PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
ESCOLA DE DIREITO, NEGÓCIOS E COMUNICAÇÃO
NÚCLEO DE PRÁTICA JURÍDICA
COORDENAÇÃO ADJUNTA DE TRABALHO DE CURSO
ARTIGO CIENTÍFICO

CRIMES CIBERNÉTICOS DURANTE A PANDEMIA EM GOIÁS:
AUMENTO DE CASOS DE ESTELIONATO ELETRÔNICO

ORIENTANDA: BEATRIZ MARQUES RODRIGUES DA SILVA

ORIENTADOR: PROF. DR. JOSÉ ANTÔNIO TIETZMANN E SILVA

GOIÂNIA
2022

BEATRIZ MARQUES RODRIGUES DA SILVA

CRIMES CIBERNÉTICOS DURANTE A PANDEMIA EM GOIÁS:
AUMENTO DE CASOS DE ESTELIONATO ELETRÔNICO

Artigo Científico apresentado à disciplina Trabalho de Curso II, da Escola de Direito, Negócios e Comunicação, Curso de Direito, da Pontifícia Universidade Católica de Goiás (PUCGOIÁS).
Prof. Orientador: Dr. José Antônio Tietzmann.

GOIÂNIA
2022

BEATRIZ MARQUES RODRIGUES DA SILVA

CRIMES CIBERNÉTICOS DURANTE A PANDEMIA EM GOIÁS:
AUMENTO DE CASOS DE ESTELIONATO ELETRÔNICO

Data da Defesa: 01/12/2022

BANCA EXAMINADORA

_____
Orientadora: Prof. Dr. José Antônio Tietzmann e Silva. Nota:__

_____
Examinador(a) Convidado(a): Prof.. Nota:_

CRIMES CIBERNÉTICOS DURANTE A PANDEMIA EM GOIÁS:

AUMENTO DE CASOS DE ESTELIONATO ELETRÔNICO

Beatriz Marques Rodrigues da Silva[1]

O presente artigo cientifico discorrerá sobre a importância da proteção de dados e aumentos dos casos de estelionato em Goiás em tempos de grande avanço tecnológico, onde tem o objetivo de abordar a importância da proteção de dados e os aumentos dos casos de estelionato eletrônico em Goiás, durante o isolamento social ocorrido devido a pandemia, respondendo os seguintes problemas: a potencialização do uso dos meios eletrônicos enfraquecem a proteção dos dados pessoais no Estado de Goiás? De fato, há segurança nos sites que pedem esses dados? As leis são suficientes para a punibilidade desses crimes o Estado de Goiás? Será utilizado para a elaboração deste artigo cientifico envolverá: levantamento de dados sobre o aumento de caso; a pesquisa teórica sobre como proteger seus dados para não ficar expostos nos meios eletrônicos; embasamento das leis que criadas para a proteção dos dados pessoais.

Palavras-chave: Crimes Cibernéticos. Goiás. Pandemia. Tecnologia.

[1] Acadêmica de Direito da Pontifícia da Universidade Católica de Goiás, Escola de Direitos e Relações Internacionais, cursando o 9º período.

INTRODUÇÃO

O presente artigo cientifico visa abordar a importância da proteção de dados e aumentos dos casos de estelionato eletrônico em Goiás, devido a facilitação dos crimes que ocorreram em sua grande maioria durante a pandemia.

Durante a pandemia de Covid-19 e período de isolamento social, o uso de computadores, celulares e tablets se intensificaram. O trabalho e estudo de forma remota foi a saída para estabelecer o distanciamento social. De acordo com a Agência Nacional de Telecomunicações (Anatel), o uso da internet no Brasil cresceu durante a quarentena, sendo um aumento entre 40% e 50%. Com o uso tão intensificado dos meios digitais, uma questão atrelada a isso veio à tona: os crimes cibernéticos.

A utilização de meios que facilitem a vida do indivíduo tem se tornado o foco nas relações interpessoais. Tendo em vista, que a agitação cotidiana traz consigo uma grande dificuldade na obtenção de tempo para resolver questões de forma presencial, a utilização da internet tem se tornado a válvula de escape para que se possa cumprir com necessidades básicas da vida civil.

A demanda pela inclusão dos serviços essenciais na internet tem se tornado cada vez mais alta, uma vez que grande parte da população busca otimizar o seu tempo, com intuito de aumentar sua produtividade, bem como o seu tempo livre. É de se notar, que de fato, a digitalização da informação tem se tornado algo essencial nos procedimentos negociais da vida civil.

Destarte, o objetivo deste artigo cientifico é abordar a importância a proteção de dados e os aumentos dos casos de estelionato eletrônico em Goiás, durante o isolamento social ocorrido devido a pandemia, sendo que tentará informar a importância da proteção de dados no meio eletrônico, estudando o aumento de casos que ocorreram durante o isolamento social no Estado de Goiás e levantando legislações atuais regulamentadoras sobre o uso de dados no meio digital.

