda a possibilidade de que a persecução desses crimes seja dificultada, pela falta de treinamento ou de meios adequados, o que não adentrou no escopo dessa pesquisa.

Quanto a tipologia criminal, o que se percebe é que há uma tendência de migração de diversos crimes antes cometidos no meio concreto para o meio virtual, como ameaças, estelionato e até estupro, possível na modalidade virtual.

Sobre essa migração é importante a reflexão sobre o aprimoramento tanto das penas, ou a sua adequação ao meio, quanto da persecução desses crimes, já que demandam meios especializados para a sua repressão, e a efetividade mostra-se relevante para a prevenção geral.

Com o aumento da conectividade digital, fica claro que o Estado do Tocantins também registrou uma crescente incidência de crimes cibernéticos entre 2021 e 2023, destacando a predominância de crimes como fraudes eletrônicas, estelionato e ameaças virtuais. A análise dos dados revela que, embora a legislação brasileira tenha evoluído com marcos como a Lei 12.737/2012 (Lei Carolina Dieckmann) e a Lei 12.965/2014 (Marco Civil da Internet), ainda há insuficiências quanto à prevenção e repressão de crimes virtuais. As normativas vigentes, embora representem avanços, encontram-se defasadas frente à complexidade e à rapidez com que surgem novas formas de praticar os crimes no ambiente virtual.

O aumento expressivo de crimes virtuais demonstra que as infraestruturas de segurança pública enfrentam dificuldades para responder à demanda de investigação e combate ao cibercrime.

Como lacuna dessa pesquisa, sugere-se que sejam feitos estudos para identificar quais são as dificuldades enfrentadas pelos órgãos da persecução penal, sejam os órgãos policiais, ministeriais e judiciais, para a efetiva punição dos delinquentes cibernéticos, pois tal pesquisa pode evidenciar que além da desatualização do conjunto normativo penal, como visto nesta pesquisa, pode haver outros fatores conjugados para o aumento do fenômeno criminal no ciberespaço nos últimos anos.

Para os limites do horizonte pesquisado neste artigo, é necessária uma reforma legislativa penal para adequação dos tipos para terem uma efetividade na prevenção geral e especial, impedindo o crescimento dos crimes pelos fatores dissuasores da pena, ressaltando que não apenas isso é suficiente, devendo ser pesquisado ainda, junto a esse aprimoramento legislativo, se os órgãos da justiça criminal estão preparados para o enfrentamento dessa crescente criminalidade, e com as ferramentas adequadas para a aplicação efetiva dos conjuntos normativos atinentes à proteção de bens jurídicos para crimes cometidos no ciberespaço.

Referências

ALMEIDA, Haian de Assis Lopes de; OLIVEIRA, Tamar Ramos de. CRIMES VIRTUAIS: O AVANÇO DOS CRIMES ELETRÔNICOS E A EVOLUÇÃO DAS LEIS ESPECÍFICAS NO BRASIL. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, [S. l.], v. 8, n. 11, p. 277–294, 2022. DOI: 10.51891/rease.v8i11.7554. Disponível em: https://periodicorease.pro.br/rease/article/view/7554. Acesso em: 30 jun. 2024.

BARROSO, Sinak Rháyner Vieira da Cunha Fernandes; SILVA, Valdirene Cássia da. Os crimes cibernéticos e os desafios enfrentados no processo investigatório. Centro Universitário Católica do Tocantins, dez. 2022. Disponível em: https://repositorioto.catolica.edu.br/jspui/handle/123456789/141. Acesso em: 30 jun. 2024.

BISPO, Adrielle da Silva; BINTO, Emanuel Vieira. CRIMES CIBERNÉTICOS: DA INEFICÁCIA DA LEI CAROLINA DIECKMANN NA PRÁTICA DE CRIMES VIRTUAIS. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, [S. l.], v. 9, n. 11, p. 354–369, 2023. DOI: 10.51891/rease.v9i11.12291. Disponível em: https://periodicorease.pro.br/rease/article/view/12291. Acesso em: 7 nov. 2024.

BRASIL. Lei nº 9.609 de fevereiro de 1998. Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências. **Diário Oficial da União**, Brasília, 20 de fev. 1998. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9609.htm. Acesso em: 30 jun. 2024.

BRASIL. Lei n° 12.965 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **Diário Oficial da União**, Brasília, 24 de abril de 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 30 jun. 2024.

BRASIL. Lei n° 12.737, 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. 2012. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 30 jun. 2024.

COMO COMEÇOU A INTERNET NO BRASIL. 2018. Disponível em: http://www.controlltec.com.br/noticias/como-comecou-a-internet-no-brasil. Acesso em: 30 jun. 2024.

CASTELLS, Manuel. A Galáxia Internet: reflexões sobre a Internet, negócios e a sociedade. Rio de Janeiro: Zahar, 2003.

CONTE, Christiany Pegorari. DESAFIOS DO DIREITO PENAL NO MUNDO GLOBALIZADO: A APLICAÇÃO DA LEI PENAL NO ESPAÇO. **Migalhas**, 2008. Disponível em: https://www.migalhas.com.br/depeso/52372/desafios-do-direito-penal-no-mundo-globalizado--a-aplicacao-da-lei-penal-no-espaco. Acesso em: 30 jun. 2024.

