PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
PRO-REITORIA DE GRADUAÇÃO
ESCOLA DE DIREITO, NEGÓCIOS E COMUNICAÇÃO
CURSO DE DIREITO
NÚCLEO DE PRÁTICA JURÍDICA
COORDENAÇÃO ADJUNTA DE TRABALHO DE CURSO

A EVOLUÇÃO CIBERNÉTICA E A FALTA DE PUNIBILIDADE CÉLERE DOS CRIMES DIGITAIS

CRIMES DIGITAIS NA PLATAFORMA WHATSAPP

ORIENTANDO (A): PAULO EDUARDO LEITE DIAS

ORIENTADOR (A): PROF. (A): DENISE FONSECA F. DE SOUSA

GOIÂNIA-GO
2023

PAULO EDUARDO LEITE DIAS

A EVOLUÇÃO CIBERNÉTICA E A FALTA DE PUNIBILIDADE CÉLERE DOS CRIMES DIGITAIS

CRIMES DIGITAIS NA PLATAFORMA WHATSAPP

Artigo Científico apresentado à disciplina Trabalho de Curso II, da Escola de Direito, Negócios e Comunicação da Pontifícia Universidade Católica de Goiás Prof. (a) Orientador (a): Dra. Denise Fonseca Felix de Sousa.

GOIÂNIA-GO
2023

PAULO EDUARDO LEITE DIAS

A EVOLUÇÃO CIBERNÉTICA E A FALTA DE PUNIBILIDADE CÉLERE DOS CRIMES DIGITAIS

CRIMES DIGITAIS NA PLATAFORMA WHATSAPP

Data da Defesa: 20 de maio de 2023

BANCA EXAMINADORA

_____

Orientador (a): Prof. (a): Dra. Denise Fonseca Felix de Sousa
Nota

_____

Examinador (a) Convidado (a): Prof. (a): Mestre. Processo Penal e Roberto Rodrigues
Nota

A EVOLUÇÃO CIBERNÉTICA E A FALTA DE PUNIBILIDADE CÉLERE DOS CRIMES DIGITAIS: CRIMES DIGITAIS NA PLATAFORMA WHATSAPP

Paulo Eduardo Leite Dias[1]

O avanço tecnológico tem facilitado a vida das pessoas, mas também possibilitado a prática de crimes virtuais. As organizações criminosas estão constantemente se aprimorando para a realização de novos golpes e práticas ilícitas, utilizando a internet como ferramenta para ocultar-se sob o manto do anonimato. Entre as condutas analisadas pelo presente projeto, destacam-se a invasão de dispositivo para obter, adulterar ou destruir dados sem autorização do proprietário e a instalação de vulnerabilidades para obtenção de vantagem ilícita. Apesar da existência de legislação específica, a punibilidade ainda é pouco efetiva e célere nos processos jurídicos. Para tanto, serão analisados os princípios da legalidade, reserva legal e analogia aos crimes cibernéticos, bem como as leis, doutrinas e jurisprudências sobre os crimes virtuais, em especial a forma de atuação dos criminosos na rede "WhatsApp" em Goiás. Conclui-se que há uma carência de legislação específica para tratar dos conflitos que crescem cada vez mais no ambiente virtual, o que dificulta a punição dos infratores. A internet é uma necessidade para a conexão e aprimoramento das atividades diárias. No entanto, a falta de cautela no uso da internet e a falta de conscientização dos usuários sobre os recursos disponíveis são fatores que afetam o desenvolvimento da internet, cuja criminalidade tem aumentado. É imperativo que haja mais pesquisas, ideias, criatividade e tecnologia para combater e prevenir efetivamente esses delitos no futuro. Por fim, há um aumento da criminalidade no Estado de Goiás, com informações sobre as ferramentas de combate e prevenção.

Palavras-chave: Crimes Cibernéticos. Goiás. Tecnologia.

[1] Paulo Eduardo Leite Dias e Bacharel em Direito na Universidade PUC/GO.

INTRODUÇÃO

A celeridade na criação de tecnologias é notável. Não obstante, constata-se que uma parcela da sociedade emprega ferramentas tecnológicas com o propósito de perpetrar ilícitos e praticar o mal, como ocorre nos delitos cometidos virtualmente. Na seara criminosa, as organizações delituosas estão constantemente aprimorando-se para a realização de novos golpes. A internet facilita a atuação dos criminosos que se utilizam da rede mundial de computadores, ocultando-se em sua maioria sob o manto do anonimato. Tal circunstância dificulta sobremaneira tanto sua identificação pessoal como sua localização.

A invasão de dispositivo com o objetivo de obter, adulterar ou destruir dados ou informações sem autorização do proprietário, ou ainda a instalação de dispositivos e programas que geram vulnerabilidades para obtenção de vantagem ilícita, serão as condutas analisadas pelo presente artigo. Apesar da existência de lei específica, faz-se necessário analisar de maneira mais abrangente como coibir essa prática delituosa de maneira mais célere e com mais rigor na aplicação da punição.

Frente a esse cenário o presente estudo tem por objetivo analisar o crime digital, nos tempos atuais e a falta de punibilidade célere a essa modalidade de delito. Como objetivos específicos buscou-se: Entender como a rotina humana está voltada em seu cotidiano ao mundo virtual; Analisar a aplicabilidade dos princípios da legalidade, reserva legal e analogia aos crimes cibernéticos; Compreender os crimes atuais cibernéticos e a forma de atuação destes criminosos na rede "WhatsApp" em Goiás; Analisar leis, doutrinas e jurisprudências sobre os crimes pontuando as principais dificuldades encontradas pelos operadores do direito no que diz respeito a punir os infratores.

A metodologia adotada para realização do estudo foi moldada por abordagem dedutiva e por procedimento bibliográfico, analisando também as legislações nacionais, estaduais e posicionamentos dos tribunais.

O presente artigo pertence à linha de pesquisa: Estado, Relações Sociais e Transformações Constitucionais.