Buscará responder alguns questionamentos acerca do tema, quais sejam: as potencializações do uso dos meios eletrônicos enfraquecem a proteção dos dados pessoais no Estado de Goiás? De fato, há segurança nos sites que pedem esses dados? As leis são suficientes para a punibilidade desses crimes o Estado de Goiás?

Para a elaboração deste artigo cientifico envolverá: levantamento de dados sobre o aumento de caso; a pesquisa teórica sobre como proteger seus dados para não ficar expostos nos meios eletrônicos; embasamento das leis que criadas para a

proteção dos dados pessoais.

Por fim, o presente artigo cientifico discorrerá sobre a importância da proteção de dados e aumentos dos casos de estelionato em Goiás em tempos de grande avanço tecnológico.

SEÇÃO I – O CRESCIMENTO DAS MÍDIAS DIGITAIS

O estabelecimento do meio digital tem crescido com a movimentação crescente do segmento de streaming de vídeo, a expansão do e-commerce, comnovos sites e Marketplace.

Uma tendência observada, foi que o consumo dos meios de comunicação favoreceu a Mídia Digital, sobretudo os veículos nativosanalógicos que também se fortaleceram no ecossistema digital, em múltiplos formatos.

Por conta disso, o meio teve crescimento expressivo de audiência e atração de verbas publicitárias, reforçando o papel de protagonismo nos últimosanos. Vale lembrar que as lives se tornaram um acontecimento nos primeiros meses das restrições sociais.

E como consequência as empresas anunciantes tiraram proveito do formato, pouco explorado até então, associando suas marcase produtos à artistas engajados na mobilização por doações para entidades e ONGs.

1.1 DADOS SOBRE USO DE TIC'S (TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO) AO LONGO DOS ÚLTIMOS ANOS

A relação entre as TIC's e educação no Brasil é antiga, pois remete a umperíodo anterior a utilização de computadores, tabletes, celulares, etc., tal comoacontece nos dias atuais. Cita-se, por exemplo, que por volta dos anos de 1920,na conhecida Rádio Sociedade do Rio de Janeiro, faziam-se programas de literatura infantil, radiotelegrafia, telefonia de línguas, entre outras atividades; bem como, no início da década de 1970 e em plena ditadura militar (1964- 1985), um programa dito como Projeto Minerva 1 objetivava educar pessoas adultas através das chamadas "aulas por rádio".

Hoje em dia, consta como representativo, o desenvolvimento da tecnologia e da educação para o maior alcance das pessoas, mesmo porque,cerca de 70% da população brasileira possui acesso à internet, esse úmero temaumentado de forma a criar um ambiente cada vez mais propício para a educação à distância.

A população brasileira está cada vez mais conectada. É isso que mostraa Pesquisa Nacional por Amostra de Domicílios (PNAD) de 2019, realizada peloInstituto Brasileiro de Geografia e Estatística (IBGE). De acordo com o levantamento,

82,7% dos domicílios nacionais possuem acesso à internet, um aumento de 3,6 pontos percentuais em relação a 2018.

O levantamento do IBGE mostra também que 12,6 milhões de domicíliosainda não tinham internet. Os motivos apontados foram falta de interesse(32,9%), serviço de acesso caro (26,2%) e o fato de nenhum morador saber usara internet (25,7%).

O Ministério das Comunicações (MCom) desenvolve importantes programas para acabar com o deserto digital do país que atinge mais de 45 milhões de brasileiros. Ações como o Wi-Fi Brasil, Norte Conectado, Nordeste Conectado e Cidades Digitais contribuem para a evolução da conectividade emterritório nacional.

1.2 USO DAS TIC'S E A PANDEMIA

A tecnologia mudou a dinâmica e a cultura da sociedade por causa de sua capacidade de trazer comodidade, sofisticação e conveniência para o dia adia das pessoas. Particularmente através da onipresença da internet smartphones, computadores, tablets, etc. A chamada sociedade da informação está incessantemente ligada as unidades de informação. Embora o uso desses métodos de comunicação tenha se tornado comum, inclusive no ambiente de trabalho incluído no estudo.

Com a pandemia, houve uma exacerbação do uso de plataformas digitais de toda sorte, e-commerce, cursos *online*, *streaming* de vídeo/áudio etc.,o que enfraqueceu a segurança na rede, diante dos grandes números de dadose informações pessoais transitando na rede.

Uma pesquisa recente do *Massachusetts Institute of Technology ("MIT")*publicada no *Journal of Data and Information Quality da ACM (Association for Computing Machinery)* aponta que vazamentos de dados a 493% no Brasil, sendo que mais de 205 milhões de dados de brasileiros vazaram de forma criminosa em 2019. Em número de incidentes relevantes, o país saltou de 3, em2018, para 16 em 2019, de acordo com a pesquisa.