COSTA, Ludymilla Sena; BEZERRA, Marco Antônio Alves. OS DESAFIOS DA INVESTIGAÇÃO CRIMINAL DE CRIMES VIRTUAIS NA ERA DIGITAL. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, [S. l.], v. 10, n. 10, p. 2111–2132, 2024. DOI: 10.51891/rease.v10i10.16023. Disponível em: https://periodicorease.pro.br/rease/article/view/16023. Acesso em: 2 nov. 2024.

CARDOSO, Rubenildo Kledir Soares. Direito digital: proteção de dados pessoais, crimes cibernéticos e liberdade de expressão na internet. **Jus.com.br**, 2023. Disponível em: https://jus.com.br/artigos/107538/direito-digital-protecao-de-dados-pessoais-crimes-ciberneticos-e-liberdade-de-expressao-na-internet. Acesso em: 2 nov. 2024.

DANTAS, Diego Maxwell Medeiros. Crimes virtuais. **Jus.com.br**, 2015. Disponível em: https://jus.com.br/artigos/42734/crimes-virtuais. Acesso em: 30 jun. 2024.

FERREIRA, Kethelyn Bianca Pereira da Silva. Crimes Cibernéticos: avanços trazidos com a lei Carolina Dieckman. **JNT - Facit Business and Technology Journal**, v. 3, n. 39, 2022. Disponível em: https://revistas.faculdadefacit.edu.br/index.php/JNT/article/view/1893/1279. Acesso em: 30 jun. 2024.

FREITAS, Victor Valério Medeiros Siqueira; SANTOS, Waldiney Batista dos; CURY, Leticia Vivianne Miranda. Crimes virtuais: um olhar sob a ótica do direito penal. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, São Paulo, v. 9, n. 05, mai. 2023.

GRECO, Rogério. Curso de Direito Penal - Vol. 2. [Digite o Local da Editora]: Grupo GEN, 2024. E-book. ISBN 9786559775811. Disponível em: https://app.minhabiblioteca.com.br/#/books/9786559775811/. Acesso em: 30 jun. 2024.

GIBSON, William. **Neuromancer.** São Paulo**:** Câmara Brasileira do Livro, 2014.

MAIA, Karolline Barbosa; COSTA, Cezar Henrique Ferreira. **CRIMES CIBERNÉTICOS**. Revista Ibero-Americana de Humanidades, Ciências e Educação, *[S. l.]*, v. 9, n. 10, p. 109–126, 2023. DOI: 10.51891/rease.v9i10.11580. Disponível em: https://periodicorease.pro.br/rease/article/view/11580. Acesso em: 27 jun. 2024.

MOREIRA, Paulo Roberto Silvério. **ESTELIONATO PRATICADO POR MEIO DA INTERNET: UMA VISÃO ACERCA DOS CRIMES DIGITAIS.** Migalhas. 2022. Disponível em: https://www.migalhas.com.br/depeso/359821/estelionato-praticado-por-meio-da-internet. Acesso em 1 nov. 2024.

REIS, Ariovaldo Nascimento Ribeiro; VIANA, Geraldo Denison. **CRIMES VIRTUAIS: LEGISLAÇÕES INSUFICIENTES OU INEFICIÊNCIA DAS AUTORIDADES COMPETENTES?**. Revista Ibero-Americana de Humanidades, Ciências e Educação, *[S. l.]*, v. 7, n. 10, p. 1607–1626, 2021. DOI: 10.51891/rease.v7i10.2684. Disponível em: https://periodicorease.pro.br/rease/article/view/2684. Acesso em: 25 jun. 2024.

SANTOS, Marconi Firmino. **Análise dos principais desafios na prevenção e combate aos crimes cibernéticos no estado do Tocantins.** JNT - Facit Business and Technology Journal, v. 3, n. 42 (2023). Disponível em: https://revistas.faculdadefacit.edu.br/index.php/JNT/article/view/2251/1518 Acesso em 30 jun. 2024.

SANTOS, Karl Heisenber Ferro. **Cibercrime :uma breve análise dos sujeitos e principais delitos virtuais.** Caderno de pós-graduação em direito: crimes digitais. Brasília, pág. 66. 2020.

SANTOS, Orismar Teixeira; NUNES, Nathalia Pereira; JUSTI, Jamson; JUSTI, Edrilene Barbosa Lima; JUSTI, Jadson. **EVOLUÇÃO DOS CRIMES CIBERNÉTICOS NA PANDEMIA.** Revista Ação Sustentável Global, Rio de Janeiro – RJ – Brasil, – Vol. 3, N. 4 – jan. / jun. 2023.

SILVA, Bento Duarte da. CONCEIÇÃO, Silvia Carla. Desafios do b-learning em tempos da cibercultura. In: **Cenários de inovação para a educação na sociedade digital**. São Paulo: Edições Loyola, 2013.

SOUZA, Henry Leones. VOLPE, Luiz Fernando Cassilhas. **Da ausência de legislação específica para os crimes virtuais**. Judicare. Disponível em:http://www.ienomat.com.br/revistas/judicare_arquivos/journals/1/articles/148/public/148-649-1-PB.pdf. Acesso em. 28 jun. 2024

TOCANTINS. Secretaria de Segurança Pública. **Estatísticas criminais: boletins de ocorrência registrados nas Delegacias de Polícia Civil.** Disponível em: https://www.to.gov.br/ssp/estatisticas/37s2impwz72k. Acesso em: 26 jun. 2024

VIEIRA, Eduardo. **Os Bastidores da Internet no Brasil: As histórias de sucesso e de fracasso que marcaram a Web brasileira.** São Paulo: Editora Manole Ltda. 2003.