1 A TECNOLOGIA E SEUS IMPACTOS NA SOCIEDADE

Desde os tempos mais remotos da história da humanidade, o ser humano sempre teve a necessidade de se relacionar com o próximo e viver em comunidade. Em decorrência disso, as pessoas sempre buscaram meios de se comunicar e interagir umas com as outras, por meio dos mais variados canais.

A internet, por sua vez, se apresenta como um importante aliado para a promoção da interação social, fato evidenciado pelo grande número de usuários que acessam essa plataforma. Desde a década de 90, com o surgimento da rede mundial de computadores, a internet revolucionou a vida humana, e essa revolução tecnológica segue em constante crescimento ao longo do século XXI. Nesse contexto, surgiram as redes sociais, atendendo à necessidade natural do ser humano de viver em sociedade e de se comunicar com os outros.

Considerando o caráter global da internet e a ausência de um domínio único sobre suas dimensões, é preciso estar atento aos efeitos do mundo virtual na vida real dos usuários. Assim, é equivocado afirmar que a internet seria um meio de livre e irrestrita circulação de informações, onde qualquer tipo de restrição ou censura seria proibida.

O termo "rede social" é utilizado para designar uma plataforma digital na qual qualquer pessoa pode criar uma identidade virtual com o intuito de interagir com outras pessoas. A criação desses perfis é rápida e prática, exigindo que o usuário insira algumas informações pessoais, as quais ficarão disponíveis aos demais usuários. Dentre as redes sociais mais comuns, destacam-se o Facebook, Instagram, Youtube, Twitter e Whatsapp.

O WhatsApp é um aplicativo de mensagens instantâneas que permite aos usuários conversar, enviar fotos, vídeos curtos, áudios e fazer chamadas em tempo real de forma prática e sincronizada com a lista de contatos do dispositivo. Além disso, é possível criar grupos com até 257 membros e compartilhar qualquer tipo de mídia, incluindo emoticons para expressar sentimentos (ALECRIM, 2019).

O empreendedor Jan Koum nasceu e cresceu em uma aldeia próxima a Kiev, na Ucrânia. Ele é filho único de uma família de baixa renda e, aos 16 anos, mudou-se com sua mãe para o Vale do Silício, nos Estados Unidos, fugindo da crise política e da violência antissemita em seu país (MARQUES, 2019).

Koum aprendeu inglês e os fundamentos da ciência da computação por conta própria. Em 1997, ele começou a trabalhar na Yahoo, onde conheceu Brian Acton e se tornaram amigos. Em 2007, eles deixaram a Yahoo e tentaram trabalhar no Facebook, mas foram rejeitados. Em

2009, Koum comprou seu primeiro iPhone e percebeu o enorme sucesso da recém-lançada App Store. Então, ele teve a ideia de desenvolver seu próprio aplicativo (ALECRIM, 2019).

Koum e Acton receberam a ajuda do programador russo Igor Solomennikov, que foi responsável pela primeira programação do aplicativo. Os três se conheceram em uma reunião de amigos em comum e Solomennikov aceitou imediatamente o convite para 4ende-los. No entanto, a primeira versão do aplicativo era muito instável.

A história do WhatsApp teve início com a concepção de um aplicativo que possibilitaria conexão direta à lista de contatos do smartphone do usuário, exibindo um pequeno status ao lado de cada nome. Atualmente, o WhatsApp é o aplicativo mais popular em todo o mundo, com mais de 1,5 bilhões de usuários ativos mensais em mais de 180 países. Seu nome é uma forma humorada da expressão “What’s Up?”, que significa “E aí, como vai?”.

O aplicativo permite a troca de mensagens, áudios, vídeos e fotos pela internet, o que revolucionou a comunicação entre as pessoas. Sua função principal é conectar diretamente à lista de contatos do smartphone do usuário e exibir um pequeno status ao lado de cada nome. O WhatsApp foi desenvolvido como um serviço de mensagens instantâneas e simultâneas para smartphones, com foco na rapidez e na capacidade de funcionar em qualquer lugar do mundo, de forma gratuita.

Inicialmente, o WhatsApp era uma alternativa ao SMS (Short Message Service), que é o serviço de mensagens entre celulares. Naquela época, era apenas possível enviar mensagens de texto, sem a possibilidade de enviar fotos, áudios, arquivos ou realizar chamadas. No entanto, com o tempo, o aplicativo evoluiu e incorporou diversas inovações, incluindo a possibilidade de enviar fotos, vídeos, áudios e realizar chamadas de vídeo e áudio.

Em 2016, o WhatsApp alcançou a marca de 1 bilhão de usuários ativos, e a equipe do aplicativo tinha cerca de 100 funcionários, incluindo 57 engenheiros de software. Nesse mesmo ano, o aplicativo deixou de cobrar US$1 a cada 12 meses, tornando-se completamente gratuito e sem anúncios de empresas. Houve discussões sobre a possibilidade de monetização do aplicativo, mas os fundadores Brian Acton e Jan Koum eram contra o uso de anúncios. Porém, Mark Zuckerberg discordava e em 2017 foi lançado o WhatsApp Business, uma versão gratuita do aplicativo voltada para empresas (NUVENS, 2018).

Lançado em 2009, o WhatsApp possui aproximadamente 1,5 bilhão de usuários em todo o mundo. É perceptível que o aplicativo está presente em todo o território nacional, promovendo a interconexão entre as pessoas e reduzindo distâncias. Entretanto, é frequente a criação de

usuários com informações falsas acerca da identidade de seus usuários, muitas vezes vinculadas a indivíduos fictícios ou reais alheios à pessoa responsável pelo perfil (NUVENS, 2018).

Os crimes de estelionato cometidos através do aplicativo de mensagens WhatsApp têm se tornado cada vez mais comuns nos dias atuais. Nesse tipo de crime, os golpistas utilizam a plataforma para obter informações pessoais e financeiras das vítimas, com o intuito de realizar fraudes e obter vantagens indevidas.

Os criminosos utilizam técnicas de engenharia social, como a criação de perfis falsos e o envio de mensagens persuasivas, para convencer as vítimas a compartilharem seus dados pessoais e bancários. Além disso, também podem utilizar técnicas de clonagem de contas para se passar por amigos ou familiares da vítima, solicitando transferências de dinheiro.