Esses dados contemplam os dois mega vazamentos noticiados recentemente pela empresa de segurança cibernética PSafe, ocorridos noBrasil: um envolvendo 223 milhões de CPFs, contendo dados de pessoas vivase falecidas, como identidades e datas de nascimento, bem como informações de104 milhões de veículos e de 40 milhões de empresas, como CNPJ, razão social,nome fantasia e data de constituição; e outro que revelou informações detalhadas de 140 milhões de pessoas,

como telefone, formação acadêmica, salário, endereços, se a pessoa mudou de cidade e fotos. As informações ficaram expostas durante meses ou anos, e não é possível saber quantas vezesforam compartilhadas e vendidas.

Essas infraestruturas correm risco de ataques de cibernéticos, em que utilizam ferramentas de buscas para encontrar servidores abertos e com dados que possam ser aproveitados. Depois de terem acesso aos dados, eles disponibilizam ou vendem, além de que podem chantagear e extorquir aspróprias companhias que tiveram seus bancos de dados expostos.

Os vazamentos de dados decorrentes de incidentes de segurança e de seu uso ilegal na *deep web* têm se tornado cada vez mais frequentes, principalmente no Brasil, o que deixa cada vez mais vulnerável os usuários dos sites.

1.3 CORRELAÇÃO COM A CRIMINALIDADE

O dado vazado, em sua maioria, faz parte de esquemas de venda dedados para trocas de informação na *deep web* e uso para fins criminosos; inclusive, a Psafe aponta que os criminosos podem usar os dados para vender bens, contrair dívidas, fazer saques indevidos de FGTS e cometer crimes, sem que o prejudicado saiba.

Outro golpe que se tornou bastante frequente foi o do boleto fictício (de internet, telefone, IPVA ou IPTU, por exemplo), que é enviado aos consumidorescom seus CPF, nomes e demais dados, sem que haja qualquer compra ou débitoa ser quitado vinculado ao documento.

Vale destacar que, ainda que o ponto focal da discussão sejam as pessoas físicas lesadas em razão dos vazamentos e como identificar os responsáveis, as empresas são igualmente vítimas dos *hackers*, de forma que sofrem sequestros de dados, *phishing* direcionado, ou *spear phishing*, enavegações de serviço com a geração de milhares de tentativas simultâneas deacesso para invasão do website ou da rede corporativa. Tais eventos impactamnão somente a reputação das empresas, mas também a continuidade dos seusnegócios e a confiança dos consumidores nas marcas.

No passado, para que uma invasão a um site ocorresse, era necessárioque um *hacker* altamente especializado estudasse as infraestruturas digitais a fundo, procurando brechas de segurança antes de conseguir realizar uma invasão. Hoje, costumamos dizer que os *hackers* já não invadem mais os sistemas, eles apenas fazem login.

Com a riqueza de informações que o vazamento proporciona aos criminosos, há a possibilidade de um aumento significativo de golpes mais sofisticados, como os chamados assassinatos de reputação e extorsão de pessoas públicas.

SEÇÃO II – OS CRIMES CIBERNÉTICOS E SEU HISTÓRICO

2.1 HISTÓRICO

Com o avanço das novas tecnologias impulsionando a globalização, a popularidade da Internet proporcionando conveniência aos usuários e a co-circulação de comércio eletrônico, dinheiro e informações, a Internet tornou-se um ambiente atraente para criminosos (TEIXEIRA, 2020).

Há pensamento que o surgimento da sociedade da informação se deu na década de 1970. Uma sociedade derivada da informação, caracterizada pela coexistência dos mundos físico e digital, exige que seus participantes acessem cada vez mais a informação, quebrem fronteiras. Nesse contexto, segundo o pensamento do autor, o surgimento da Internet faz com que as pessoas busquem sempre mais informações em tempo real (PINHEIRO, 2021).

> A informatização crescente das várias atividades desenvolvidas individual ou coletivamente na sociedade veio colocar novos instrumentos nas mãos dos criminosos, cujo alcance ainda não foi corretamente avaliado, pois surgem a cada dia novas modalidades de lesões aos mais variados bens e interesses que incumbe ao Estado tutelar, propiciando a formação de uma criminalidade específica da informática, cuja tendência é aumentar quantitativamente e, qualitativamente, aperfeiçoar os seus métodos de execução (TEIXEIRA, 2020, p. 214)

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

2.2 CONCEITO DE CRIME CIBERNÉTICO PARA O DIREITO

Embora a doutrina enumere várias denominações, as denominações mais comuns são citadas em escritos sobre o assunto, incluindo crime de computador, crime pela Internet, crime de computador, crime pela Internet, crime pelo computador, crime de tecnologia, crime de Internet, crime digital, crime cibernético, crime de

informação, etc. (TEIXEIRA, 2020).

