FACULDADES INTEGRADAS RUI BARBOSA – FIRB
UNIVERSIDADE BRASIL

MARCOS FAUSTINO CALIRI

BREVE ANÁLISE DO CRIME DE ESTELIONATO COMETIDO POR MEIO ELETRÔNICO NO CONTEXTO DAS VÍTIMAS BENEFICIÁRIAS DO AUXÍLIO BRASIL

Andradina – SP
Junho/2023

MARCOS FAUSTINO CALIRI

BREVE ANÁLISE DO CRIME DE ESTELIONATO COMETIDO POR MEIO ELETRÔNICO NO CONTEXTO DAS VÍTIMAS BENEFICIÁRIAS DO AUXÍLIO BRASIL

Trabalho de Conclusão de Curso apresentado nas Faculdades Integradas Rui Barbosa – FIRB, sob orientação do Professor Especialista Diego da Silva Santos como requisito parcial para obtenção do título de bacharel em Direito.

Andradina – SP
Junho/2023

MARCOS FAUSTINO CALIRI

BREVE ANÁLISE DO CRIME DE ESTELIONATO COMETIDO POR MEIO ELETRÔNICO NO CONTEXTO DAS VÍTIMAS BENEFICIÁRIAS DO AUXÍLIO BRASIL

Trabalho de Conclusão de Curso apresentado à banca examinadora como requisito parcial para obtenção do Bacharelado em Direito nas Faculdades Integradas Rui Barbosa – FIRB. Defendido e aprovado em ___ de _____ de 2023 pela banca examinadora constituída por:

Prof(a). MSc. _____
Instituição: Faculdades Integradas Rui Barbosa - FIRB

Prof(a). MSc. _____
Instituição: Faculdades Integradas Rui Barbosa - FIRB

Prof(a). MSc. _____
Instituição: Faculdades Integradas Rui Barbosa – FIRB

NOTA: ( ) Aprovado ( ) Reprovado

Andradina, ___ de _____ de 2023

DEDICATÓRIA

"Dedico esta monografia à memória da minha amada mãe, Lucília, cujo amor incondicional e apoio constante foram fundamentais em minha jornada acadêmica. Sua presença permanece viva em meu coração e suas palavras de encorajamento ecoam em minha mente.

Ao meu pai, Apparecido, agradeço por seu incansável suporte e exemplo de determinação. Sua sabedoria, paciência e sacrifícios não passaram despercebidos e foram a base que me sustentou durante todo esse percurso. Seu sonho de me ver formado me deu força em cada dificuldade que encontrei e superei.

E, por fim, dedico este trabalho à minha querida esposa, Andreia, que sempre esteve ao meu lado, apoiando-me incondicionalmente. Seu amor, compreensão e incentivo foram essenciais para superar os desafios e alcançar esta conquista. Sua presença trouxe alegria e equilíbrio à minha vida, e sou grato por tê-la ao meu lado.

A todos vocês, mãe, pai e esposa, dedico esta monografia com profundo carinho e gratidão."

AGRADECIMENTOS

Em primeiro lugar, a Deus, que permitiu e me guiou para que meus objetivos fossem alcançados, durante a realização dos estudos para a produção deste trabalho, bem como, em todos os momentos de estudo neste curso.

À minha Mãe Lucília (*in memoriam*) e meu Pai Apparecido que sonharam comigo esse sonho de me ver formado, e me deram todo o apoio e incentivo, que foram determinantes em minha vida.

À minha esposa Andréia, que lutou, estudou comigo, me incentivou e apoiou, e que com paciência compreendeu todas as minhas ausências

As minhas irmãs, sobrinhos, cunhados, e a todos os familiares e amigos, por todo o apoio, ajuda, incentivo e compreensão, que muito contribuíram para a realização de alcançar este sonho.

Ao meu professor e orientador Diego da Silva Santos, por ter me orientado com tamanha presteza, me concedendo seu tempo e conhecimento de forma tão dedicada e amiga.

A todos que participaram, direta ou indiretamente do desenvolvimento deste trabalho, enriquecendo o meu aprendizado.