2 CRIMES VIRTUAIS E A LEGISLAÇÃO BRASILEIRA

O avanço das novas tecnologias impulsionando a globalização, a crescente popularidade da Internet proporcionando conveniência aos usuários, bem como a circulação de comércio eletrônico, dinheiro e informações, contribuíram para que a Internet se tornasse um ambiente extremamente atraente para a prática de crimes por parte de indivíduos mal-intencionados (TEIXEIRA, 2020).

Há o entendimento de que o surgimento da sociedade da informação teve início na década de 1970, caracterizada pela coexistência dos mundos físico e digital, exigindo que seus participantes acessem cada vez mais informações e transponham fronteiras. Nesse contexto, conforme o pensamento do autor, o surgimento da Internet faz com que as pessoas busquem incessantemente informações em tempo real (PINHEIRO, 2021).

A crescente informatização das diversas atividades desenvolvidas pela sociedade, tanto individualmente quanto coletivamente, tem fornecido aos criminosos novas ferramentas, cujo impacto ainda não foi adequadamente avaliado, uma vez que surgem diariamente novas formas de lesão aos mais variados bens e interesses, que é incumbência do Estado proteger, propiciando assim o surgimento de uma criminalidade específica da informática, cuja tendência é aumentar quantitativa e qualitativamente e aprimorar seus métodos de execução (TEIXEIRA, 2020).

Assim, conforme evidenciado, a velocidade do desenvolvimento tecnológico proporcionado pelo avanço da Internet tem gerado uma atividade criminosa especializada e cada vez mais bem equipada.

Embora a doutrina apresente diversas denominações, as mais comuns são mencionadas em publicações sobre o tema, tais como: crime de computador, crime pela Internet, crime de tecnologia, crime digital, crime cibernético, crime de informação, entre outras (TEIXEIRA, 2020). Ademais, o crime de informática pode ser definido como aquele que utiliza meios informáticos como instrumento para alcançar o resultado pretendido, conforme explica Teixeira (2020).

Destaca-se que o cybercrime se configura como qualquer conduta ilegal, não ética ou não autorizada que envolva o processamento automático de dados e/ou transmissão de dados. Essa forma de criminalidade apresenta características como transnacionalidade, por ser veiculada virtualmente, com acesso e uso por todos os países; universalidade, por ser um fenômeno de massa e não de elite; e ubiquidade, por estar presente nos setores privados e públicos (LORENZO; SCAVARELLI, 2021).

Em geral, o cybercrime é caracterizado pelos meios utilizados para cometer atos ilícitos, ou seja, com o auxílio da Internet e dispositivos eletrônicos, podendo ser realizado em qualquer lugar do país, tendo em vista que qualquer pessoa pode ser vítima.

É importante destacar que o delito cibernético ou eletrônico possui natureza criminal, com exceção dos delitos cometidos por hackers, que ocorrem exclusivamente em ambiente virtual, no qual o delito é materializado, embora em alguns casos não seja perceptível. O crime eletrônico assume diferentes formas, dependendo dos interesses jurídicos protegidos pela norma. A Internet surge como um meio facilitador para a aplicação dos conceitos de crime e outros termos no âmbito do Direito Penal (PINHEIRO, 2009).

Nesse sentido, a análise do conceito de crime permite concluir que os crimes cibernéticos são atos típicos, ilegais e criminosos cometidos contra ou por meio de sistemas informatizados (ALMEIDA, 2015).

Assim, de acordo com o entendimento do autor, toda ação prevista no Código Penal pode ser considerada como um possível crime virtual se for cometida por meio de dispositivo conectado à Internet. Os crimes virtuais podem ser classificados como abertos e exclusivamente cibernéticos, que só podem ser cometidos por meio de computadores ou outros dispositivos técnicos que permitam o acesso à Internet, e aqueles que também podem ser praticados de forma convencional, mas que estão relacionados ao acesso à Internet (WENDT; JORGE, 2013).

Tabosa e Faria (2021) afirmam que o crime digital é qualquer conduta tipificada em lei como crime, que utilize o computador como instrumento ou objeto material.

Os crimes cibernéticos podem ser classificados como legítimos ou ilegítimos. No primeiro caso, a ação visa atingir a confiabilidade, integridade ou disponibilidade do sistema. No segundo caso, o ato criminoso pode ser realizado com o uso de mecanismos informatizados, mas também pode ocorrer de outras formas (VIEIRA, 2021).

Em face da relevância do tema e da responsabilidade inerente ao poder público de proteger os direitos e garantias fundamentais, a legislação para criminalizar o cibercrime e os meios para preveni-lo e reprimi-lo ainda permanecem inadequados. Em conclusão, as Leis nº 12.735/12, 12.737/12 e 12.965/14 ainda não possuem eficácia suficiente para combater tais crimes de forma efetiva.

O Poder Executivo reconhece a relevância de proteger a sociedade no âmbito virtual e promulgou a Lei nº 14.155/2021 no Diário Oficial da União, que aumenta as sanções para delitos como fraudes, furtos e descaminhos realizados por meio de dispositivos eletrônicos como celulares, computadores e tablets.

Digno de nota é o art. 154-A, do Código Penal, recentemente modificado, cuja redação é a seguinte:

> 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 (BRASIL, 1940).

A Lei nº 12.737/12, que tipifica os crimes informáticos, introduziu modificações no Decreto nº 2.848/40 (Código Penal Brasileiro), sendo que seu art. 266, §2º prevê a aplicação da pena em dobro se o crime for praticado em situação de calamidade pública. Em casos excepcionais, como o da pandemia de COVID-19, os delitos cometidos por meio da informática são sancionados com a agravante da situação flagrante, de acordo com as disposições regulamentares (BRASIL, 2012).

Assim sendo, cabe à legislação cumprir rigorosamente seu papel de punir os indivíduos que, utilizando habilidades e conhecimentos específicos relacionados à tecnologia, criam softwares intrusivos capazes de coletar e divulgar ilegalmente informações em ambientes virtuais. Esse é um meio de comunicação alternativo, mas profissionalmente, socialmente e, politicamente, urgente e necessário, sobretudo diante das medidas legais de distanciamento, isolamento, uso de máscaras e álcool gel estabelecidas pelo Ministério da Saúde durante a pandemia.