No mais “crime de informática é aquele que, quando praticado, utiliza-se de meios informáticos como instrumento de alcance ao resultado pretendido, [...]” (TEIXEIRA, 2020, p. 214)

Destaca-se:

> Qualquer conduta ilegal, não ética, ou não autorizada que envolva o processamento automático de dados e/ou transmissão de dados. Essa criminalidade apresenta algumas características, entre elas: transnacionalidade (veiculada virtualmente, todos os países têm acesso e fazem o uso da informação), universalidade (é um fenômeno de massa e não de elite) e ubiquidade (está presente nos setores privados e públicos) (LORENZO; SCAVARELLI, 2021, p. 54).

Em geral, o *cybercrime* caracteriza-se pelos meios utilizados para cometer atos ilícitos, ou seja, com o auxílio da Internet dos dispositivos, podendo assim ser realizado em qualquer lugar do país, levando-se em conta que qualquer pessoa pode ser vítima.

2.3 CLASSIFICAÇÃO DOS CRIMES CIBERNÉTICOS

Vale ressaltar que o crime cibernético ou crime eletrônico é de natureza criminosa, com exceção dos crimes cometidos por *hackers*, na forma em que apenas ocorrem em ambiente virtual, pelo qual o crime é corporificado, mas em alguns casos o crime é não encontro. O crime eletrônico assume diferentes formas, dependendo dos bens jurídicos protegidos pela norma. A Internet só surgiu como um facilitador para que questões sobre o conceito de crime e outros termos se apliquem igualmente ao direito penal (PINHEIRO, 2009).

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

Portanto, segundo o pensamento do autor, qualquer conduta descrita no Código Penal, em tese, caracteriza-se como crime virtual se realizada por meio de dispositivo habilitado para internet.

Pode ser classificado como aberto e totalmente cibernético, estes só podem ser praticados por meio de computadores ou outros recursos técnicos que permitem o acesso à Internet, e aqueles recursos técnicos que podem ser praticados de forma tradicional que servem ao acesso à Internet (WENDT; JORGE, 2013).

Tabosa e Faria (2021, p. 12), trazem que: “Crime digital é toda conduta, definida em lei como crime, em que o computador tiver sido utilizado como instrumento de sua perpetração ou consistir em seu objeto material”.

Os crimes cibernéticos podem ser divididos em crimes legítimos e ilegítimos. Posse, quando o ato se destina a atingir o sistema, viola a confiabilidade, integridade ou disponibilidade; inadequado, quando o ato criminoso é considerado generalizado, no sentido de que pode ser realizado com o apoio de mecanismos informatizados, mas pode acontecer por outro lado (VIEIRA, 2021).

SEÇÃO III – A LEGISLAÇÃO BRASILEIRA E SEU REGULAMENTO DOS CRIMES CIBERNÉTICOS

O operador jurídico, em conjunto com o legislador competente, tem discutido amplamente o papel da legalização e investigação dos crimes virtuais no Brasil, com o objetivo de esclarecer e demonstrar os mecanismos existentes de combate a esses crimes com o advento da Internet e das comunicações virtuais.

Outro aspecto relevante é a celeridade do processo penal. Esses programas são um aspecto fundamental para conter o crescimento dessas atividades ilegais na Internet. Dada a importância do tema e a responsabilidade inerente ao poder público de proteger os direitos e garantias fundamentais, a legislação para criminalizar o *cybercrime* e os meios para preveni-lo e reprimi-lo permanecem inadequados. Concluindo, as Leis nº 12.735/12, 12.737/12 e 12.965/14 ainda não são eficazes o suficiente para combater esses crimes de forma eficaz.

O governo federal entende a importância de proteger a sociedade no ciberespaço e publicou a Lei nº 14.155 de 2021 no Diário Oficial da União, aumentando as penas para fraudes, furtos e descaminhos utilizando aparelhos eletrônicos como celulares, computadores e tablets.

Destaca-se o art. 154-A, do Código Penal, uma recém alteração, in verbis:

> 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.

Trata-se de um caso de crime conjunto, existência múltipla, e a tutela jurisdicional pode ser dividida para resguardar a inviolabilidade da intimidade e da vida

privada, além dos dados e informações dos dispositivos (RODRIGUES, 2021).

Ainda para o referido autor, o crime é praticado (crime oficial) no momento da intrusão culposa em equipamento informático, uma vez que se trata de um crime múltiplo em curso, a tentativa é possível, o ato pode ser parcial, e neste caso sob a violação de dados bancários, conforme regras profissionais, não é utilizado o tipo legal de direito penal, mas sim a lei 7.492/86 (RODRIGUES, 2021).

A Lei nº 12.737/12 que criminaliza os crimes de informática e altera o Decreto nº 2.848/40 (Código Penal Brasileiro) em que seu art. 266, §2: “Aplicam-se as penas em dobro se o crime for cometido por ocasião de calamidade pública. ”

Em casos catastróficos como a pandemia de COVID-19, os crimes cometidos por meios informáticos são punidos duas vezes por circunstâncias flagrantes, de acordo com os regulamentos.