Por fim, agradeço as Faculdades Integradas Rui Barbosa – Firb e Universidade Brasil, na pessoa da Coordenadora do Curso de Direito, Professora Larissa Komuro e a todo seu corpo docente, que estiveram comigo no trilhar deste caminho da minha formação acadêmica, sendo mais que professores e professoras, todos vocês foram amigos e apoiadores, guardarei para sempre em meu coração cada um de vocês.

Epígrafe

Corra, porém, o juízo como as águas, e a justiça como o ribeiro impetuoso. Amós 5:24 ACF.

Na era digital, as ameaças podem se esconder por trás de um clique, e a segurança depende da nossa capacidade de entender e antecipar os riscos que enfrentamos. Marc Goodman

RESUMO

CALIRI, M F. **Breve análise do crime de estelionato cometido por meio eletrônico no contexto das vítimas beneficiárias do Auxílio Brasil.** Trabalho de Conclusão de Curso (Graduação em Direito). Faculdades Integradas Rui Barbosa – FIRB, 2023.

A crescente utilização da internet trouxe grandes benefícios para as demandas contemporâneas, por outra perspectiva houve a expansão da criminalidade no ambiente virtual. Desta maneira, o presente trabalho aborda os crimes cometidos virtualmente, o ordenamento jurídico a respeito desses crimes e por fim uma análise de um golpe praticado sobre o benefício do Governo Federal – Auxílio Brasil. Serão Analisados os aspectos jurídicos dos crimes virtuais, destacando a Lei 12.737/2012 – Lei Carolina Dieckmann, a Lei 12.965 – Marco Civil da Internet e a Lei 13.709/18 – Lei Geral de Proteção de Dados. Desta forma, o presente trabalho tem como objetivo elencar as leis atualmente em vigor no Brasil, e também uma lista dos principais crimes virtuais, mais comumente cometidos na internet em nosso país. Em um segundo momento, serão abordados alguns crimes de internet especificamente, com detalhamento do crime e jurisprudência a respeito. Ao final do trabalho, será apresentado um estudo de como criminosos virtuais aplicam golpes para capturar dados dos cidadãos, para posteriormente solicitar em nome do cidadão o benefício do Auxílio Brasil do Governo Federal. Assim, verifica-se que normas estudadas, criadas especificamente para a proteção das pessoas, na sociedade, no que tange ao campo da internet trata-se de um bom primeiro passo, para o cumprimento desse objetivo, mas estas normas somente serão eficazes se conseguirem manter-se atuais frente ao constante desenvolvimento tecnológico.

Palavras-chave: Crimes cibernéticos. Crimes virtuais. Lei Geral de Proteção de Dados.

ABSTRACT

CALIRI, M F. **Breve análise do crime de estelionato cometido por meio eletrônico no contexto das vítimas beneficiárias do Auxílio Brasil.** Trabalho de Conclusão de Curso (Graduação em Direito). Faculdades Integradas Rui Barbosa – FIRB, 2023.

The increasing use of the internet has brought significant benefits to contemporary demands. However, from another perspective, it has also led to the expansion of cybercrime. Thus, this present work addresses crimes committed virtually, the legal framework regarding these crimes, and finally, an analysis of a scam perpetrated concerning the Federal Government's program - Auxílio Brasil. We will analyze the legal aspects of cybercrimes, focusing on Law 12.737/2012 - the Carolina Dieckmann Law, Law 12.965 - the Internet Civil Rights Framework, and Law 13.709/18 - the General Data Protection Law. Therefore, the objective of this work is to list the currently effective laws in Brazil, as well as a list of the main cybercrimes commonly committed on the internet in our country. In a second part, we delve into specific internet crimes, providing details of the crimes and relevant case law. At the end of the study, we present an analysis of how cybercriminals employ scams to obtain citizens' data and subsequently apply for the Auxílio Brasil program on behalf of the citizens. Thus, it is evident that the studied regulations, specifically created for the protection of individuals in society concerning the internet field, represent a good first step towards achieving this goal. However, these regulations will only be effective if they can remain up-to-date in the face of constant technological developments.

Keywords: Cybercrimes, Virtual crimes, General Data Protection Law.