De outra forma, a Lei nº 12.735/12 normatiza as condutas cometidas em desfavor de sistemas informáticos e institui departamentos especializados conforme o ordenamento jurídico, sendo relevante salientar o art. 4º do referido diploma legal que determina que "os órgãos da polícia judiciária organizarão, nos moldes de regulamentação, setores e grupos especializados no enfrentamento de atividades criminosas em rede de computadores, aparelho de comunicação ou sistema informatizado".

Em conformidade com o Marco Civil Histórico da Internet, Lei nº 12.965/14, o artigo 1º estabelece princípios, garantias, direitos e deveres para a utilização da internet no território nacional, e estabelece as diretrizes para a atuação da União, dos Estados, do Distrito Federal e dos Municípios nessa matéria. Essa legislação define os direitos e obrigações dos usuários da internet em relação à proteção de dados pessoais e privacidade. Sendo assim, a confidencialidade de dados e informações pessoais em ambientes virtuais somente poderá ser violada mediante ordem judicial.

O acesso à internet é considerado essencial para o exercício da cidadania e, portanto, a Lei 12.965/14 assegura aos usuários os seguintes direitos:

> Art. 7º.
> VI – Informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicaçõesde internet, bem como sobre práticasde gerenciamento da rede quepossam afetar sua qualidade;
> VII – não fornecimento a terceiros deseus dados pessoais, inclusiveregistros de conexão, e de acesso aaplicações de internet, salvo medianteconsentimento livre, expresso einformado ou nas hipóteses previstasem lei; (BRASIL, 2014)

Conforme estabelecido em seu artigo 4º, a Lei 12.965/14 tem como objetivos: assegurar o direito de acesso à internet para todos; fomentar o acesso à informação, ao conhecimento e à participação na vida cultural e na gestão dos assuntos públicos; incentivar a inovação e a ampla disseminação de novas tecnologias e modelos de uso e acesso; e estimular a adoção de padrões tecnológicos abertos que possibilitem a comunicação, a acessibilidade e a interoperabilidade entre aplicações e bancos de dados.

Os direitos e garantias dos usuários estão previstos no artigo 7° da Lei 12.965/14, os quais guardam semelhança com o artigo 5° da Constituição Federal, e incluem: inviolabilidade da intimidade e da vida privada, com direito a proteção e indenização por danos materiais ou morais decorrentes de sua violação; inviolabilidade e sigilo do fluxo de comunicações pela internet, salvo por ordem judicial, nos termos da lei; inviolabilidade e sigilo das comunicações

privadas armazenadas, salvo por ordem judicial. É importante observar que essas garantias de inviolabilidade são semelhantes às previstas na Constituição Federal, que estabelece a proteção ao sigilo das comunicações, exceto por ordem judicial e na forma da lei, e a proteção das informações privadas armazenadas na internet, como redes sociais e e-mails.

2.1 LEI ESTADUAL Nº 19.907 DE 14 DE DEZEMBRO DE 2017

A Lei nº 19.907 de 14 de dezembro de 2017 é uma legislação que dispõe sobre a criação de várias delegacias especializadas em Goiás, com o objetivo de combater diferentes tipos de crimes que ocorrem no estado.

A primeira delegacia criada pela lei é a Delegacia Estadual de Repressão a Crimes Rurais (DERCR), que tem como objetivo investigar e reprimir crimes praticados no meio rural, como roubo de animais, invasão de propriedades e outros delitos relacionados. A segunda delegacia criada é a Delegacia Estadual de Repressão a Crimes Cibernéticos (DERCC), que tem a finalidade de investigar crimes cometidos por meio da internet, como fraudes eletrônicas, cyberbullying, ataques virtuais e outros. Além dessas duas delegacias, a lei também cria três Delegacias Especializadas no Atendimento à Pessoa com Deficiência (DEAPD), localizadas nas cidades de Goiânia, Anápolis e Aparecida de Goiânia. Essas delegacias têm como objetivo atender e proteger os direitos das pessoas com deficiência, além de investigar crimes relacionados a esse grupo social. Por fim, a lei também cria a Delegacia Especializada no Atendimento ao Idoso de Aparecida de Goiânia (DEAI), com a finalidade de proteger e atender os direitos das pessoas idosas, além de investigar crimes relacionados a esse grupo vulnerável.

A criação dessas delegacias especializadas foram importantes para o fortalecimento ao combate a diferentes tipos de crimes em Goiás e garantir a proteção dos direitos das pessoas com deficiência e idosos, além de reforçar a atuação do Estado no combate aos crimes rurais e cibernéticos.

Criada através da referida lei a Delegacia Estadual de Repressão a Crimes Cibernéticos (DERCC) é uma unidade especializada da Polícia Civil responsável por investigar crimes cometidos por meio eletrônico, como fraudes, estelionatos, crimes contra a honra, pedofilia, entre outros.

A DERCC possui uma equipe de policiais civis treinados e capacitados para atuar em ambientes virtuais, utilizando técnicas de investigação e tecnologia para coletar e analisar evidências digitais. Além disso, a unidade atua em parceria com outras instituições, como o

Ministério Público e a Justiça, para garantir a efetividade das investigações e a punição dos criminosos.

Entre as principais atividades realizadas pela DERCC estão a identificação de perfis falsos em redes sociais, a investigação de crimes de invasão de sistemas e a recuperação de dados e informações roubados. A unidade também atua na orientação da população sobre como se prevenir de crimes virtuais e na promoção de campanhas educativas sobre segurança digital.

Com a crescente utilização da internet e das redes sociais, a DERCC se torna cada vez mais importante para garantir a segurança da população no ambiente virtual, contribuindo para a redução dos índices de criminalidade nessa área.