Desta forma, o estrito papel da legislação em punir indivíduos que utilizam habilidades e conhecimentos específicos relacionados à tecnologia para criar softwares intrusivos capazes de coletar e divulgar ilegalmente informações em ambientes virtuais, uma alternativa à comunicação pessoal, urgente e necessária profissional, social e politicamente, impulsionado pelas medidas legais de distanciamento, isolamento, uso de máscaras e álcool gel estabelecidas pelo Ministério da Saúde durante a pandemia.

Por outro lado, a Lei nº 12.735/12 regulamenta os atos praticados contra sistemas informatizados e estabelece delegacias especializadas de acordo com o regulamento artístico, vale destacar o art. 4º da respectiva lei “os órgãos da polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado”.

Ainda nesse sentido, o Marco Civil Histórico da Internet na Lei nº 12.965/14, em seu art. 1º destaca: “Esta lei estabelece princípios, garantias, direitos e deveres para o uso da internet no brasil e determina as diretrizes para a atuação da União, Estados, Distrito Federal e Municípios em relação a matéria”.

Com a definição dos direitos e obrigações dos internautas de proteger os dados pessoais e a privacidade do usuário. Dessa forma, a confidencialidade dos dados e informações pessoais presentes no ambiente virtual só poderá ser violada por ordem judicial.

3.1 AS VÍTIMAS DO *CYBERCRIME*

O ano de 2020 foi uma surpresa para o mundo inteiro, com o surgimento do vírus e as mudanças dramáticas que as pessoas fizeram para conter sua disseminação, principalmente o *Home Office* como forma de trabalhar. A Internet é a principal ferramenta que torna este modelo possível.

O grande número de novos usuários e a facilidade de criação de perfis sociais sem a necessidade de grandes quantidades de informações tem contribuído para o aumento do uso de crimes na Internet, onde os criminosos utilizam o pseudo-anonimato fornecido pela Internet para cometer crimes porque não exigir que um agente esteja fisicamente presente para cometer um ato ilegal.

A falsa sensação de disponibilidade de tempo criada por pessoas que ficam em casa por longos períodos de tempo leva os usuários a relaxar as medidas de segurança na Internet, sendo que: “[...] a individualização do usuário cresce, fazendo com que o celular se torne um prolongamento de sua existência no mundo digital” (PINHEIRO, 2009, p. 228).

Com isso, vê-se que para aumentar a segurança dos usuários, é necessária uma autenticação mais confiável. Schneier (2020, p. 45) explica que:

> Associar algo à sua identidade lhe oferece um meio confiável de provar quem você é, e que ninguém mais é você. Isso inclui autenticação, mas também algo mais forte que isso. É possível autenticar uma conta de banco anônima, o que prova que você é a mesma pessoa que depositou dinheiro na semana anterior. Identificar uma conta bancária prova que o dinheiro lhe pertence de acordo com o nome.

Desta forma, de acordo com a linha de pensamento do autor, o celular é atualmente encarado como um dispositivo que confere ao utilizador uma presença no mundo virtual, pelo que o celular está associado ao perfil físico do titular, e através da utilização comprova-se que é o legítimo proprietário.

Nesse caso, para poder utilizar o ambiente virtual de forma tranquila, é necessário utilizar meios de autenticação mais eficazes e senhas mais complexas, como evitar o uso de parentes ou a data de nascimento do próprio usuário, visto que tais informações podem ser facilmente encontradas através das redes sociais, como *facebook* e *instagram*. Quando se trata de crimes de corrupção, o *Whatsapp* e o *Facebook* são, sem dúvida, os mais populares, pois são gratuitos e de fácil acesso (SCHEINER, 2020).

O usuário, como primeira testemunha do crime, tem papel importante nessa

forma de repressão criminal, pois registra ativamente os fatos para comprovar a existência do crime, considerando que a maioria das investigações exigem uma quebra de confidencialidade (PINHEIRO, 2009).

Nesse caso, o Estado não pode interferir na vida privada das pessoas, e as violações de dispositivos constitucionais sobre intimidade e vida privada serão punidas, demonstrando a importância de justificar a medida.

Com a atualização da Lei nº 13.964/19, em especial no artigo 171, §5º do Código Penal, atos fraudulentos cometidos por meio da Internet, a ação passa a depender do representante das pessoas ofendidas, mas nas circunstâncias mencionadas em seu projeto, a conduta será pública, tornando mais visível o papel das vítimas nas investigações criminais, como um dos principais interessados.

Além disso, é importante destacar a seguinte lição:

> Para o Direito Digital, IP constitui uma forma de identificação virtual. Isso significa que o anonimato na rede é relativo, assim como muitas identidades virtuais podem não ter um correspondente de identidade real. Como analogia, é o mesmo que ocorre quanto a contas e empresas fantasmas, cuja identidade física pode ser falsa. Esta na rede, devido a sua dimensão e caráter globalizado, faz com que a facilidade para “criar laranjas” seja ainda maior.