LISTA DE FIGURAS

SUMÁRIO

1 INTRODUÇÃO

O presente trabalho analisará a Lei 12.737/12 conhecida como “Lei Carolina Dieckmann”, a Lei 12.965/14 oficialmente chamada de Marco Civil da Internet, a importância da Lei 13.709/18 – Lei Geral de Proteção de Dados, trazendo o entendimento dos tribunais sobre os meios de barrar as condutas criminosas, identificar e punir os infratores dos delitos cometidos no ambiente virtual, e por fim um estudo sobre como criminosos virtuais aplicam um golpe no cidadão fraudando o benefício do Governo Federal Auxílio Brasil.

Apesar dos problemas gerados pela dependência tecnológica, vale ressaltar que grande parte da população mundial utiliza a internet para realizar tarefas diárias, em seu trabalho, casa e estudos. Tendo isso em vista, criminosos virtuais aproveitam-se de falhas em sistemas e utilizam-se artimanhas para cometer crimes fraudando e prejudicando a sociedade de diversas maneiras, cometendo atos ilícitos denominados como crimes virtuais.

Sendo uma das primeiras, a lei ordinária 12.735/2012 e a lei 12.737/2012, que ficou popularmente conhecida como “Lei Carolina Dieckman”, criada após o vazamento de fotos pessoais da referida atriz, de seu computador pessoal, invadido por hackers, com posterior cobrança de dinheiro para que os criminosos não divulgassem as fotos na internet.

O caso ganhou ampla repercussão na mídia e levantou questões sobre segurança digital, privacidade e legislação relacionada a crimes cibernéticos. Na época, a legislação brasileira não possuía dispositivos específicos para lidar com esses tipos de crimes. O caso Carolina Dieckmann foi um dos eventos que contribuíram para a aprovação da Lei 12.737/2012, também conhecida como "Lei Carolina Dieckmann", que criminaliza atividades como invasão de dispositivos eletrônicos e divulgação não autorizada de informações.

No entanto, apesar da criação das referidas leis, muitas são as dificuldades enfrentadas pelos investigadores e operadores do direito responsável pela persecução penal, assim, de fato, há necessidade de uma melhor formação dos profissionais atuantes nessa área.

Considerando todos os fatos mencionados é de praxe que apesar da norma jurídica brasileira ter avançado nos últimos anos, ainda se faz necessário o avanço da capacitação dos profissionais, a constante atualização das leis concernentes ao

desenvolvimento da tecnologia e o consequente acompanhamento da legislação para o surgimento de novas ameaças virtuais, tudo isso na busca de uma evolução das penalidades no cenário virtual.

Da mesma forma, será abordada também a Lei Geral de Proteção de Dados LGPD (Lei nº 13.709/18), sua origem, evolução, características e aplicação, dentre outros aspectos, no território brasileiro.

O embasamento teórico deste trabalho está amparado, sobretudo, em leis referentes ao tema: Lei de Acesso à Informação (Lei nº 12.527/2011); o Art.º 5 da Constituição Federal, que se refere ao Direito à Privacidade, e o Marco Civil da Internet (Lei nº 12.965/ 14), as quais serão explicadas brevemente, considerando os seus aspectos jurídicos e sua influência no campo da Ciência da Informação.

Sendo assim, serão discutidas as características e as aplicações das Leis referentes ao combate aos crimes digitais.

Por fim, se fará um estudo sobre a aplicação, cada vez mais crescente, de um golpe, disseminado por vias digitais, principalmente por redes sociais, que consiste de alguma forma acessar os dados pessoais dos cidadãos para requerer fraudulentamente benefícios assistências de programas do Governo Federal, em especial o benefício Auxílio Brasil.

Para alcançar tais resultados, será necessária a leitura das principais legislações que existem atualmente, e também pesquisar quais foram os motivos impulsionadores para a criação de tais leis.

2. DISCUSSÃO TEÓRICA

2.1 - CRIMES VIRTUAIS

Ao longo dos anos e da evolução da tecnologia digital, tornou-se necessário criar e publicar normas jurídicas com a finalidade expressa de regular o comportamento dos usuários que utilizam a Internet.

Nesse sentido, é necessário conhecer as disposições da lei e tomar alguns cuidados, para não ser a futura vítima desses crimes.