2.2 LEGISLAÇÃO INTERNACIONAL

Considerando a universalidade da prática de ilícitos penais virtuais e a necessidade de cooperação internacional para lidar com essa questão, diante da complexidade dos fatos apresentados no primeiro capítulo e do elevado potencial de lesividade, tais como a perda de privacidade, o anonimato do infrator, a facilidade de propagação e a transnacionalidade desses crimes, é essencial tratar esse tipo de criminalidade para garantir a segurança global das sociedades.

Conforme preceitua Cláudia Perrone Moisés, seguindo a tradição de Nuremberg, o direito internacional penal pode ser qualificado, em primeiro lugar, como um direito que protege interesses fundamentais e bens supremos, como a paz e a dignidade do ser humano. Portanto, os delitos regulados por esse direito são atos que violam a ordem pública internacional por meio de infrações contra o direito internacional. Tais infrações interessam ao conjunto da comunidade internacional por atingirem valores considerados fundamentais para todos os Estados (MOISÉS, 2012).

No presente contexto, os delitos virtuais podem ser tutelados pelo Direito Penal Internacional, visto que configuram atos transgressores da ordem pública internacional, ultrapassando as fronteiras nacionais e afetando valores essenciais dos Estados, colocando em risco a ordem jurídica global. Tendo em vista que a internet não se circunscreve a limites geográficos específicos, é imprescindível uma regulamentação global. A Convenção de Budapeste sobre o Cibercrime, firmada em 2001, representa um avanço na cooperação penal e regulação transnacional, visando à mais efetiva repressão de infrações cibernéticas. Referida Convenção, que

conta com a adesão de 43 países, é considerada uma legislação de referência mundial em matéria de crimes na internet (CÂMARA DOS DEPUTADOS, 2011).

A Convenção de Budapeste sobre o Cibercrime possui relevante finalidade voltada à defesa da sociedade internacional, mediante a adoção de uma legislação e a promoção da cooperação internacional. Compreende diversos delitos, tais como fraudes informáticas, violações de direito autoral, pornografia infantil e invasões de computadores, estabelecendo ainda procedimentos entre os Estados-partes.

A referida Convenção constitui um importante marco para a cooperação penal internacional, tendo em vista o aprimoramento das ferramentas de auxílio mútuo e produção de provas, bem como a implementação de mecanismos de preservação dos elementos probatórios em forma de dados e a celeridade nas investigações e processos penais, por meio da divulgação expedita de dados de tráfego preservados. Tais medidas visam aprimorar a persecução penal no combate à criminalidade informática, antes inexistente (ALMEIDA, 2015).

A elaboração de tratados e convenções internacionais em matéria penal, especialmente relacionados aos crimes virtuais, possibilita a integração entre países com o intuito de elaborar normas eficazes de repressão aos crimes. No entanto, mesmo diante da característica transnacional dos cibercrimes, existem mecanismos legislativos e preventivos nacionais que devem ser aperfeiçoados e aplicados sobre o assunto. No Brasil, existem órgãos especializados no combate aos cibercrimes, como ação conjunta entre o Ministério Público Federal, a Polícia Federal e a Organização não governamental Safernet, que recebem e agilizam denúncias relacionadas aos crimes virtuais. Na esfera estadual, contudo, a realidade é outra, visto que poucas Polícias Civis têm mecanismos especializados em investigação e combate aos crimes virtuais, o que resulta em profissionais despreparados para lidar com os delinquentes (WENDT, 2011).

Diante das dificuldades enfrentadas no âmbito legislativo e na atuação de órgãos especializados, surgem dúvidas acerca do procedimento a ser adotado em casos de cibercrime. A questão sobre como agir e o que fazer quando se é vítima de um delito virtual é frequente no Brasil, bem como as modalidades de prova utilizadas nesses casos, que se apresentam como um obstáculo à obtenção de tutela jurisdicional.

3 ESTELIONATO VIRTUAL

O crime de estelionato virtual é caracterizado pela utilização de equipamentos tecnológicos e acesso à rede de dados, com o intuito de obter vantagem ilícita em proveito próprio ou

alheio, por meio da indução ou manutenção da vítima em erro, mediante a utilização de artifícios fraudulentos (OLIVEIRA, 2020).

Paulo Roberto Silvério Moreira (2022) exemplifica a ocorrência do crime de estelionato virtual ao destacar que os criminosos criam páginas falsas oferecendo oportunidades surreais e enviam mensagens por WhatsApp, enganando as vítimas mais vulneráveis. Essas condutas fraudulentas caracterizam o crime de estelionato virtual, cujos exemplos comuns incluem propostas de empréstimo com taxas de juros baixas ou inexistentes, ofertas de empregos na internet com altos salários, mas com a exigência de pagamento de taxa para inscrição, sites de vendas de produtos inexistentes e mensagens em massa via WhatsApp, conhecidas como correntes. Todas essas condutas têm em comum a busca por obter vantagem patrimonial ilícita, induzindo as pessoas ao erro.

No cenário atual, o estelionato virtual apresenta ampla abrangência e frequência na sociedade, devido à forma como as informações são disseminadas na internet e nas redes sociais, bem como à crença de muitas pessoas nessas informações, seja por equívoco, avidez ou falta de conhecimento seguro sobre o uso adequado da rede.

O crime de estelionato qualificado pelo uso de meio eletrônico ocorre quando há utilização de informações fornecidas pela vítima ou terceiro induzido a erro por meio das redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento ou qualquer outro meio fraudulento análogo. Essa conduta encontra previsão no art. 171, §2º-A do Código Penal. Ademais, o §2º-B do mesmo dispositivo legal prevê aumento de pena de 1/3 a 2/3 na referida modalidade de crime, caso os servidores utilizados para a prática do delito estejam localizados no exterior (MERLIN, 2021).

3.1 CRIMES VIRTUAIS COMETIDOS EM GOIÁS

A partir de março de 2020, com a implantação de diversas medidas de saúde visando conter a disseminação do vírus Covid-19, as transações eletrônicas cresceram de forma exponencial, o que obrigou as pessoas a se adaptarem a novos modos de vida. Apesar de sua concepção original ser pautada na total liberdade, a Internet tem sido o ambiente propício para a prática de inúmeros delitos civis e criminais, os quais potencializam as violações perpetradas, já que têm a capacidade de afetar um grande número de pessoas. (TEIXEIRA, 2020).