Normalmente, todas as visitas ao site são registradas, inclusive no histórico do dispositivo utilizado para a visita. O registro contém pelo menos o endereço IP de origem e a hora em que o acesso foi realizado.

Diante disso, o acesso aos dados de conexão torna-se fundamental na identificação dos responsáveis pelos crimes cometidos pela Internet, pois os criminosos podem facilmente cometer crimes de qualquer lugar do país e o crime se espalha muito rapidamente pelo país e, portanto, ainda mais, eles não precisam estar fisicamente presentes para cometer o crime, ainda mais porque é difícil localizá-los em redes abertas de internet.

3.2 A ENGENHARIA SOCIAL NECESSÁRIA PARA OS CRIMINOSOS DO *CYBERCRIME*

De antemão, ressalta-se:

> Engenharia social é a utilização de um conjunto de técnicas destinadas a ludibriar a vítima, de forma que ela acredite nas informações prestadas e se convença a fornecer dados pessoais nos quais o criminoso tenha interesse

> ou a executar alguma tarefa e/ou aplicativo (WENDT; EMERSON, 2013, p. 21)

Segundo os autores, a engenharia social aplicada ao crime por meio virtual, cuja principal função é obter informações sensíveis das vítimas, estimular sua curiosidade por meio de meios de fácil acesso e ameaçar perder uma oportunidade imaginária de alto lucro. A principal técnica utilizada pelos engenheiros sociais é baseada na manipulação das emoções do “alvo”. Como tal, eles trabalham principalmente por medo, ganância, compaixão e, finalmente, curiosidade (WENDT, EMERSON, 2013).

Ainda seguindo a linha de pensamento do autor, ensinam os criminosos a se passarem por empresa, banco ou instituição pública para dar um golpe de estado a fim de aumentar a credibilidade da ação, a fim de incentivar os usuários a confiar na operação, em vez de do que tomar as precauções usuais, uma ação conhecida como Ancoragem (WENDT, EMERSON, 2013).

Ainda assim:

> [...], a fraude eletrônica consiste em uma mensagem não solicitada que se passa por comunicação de uma instituição conhecida, como um banco, empresa ou site popular, e procura induzir usuários ao fornecimento de dados pessoais e financeiros. inicialmente, esse tipo de mensagem induzia o usuário ao acesso a páginas fraudulentas na Internet. Atualmente, o termo também se refere à mensagem que induz o usuário à instalação de códigos maliciosos, além da mensagem que, no próprio conteúdo, apresenta formulários para preenchimento e envio de dados pessoais.

A fraude por meio de aplicativos de *phishing scam* é uma das formas pelas quais os criminosos tentam obter dados pessoais e financeiros das vítimas combinando meios técnicos e engenharia social, também cita algumas das formas mais comuns de tentativas, à ocorrência de fraudes, das quais vale destacar que o envio de mensagens via *SMS*, atualmente *Whatsapp*, sugerindo a instalação de ferramentas ou atualização do aplicativo é o mais comum.

Uma boa estratégia para evitar ser vítima desses comportamentos é verificar se há erros gramaticais no corpo da mensagem, e também recomendam usar o mouse para verificar a página de endereço real, na barra de *status*, porque às vezes o usuário verifica que possui um *link* na mensagem e ao clicar é direcionado para um destino diferente, com isso:

> A maioria desses golpes funciona porque as vítimas acreditam que se trata de algo verdadeiro e, então, entregam aos criminosos suas informações com

> mais facilidade. O principal objetivo do criminoso, nesse caso, é convencer a vítima a entregar suas informações voluntariamente em vez de usar ameaças ou intimidação forçada (PEREIRA, 2021, p. 18).

Nesse sentido, observou-se que os usuários são diligentes no uso da Internet, lembrando que os cuidados que se aplicam ao mundo real também se aplicam ao mundo virtual, por isso é necessário estar atento aos riscos do usuário no ambiente virtual (WENDT; EMERSON, 2013).

Durante a pandemia de covid-19 e adaptando-se às atividades remotas, os usuários ficam mais tempo expostos à Internet e, portanto, ao uso das redes sociais, onde são bombardeados com propagandas e informações injustificadas de todas as direções, e que, por pensarem nisso como uma teia de confiança que acabou caindo em um golpe. Assevera-se que:

> Ao navegar na internet é preciso ficar atento aos links onde clica os arquivos que baixa e sites onde irá cadastrar suas informações pessoais ou bancárias. Isso porque existem diferentes crimes virtuais sendo aplicados por criminosos que buscam obter vantagens à custa das vítimas desatentas. O importante é o entendimento de que em todos os golpes já aplicados o problema foi acarretado por descuidos com a segurança, como pouco cuidado nos sites acessados, ou falta de malícia para identificar falsas informações, promoções ou ofertas de emprego irrealistas (PEREIRA, 2021, p. 18).