Diante disso, torna-se relevante evidenciar o aumento da criminalidade virtual durante a pandemia no Estado de Goiás, em que os periódicos locais destacam a ocorrência de dois

casos de estelionato virtual por semana, totalizando 112 registros ao longo do ano de 2021. Especialistas em segurança cibernética advertem que a prática delituosa tende a crescer em paralelo com a expansão do uso da internet e ressaltam a necessidade imperiosa de a população adotar medidas de proteção contra essa atividade criminosa (O POPULAR, 2022).

Uma das fraudes mais conhecidas que vinha ocorrendo em todo o território brasileiro, e, também em Goiás, consistia na suposta venda de móveis, mediante anúncio de um móvel a um preço bastante atrativo, o que acabava despertando o interesse das pessoas, as quais efetuavam o pagamento por meio do sistema de pagamentos instantâneos conhecido como pix.

Assim como ocorrem tentativas de golpes cibernéticos pelo WhatsApp, também são praticados e efetivados golpes em outras redes sociais que pertencem ao mesmo grupo tecnológico, como é o caso do Instagram. A corretora de imóveis Joana Darc de Oliveira, de 47 anos, foi vítima de um estelionato virtual em maio de 2022. Enquanto utilizava o aplicativo Instagram, o perfil de uma amiga esteticista começou a divulgar uma série de stories anunciando promoções de procedimentos estéticos e a venda de outros objetos, como uma máquina de lavar roupas e um micro-ondas. Joana Darc entrou em contato com a pessoa, que alegou ser a amiga da esteticista, e afirmou que os itens eram de uma funcionária que precisava 13ende-los com urgência. Joana Darc, interessada em adquirir um pacote de procedimentos estéticos e um micro-ondas, acabou sofrendo um prejuízo de R$ 600,00 (seiscentos reais).

Durante a entrevista, o Delegado da Delegacia Estadual de Repressão a Crimes Cibernéticos do Estado de Goiás, Davi Rezende, esclareceu que o crime de estelionato ocorre quando um indivíduo obtém vantagem indevida usando de fraude, caracterizando-se pelo engano e obtenção de algo em prejuízo da vítima. O estelionato digital ocorre quando esse crime é praticado por meio eletrônico, e mesmo virtualmente, os criminosos utilizam da engenharia social para aplicar golpes. Eles se valem dessa técnica para ludibriar pessoas (O POPULAR, 2022).

O delegado da Delegacia Estadual de Repressão a Crimes Cibernéticos, de Goiás, explicou que em caso de vítima de crime cibernético, a primeira medida a ser tomada é a denúncia do delito diretamente na plataforma onde a fraude ocorreu, seja um aplicativo bancário, rede social ou site de compras. Isso porque, quanto maior o número de denúncias, mais rápida e efetiva será a atuação da empresa responsável pela plataforma.

É relevante apresentar alguns dados sobre crimes virtuais em Goiás em 2022: a média diária de golpes virtuais em Goiás é superior a 100, de acordo com informações da Secretaria de Segurança Pública (SSP). Entre janeiro e abril de 2022, foram registrados 12.839 casos. A Polícia Civil afirma que uma das principais formas de prevenir fraudes é habilitar a autenticação

em duas etapas nos aplicativos móveis. Os golpes mais comuns incluem a fraude do novo número, a invasão de contas de redes sociais e a substituição do número de telefone associado a uma conta sem autorização da vítima (G1, 2022).

A prevenção pode ser iniciada pela divulgação de informações para aumentar a conscientização do público pelo Ministério da Ciência e Tecnologia, bem como pelo fornecimento de recursos adequados para os órgãos e autoridades encarregados de combater os crimes mencionados neste trabalho e fortalecer a supervisão dos pais sobre os filhos menores que utilizam a internet por meio dos dispositivos dos pais.

4 ANÁLISE DE CASO CONCRETO

Com base nas informações apresentadas, é possível verificar que o Brasil está suscetível a sofrer ataques de cibercrimes, sendo o phishing (Isso quer dizer a prática de “pescar” as informações e dados secretos dos usuários através de informações falsas ou dados não reais, porém muito atrativos) apontado como um dos mais frequentes após o surgimento da pandemia. A legislação brasileira tem como objetivo combater e regulamentar tais crimes, implementando alterações relevantes no campo da informática. Entretanto, é necessário ressaltar que essas medidas ainda não são suficientes para preencher a lacuna legislativa e inibir a prática desses delitos, que continuam a crescer em número.

Assim sendo, o Direito Digital estabelece uma conexão entre o Direito Positivado e o Direito Consuetudinário, aplicando-se as melhores ferramentas de cada um para solucionar as demandas da sociedade virtual. O ordenamento jurídico brasileiro conta com regulamentações pertinentes ao direito digital, a exemplo do Marco Civil da Internet, da Lei Carolina Dieckman e do Código Penal. Entretanto, devido à constante evolução e dinamismo da internet, é necessário recorrer ao Direito Consuetudinário, aplicado na arbitragem (PINHEIRO, 2021).

Conforme afirmação de Patrícia Peck, o Direito Digital utiliza elementos do Direito Costumeiro, que são a generalidade, a uniformidade, a continuidade, a durabilidade e a notoriedade. Para que tais elementos sejam aplicados no Direito Digital, é necessário considerar o fator temporal. Desse modo, uma das características centrais é a repetição de um comportamento em um número razoável de vezes para evidenciar a existência de uma regra, que serve como base da jurisprudência (PINHEIRO, 2021).