Para resumir, os engenheiros sociais simplesmente se beneficiam da ingenuidade das pessoas e da crença de que o que acontece na Internet não pode se refletir fortemente na realidade, aproveitando os momentos de crise financeira e classes sociais específicas para menos orientação e educação. O objetivo é conscientizar e orientar as pessoas no uso de métodos de defesa contra esses comportamentos.

SEÇÃO IV – O CRESCIMENTO DOS CRIMES VIRTUAIS DURANTE A PANDEMIA NO ESTADO DE GOIÁS

Com várias medidas de saúde em vigor para conter a propagação do vírus Covid-19, as transações eletrônicas cresceram exponencialmente, levando as pessoas a se adaptarem a novos estilos de vida. Em seu conceito original de liberdade total, a Internet tem sido a arena para o cometimento de vários crimes civis e criminais, que reforçam as violações pelo potencial de atingir um número muito grande de pessoas (TEIXEIRA, 2020).

Com isso é importante demonstrar o aumento da criminalidade virtual durante

a pandemia no Estado de Goiás, onde os jornais evidenciaram que:

> Goiás registra dois estelionatos virtuais por semana, foram 112 ocorrencias ao longo de todo o ano de 2021, especialistas dizem que a pratica do crime cresce junto com o avanço da internet e alertam a importância da proteção (...) Especialistas argumentam que a pratica do crime deve continuar aumentando com o avanço do uso da internet no cotidiano das pessoas e alertam para a importância de a população se proteger contra este tipo de atividade criminosa (...) (OPOPULAR, 2022, *online*).

Um dos golpes mais famosos que estava ocorrendo em todo o Brasil, era a, suposta, venda de móveis, onde se anunciava um móvel por um valor bastante atrativo e que fazia com que as pessoas se interessassem, fazendo então um pagamento por meio do pix.

> A corretora de imóveis Joana Darc de Oliveira, de 47 anos, foi vítima de um estelionato virtual em maio deste ano. Ela estava usando o aplicativo do Instagram quando o perfil de uma amiga que é esteticista começou a publicar uma série de *stories* anunciando promoções de procedimentos estéticos e também a venda de outros objetos como, por exemplo, uma máquina de lavar roupas e um micro-ondas.
> "Na hora achei que era um bom negócio e chamei ela no chat. A pessoa conversou comigo como se fosse ela e disse que os itens eram de uma funcionária que estava se separando e precisava vender tudo com urgência"
> A intenção de Joana Darc era adquirir um pacote de procedimentos estéticos e um micro-ondas. Entretanto, ela acabou ficando apenas com um prejuízo de R$ 600,00 (seiscentos reais) (OPOPULAR, 2022, *online*).

Durante a entrevista, o delegado da Delegacia Estadual de Repressão a Crimes Cibernéticos, de Goiás, Davi Rezende, esclareceu que:

> O crime de estelionato é quando um indivíduo obtém alguma vantagem indevida usando de fraude, é aquela máxima: eu te engano e você me entrega algo. O estelionato digital é quando este crime acontece por meio eletrônico (...) mesmo virtualmente, eles usam da engenharia social para poder aplicar esses golpes. Eles se utilizam sempre dessa técnica de ludibriar pessoas (OPOPULAR, 2022, *online*).

O delegado ainda explicou que se a pessoa for vítima, a primeira coisa a fazer é denunciar o crime na própria plataforma, seja um aplicativo bancário, uma rede social ou um site de compras. Quanto mais pessoas denunciarem, mais rápido a empresa agirá (OPOPULAR, 2022)

É importante trazer alguns números dos golpes por meio da internet em Goiás em 2022:

> Goiás tem, em média, mais de 100 golpes pela internet por dia, segundo

> dados da Secretaria de Segurança Pública (SSP). De janeiro a abril de 2022, foram 12.839 casos registrados. A Polícia Civil diz que um dos principais meios de evitar fraudes é adicionar a verificação em duas etapas nos aplicativos do celular. (...)os golpes mais aplicados são o do novo número, a invasão de contas de redes sociais e a troca do número de telefone para outro chip sem autorização das vítimas (G1, 2022, *online*).

A prevenção pode começar com a divulgação de informações para aumentar a conscientização do Ministério da Ciência e Tecnologia, para melhor equipar os órgãos e autoridades responsáveis pelo combate aos crimes mencionados neste trabalho, e fortalecer a fiscalização dos pais de filhos menores, quando eles estão usando a rede no dispositivo de seus pais.

CONCLUSÃO

Os benefícios da Internet para a sociedade foram e continuarão a ser enormes. Ela mudou a vida das pessoas de inúmeras maneiras e agora as pessoas não conseguem imaginar a vida sem ela e a conexão se tornou uma necessidade.

Dadas as restrições financeiras e a dificuldade de encontrar autores conhecidos sobre o tema, a pesquisa limitou-se a bibliografias, documentos, leis esparsas etc., o que resultou em um escopo de pesquisa pequeno.