Considerando o cenário de pandemia da Covid-19, que resultou em um significativo aumento de casos de fraudes digitais, notadamente de estelionato virtual, segue abaixo jurisprudência pertinente ao tema:

> PODER JUDICIÁRIO TRIBUNAL DE JUSTIÇA DO ESTADO DA BAHIA Quinta Câmara Cível Processo: AGRAVO DE INSTRUMENTO n. 8030136-91.2021.8.05.0000 Órgão Julgador: Quinta Câmara Cível AGRAVANTE: LEANDRO DA SILVA COIMBRA e outros Advogado(s): JULIANA DA SILVA COIMBRA, VANESSA VILAS BOAS BITTENCOURT DE ANDRADE AGRAVADO: BANCO FICSA S/A. E outros (3) Advogado(s): EMENTA Agravo de Instrumento. Compra e venda de veículo automotor através de plataforma eletrônica. Suposta fraude. Buscam os recorrentes o bloqueio das contas correntes indicadas, na medida em que há indícios de que foram vítimas de suposto golpe, considerando-se a utilização de um perfil falso em plataforma digital de venda de produtos e serviços, onde foi anunciada a venda de veículo automotor para compra por terceiros interessados. Há nos autos prova do pagamento da quantia de R$ 26.000,00, por meio de depósitos bancários (pix e transferência via TED), acompanhado de boletim de ocorrência policial onde os agravantes registraram que não receberam o veículo, sendo, assim, possíveis vítimas de estelionato. Os documentos acostados aos autos, a princípio, demonstraram a probabilidade do direito alegado, bem como o perigo de dano ou o risco ao resultado útil do processo. Diante do poder geral de cautela do juiz, imperativo o boqueio da conta bancária dos agravados, até o limite do valor da transação (R$ 26.000,00), a fim de se salvaguardar o direito dos recorrentes, garantindo-se, assim, o resultado útil da ação principal, acaso julgada procedente, privilegiando a efetividade da justiça. Agravo de Instrumento provido. (Classe: Agravo de Instrumento,Número do Processo: 8030136- 91.2021.8.05.0000, Relator(a): JOSE CICERO LANDIN NETO, Publicado em: 30/08/2022).

O caso em apreço configura o delito de estelionato mediante fraude eletrônica, tipificado no artigo 171, § 2º-A, do Código Penal, em que as vítimas adquiriram um veículo por intermédio de um perfil falso em plataforma eletrônica. Situações como essa tornaram-se recorrentes durante o período de pandemia.

As decisões apresentadas no campo da jurisprudência não são suficientes para a garantia da segurança dos usuários das redes, uma vez que a maioria das penas são mínimas e não possuem um suporte necessário para a tipificação, sendo essencial a elaboração de leis mais modernas e complexas. De acordo com Fabrizio Rosa, não se deve confundir um crime comum praticado pelo uso ou contra o computador de um “crime de informática” propriamente dito. Daí a necessidade de uma legislação específica para esses delitos. Ao formular uma nova categorização, o legislador atrai a atenção da indústria, do mundo acadêmico e do governo para o fato em si, que então se torna objeto de aprofundada reflexão jurídica e técnica (ROSA, 2006).

Ademais, é imprescindível ressaltar que a atualização das leis é insuficiente caso as forças policiais não possuam recursos técnicos adequados para investigar tais delitos, que frequentemente são cometidos de forma anônima, dificultando a identificação da autoria do crime.

CONCLUSÃO

Os benefícios da internet para a sociedade são amplamente conhecidos e reconhecidos, tendo se tornado uma necessidade para a conexão e aprimoramento das atividades diárias. É fato que a internet mudou significativamente a vida das pessoas em diversos aspectos, desde a forma como as pessoas se comunicam até a maneira como realizam suas atividades profissionais e pessoais.

O estudo discutiu algumas das razões que levaram ao aumento da criminalidade na internet, destacando o papel das vítimas ao cederem às tentações expressas pelos criminosos em sua busca por lucro. As pessoas frequentemente se deslumbram com as possibilidades oferecidas pelas novas tecnologias de rede, sem considerar o impacto social significativo no mundo real. Os criminosos exploram a vulnerabilidade das vítimas em ambientes virtuais para exigir valores ou cometer fraudes.

Esta pesquisa confirma que o excesso de entusiasmo e a falta de cautela no uso da internet, juntamente com a falta de conscientização dos usuários sobre os recursos humanos e tecnológicos disponíveis nos setores público e privado, são fatores relevantes que afetam o comportamento dos usuários na internet e podem estar contribuindo para o aumento da criminalidade virtual.

Concomitantemente, as leis, regras e regulamentos são elaborados em uma perspectiva de uma internet benigna, supondo que todos os indivíduos sejam bem-intencionados. No entanto, a forma como a internet vem sendo utilizada, mudou substancialmente, o que tem levado os governos a adotarem medidas mais enérgicas. É imperativo que haja mais pesquisas, ideias, criatividade e tecnologia para combater e prevenir efetivamente esses delitos no futuro.

Por fim, cumpre salientar, em breves termos, o aumento da criminalidade no Estado de Goiás, fornecendo informações com a criação das delegacias especializadas foram importantes para o fortalecimento ao combate a diferentes tipos de crimes em Goiás e garantir a proteção dos direitos das pessoas com deficiência e idosos, além de reforçar a atuação do Estado no combate aos crimes rurais e cibernéticos. sobre as ferramentas de combate e denúncia de tais crimes, bem como os métodos de prevenção, explicando como identificar sites e páginas da web superficiais.

THE CYBER EVOLUTION AND THE LACK OF TIMELY PUNISHMENT OF DIGITAL CRIMES: DIGITAL CRIMES ON THE WHATSAPP PLATFORM

ABSTRACT

Technological advances have made people's lives easier, but also enabled the practice of virtual crimes. Criminal organizations are constantly improving themselves to carry out new scams and illicit practices, using the internet as a tool to hide under the cloak of anonymity. Among the behaviors analyzed by this project, the invasion of a device to obtain, adulterate or destroy data without the owner's authorization and the installation of vulnerabilities to obtain an illicit advantage stand out. Despite the existence of specific legislation, punishment is still ineffective and quick in legal processes. To this end, the principles of legality, legal reserve and analogy to cybercrimes will be analyzed, as well as the laws, doctrines and jurisprudence on virtual crimes, in particular the way criminals act on the "WhatsApp" network in Goiás. It is concluded that there is a lack of specific legislation to deal with conflicts that are growing more and more in the virtual environment, which makes it difficult to punish offenders. The internet is a necessity for connecting and improving daily activities. However, the lack of caution in the use of the internet and the lack of awareness of users about the available resources are factors that affect the development of the internet, whose criminality has increased. It is imperative that there is more research, ideas, creativity and technology to effectively combat and prevent these crimes in the future. Finally, there is an increase in crime in the State of Goiás, with information on combat and prevention tools.