São discutidas algumas das razões para o aumento da criminalidade, enfatizando o papel das vítimas em cair nas tentações expressas pelos criminosos por sua ganância de lucro. As pessoas ficam fascinadas com as capacidades dessas novas tecnologias de rede, ignorando o profundo impacto social no mundo real. Os criminosos exploram a vulnerabilidade das vítimas em ambientes virtuais para exigir valor ou cometer fraudes.

Este estudo confirma que a falta de entusiasmo e cautela no uso da Internet, juntamente com a falta de conscientização dos usuários sobre os recursos humanos e tecnológicos nos setores público e privado, é um dos fatores marcantes que afetam o desenvolvimento da Internet, onde a criminalidade só aumentou.

Ao mesmo tempo, leis, regras e regulamentos são construídos em uma internet benigna, supondo que todos sejam bem-intencionados. Mas a natureza da internet mudou, levando os governos a agir. Deve haver mais pesquisas, mais ideias, mais criatividade e mais tecnologia para combater e prevenir efetivamente esses crimes no futuro.

Por fim, é feito um breve acréscimo ao crescimento da criminalidade em Goiás para informar ferramentas de combate e denunciar tal crime e métodos de prevenção, explicando como identificar sites e páginas da web superficiais.

REFERÊNCIAS

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.

BRASIL, LEI Nº 13.964, DE 24 DE DEZEMBRO DE 2019. Aperfeiçoa a legislação penal e processual penal.

CASA CIVIL. 90% dos lares brasileiros já tem acesso à internet no Brasil, aponta pesquisa. Disponível em: https://www.gov.br/casacivil/pt-br/assuntos/noticias-2022/setembro/90-dos-lares-brasileiros-ja-tem-acesso-a-internet-no-brasil-aponta-pesquisa#:~:text=Em%202021%2C%20o%20n%C3%BAmero%20de,mais%20do%20que%20em%202019. Acesso em: 06 mai. 2022.

CNN BRASIL. Fotos e até salários estão entre os dados vazados de 223 milhões de brasileiros. Disponível em: https://www.cnnbrasil.com.br/business/fotos-e-ate-salarios-estao-entre-os-dados-vazados-de-223-milhoes-de-brasileiros/. Acesso em: 06 mai. 2022.

DEMELLO, Marco. Cibersegurança para empresas: o fator humano como falha de proteção. Disponível em: https://www.psafe.com/blog/ciberseguranca-para-empresas-o-fator-humano-como-falha-de-protecao/. Acesso em: 06 mai. 2022.

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

IBGE. Uso de internet, televisão e celular no Brasil. Disponível em: https://educa.ibge.gov.br/jovens/materias-especiais/20787-uso-de-internet-televisao-e-celular-no-brasil.html. Acesso em: 06 mai. 2022.

LORENZO, Larissa Papandreus; SCARAVELLI, Gabriela Piva. CIBERCRIMES E A LEGISLAÇÃO BRASILEIRA. Disponível em https://dir.fag.edu.br/index.php/direito/article/view/83. Acesso em : 02 set. 2022.

OPOPULAR. Goiás registra dois estelionatos virtuais por semana. Disponível em: https://opopular.com.br/noticias/cidades/goi%C3%A1s-registra-dois-estelionatos-virtuais-por-semana-1.2484192. Acesso em: 17 set. 2022.

PEREIRA, Deocley Pedrada. Crimes cibernéticos: pequenos passos na prevenção de fraudes por meio de dispositivos móveis. 2021. 31f. Trabalho de Conclusão de Curso (Tecnologia em Redes de Computadores) – Instituto Federal do Amapá, Macapá, AP, 2021.

PINHEIRO, Patricia Peck. Direito digital, 3 ed, São Paulo: Saraiva, 2009.

Rodrigues, Cristiano, Manual de direito penal. 2. ed. São Paulo: Editora Foco, 2021.

SCHEINER, B. Crimes na internet. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788550808871/. Acesso em: 07 set. 2022.

SCHMIDT, Guilherme. Crimes cibernéticos. Jusbrasil, 2014. Disponível em: http://gschmidtadv.jusbrasil.com.br/artigos/149726370/crimes-ciberneticos>. Acesso em: 02 set. 2022.

TABOSA, Queving Fontenele; FARIA, Emerson Oliveira. TERRA DE NINGUÉM: A (IN)EFETIVIDADE DA RESPONSABILIZAÇÃO PELOS CRIMES CIBERNÉTICOS NO BRASIL. Disponível em: https://semanaacademica.org.br/artigo/terra-de-ninguemineefetividade-da-responsabilizacao-pelos-crimes-ciberneticos-no-brasil. Acesso em: 02 set. 2022.

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

VIEIRA, Cláudio Guimarães Lima. CRIMES CIBERNÉTICOS O LADO OBSCURO DA REDE. Disponível em: https://repositorio.pucgoias.edu.br/jspui/handle/123456789/2419. Acesso em: 02 set. 2022.

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