Keywords: Cyber Crimes. Goiás. Technology.

REFERÊNCIAS

ALECRIM, E. **Dez anos de WhatsApp: como o serviço de mensagens conquistou o mundo.** Tecnoblog. Disponível em: https://tecnoblog.net/especiais/whatsapp-dez-anos-historia/. Acesso em: 23 mar. 2023.

ALMEIDA, J.J. Crimes cibernéticos. **Caderno De Graduação - Ciências Humanas E Sociais - UNIT - SERGIPE**, v.2, n.3, p.215–236, 2015.

BRASIL. **LEI Nº 12.735, DE 30 DE NOVEMBRO DE 2012.** Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências.

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.

BRASIL. **LEI Nº 12.965, DE 23 DE ABRIL DE 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

BRASIL. **LEI Nº 14.155, DE 27 DE MAIO DE 2021.** Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato.

BRASIL. **DECRETO-LEI No 2.848, DE 7 DE DEZEMBRO DE 1940.** Código Penal. 2021. Disponível em https://dir.fag.edu.br/index.php/direito/article/view/83. Acesso em: 02 mar. 2023.

BRASIL. **LEI Nº 13.964, DE 24 DE DEZEMBRO DE 2019.** Aperfeiçoa a legislação penal e processual penal. 2021. Disponível em https://dir.fag.edu.br/index.php/direito/article/view/83. Acesso em: 02 mar. 2023.

CÂMARA DOS DEPUTADOS. **CCJ aprova projeto que agrava pena para crimes cibernéticos – notícias.** CCJ aprova projeto que agrava pena para crimes cibernéticos - Notícias. Portal da Câmara dos Deputados. Disponível em: https://www.camara.leg.br/noticias/594044-ccj-aprova-projeto-que-agrava-penapara-crimes-ciberneticos/. Acesso em: 01 mar. 2023.

G1. **Goiás tem mais de 100 golpes pela internet por dia; veja como se proteger.** 2022. Disponível em: https://g1.globo.com/go/goias/noticia/2022/06/03/goias-tem-mais-de100-golpes-pela-internet-por-dia-veja-como-se-proteger.ghtml. Acesso em: 17 fev. 2023.

LORENZO, L.P.; SCARAVELLI, G.P. **Cibercrimes e a legislação brasileira.** 2021. Disponível em https://dir.fag.edu.br/index.php/direito/article/view/83. Acesso em: 02 mar. 2023.

MARQUES, J. **Quem inventou o WhatsApp?** Veja oito curiosidades sobre a história do app. Techtudo. Disponível em: https://www.techtudo.com.br/listas/2019/01/quem-inventou-o-whatsapp-veja-oito-curiosidades-sobre-a-historia-do-app.ghtml. Acesso em: 23 mar. 2023.

MERLIN, L.H. **A nova lei de fraudes eletrônicas: Lei 14.155/21.** 2021. Disponível em: https://juristas.com.br/2021/05/29/a-nova-lei-de-fraudeseletronicas-lei-14-155-21/. Acesso em: 09 fev. 2023.

MOISÉS, C. **Direito internacional penal:** imunidades e anistias. Barueri, SP: Manole, 2012.

MOREIRA, P.R.S. **Estelionato praticado por meio da internet: uma visão acerca dos crimes digitais.** 2022.20 fls. Artigo (Bacharel em Direito). Centro Universitário UMA, 2022.

NUVENS, E. **WhatsApp:** história, dicas e tudo que você precisa saber sobre o app. Olhar Digital. Disponível em: https://olhardigital.com.br/2018/12/20/noticias/whatsapp-historia-dicas-e-tudo-que-voce-precisa-saber-sobre-o-app/. Acesso em: 23 mar. 2023.

OLIVEIRA, H.C. **Cybercrimes: do estelionato virtual.** 2020. 48 fls. Monografia (Bacharel em Direito) Faculdade Evangélica de Rubiataba. Rubiataba, 2020.

O POPULAR. **Goiás registra dois estelionatos virtuais por semana.** 2021. Disponível em: https://opopular.com.br/noticias/cidades/goi%C3%A1s-registra-dois-estelionatos-virtuais-por-semana-1.2484192. Acesso em: 28 fev. 2023.

PINHEIRO, P.P. **Direito digital.** 3 ed, São Paulo: Saraiva, 2009.

PINHEIRO, P.P. **Direito Digital.** 7. ed. rev. atual. e aum. São Paulo: Saraiva, 2021.

ROSA, F. **Crimes de Informática.** 2. ed. Campinas: Bookseller, 2006.

TABOSA, Q.F.; FARIA, E.O. **Terra de ninguém: a (in)efetividade da responsabilização pelos crimes cibernéticos no Brasil.** 2021. Disponível em: https://semanaacademica.org.br/artigo/terra-de-ningueminefetividade-da-responsabilizacao-pelos-crimes-cibernetico s-no-brasil. Acesso em: 03 mar. 2023.

TEIXEIRA, T. **Direito Digital e Processo Eletrônico.** 1 ed. São Paulo: Editora Saraiva, 2020.

VIEIRA, C.G.L. **Crimes cibernéticos o lado obscuro da rede.** 2021. 27fls. Trabalho de Conclusão de Curso (Bacharel em Direito). Pontifícia Universidade Católica de Goiás. Goiânia, 2021.

Wendt, E. **Inteligência cibernética:** da ciberguerra ao cibercrime a (in)segurança virtual no Brasil – livro digital. – São Paulo: Editora Delfos, 2011.

WENDT, E.; JORGE, N.V.H, **Crimes cibernéticos, ameaças e procedimentos de investigação.** 2ª ed. Rio de Janeiro: Brasport, 2013.