Em geral, os crimes cibernéticos mais comuns cometidos no ciberespaço são os crimes sexuais e os crimes contra a honra. Isso refere-se aos crimes de, por exemplo, calúnia e difamação. Além disso, as fraudes e outras práticas fraudulentas têm aumentado nos últimos tempos, com o objetivo de enganar as vítimas e obter dados para requerer benefícios financeiros ilegalmente.

2.2 - O CONCEITO DE CRIME VIRTUAL

O crime cibernético envolve um ato intencional cometido em um ambiente virtual, tendo como principal ferramenta de ataque o uso de um computador ou rede de computadores com conexão à Internet, ou ainda, a outros tipos de dispositivos eletrônicos como celulares smartphones. Os crimes cibernéticos também são chamados de crimes informáticos e crimes digitais ou crimes virtuais. Todas essas palavras se referem ao mesmo problema.

Aldemario Araújo Castro conceitua os crimes virtuais:

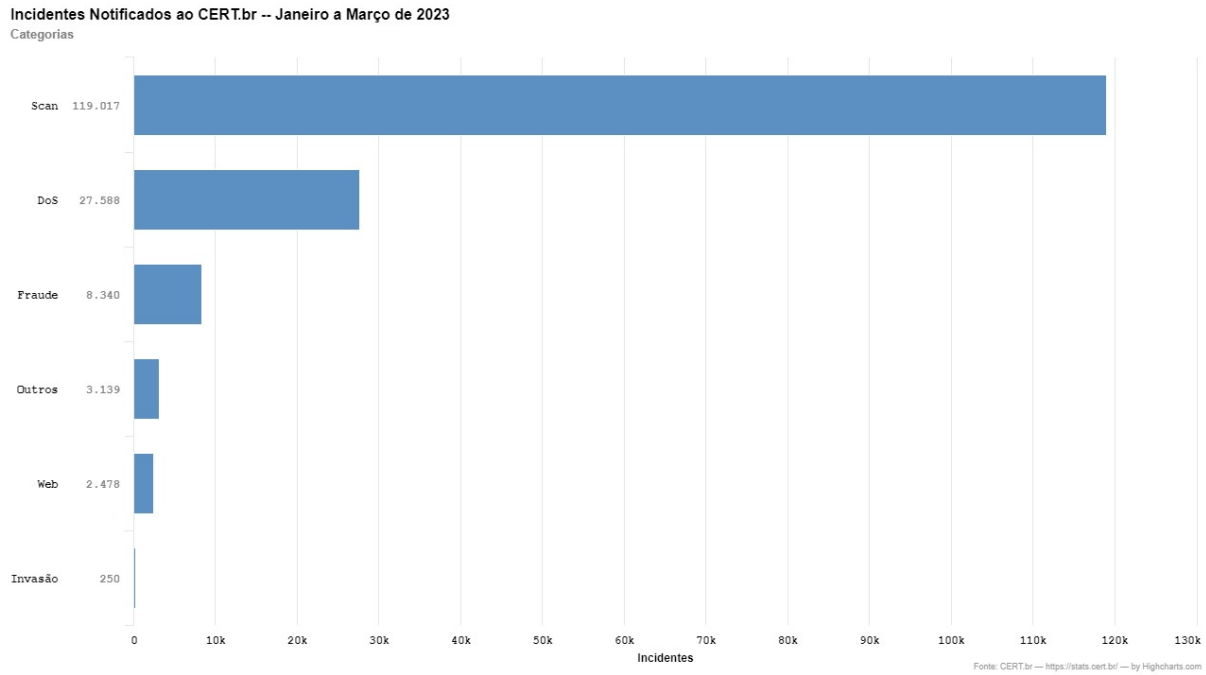
> [...] são denominados de "crimes de informática" as condutas descritas em tipos penais realizadas através de computadores ou voltadas contra computadores, sistemas de informática ou os dados e as informações neles utilizados (armazenados ou processados). (CASTRO, 2003, p.1).

Alessandro Gonçalves Barreto também conceitua crimes virtuais da seguinte forma:

> Os crimes tecnológicos são aqueles que envolvem o uso de tecnologias (computador, internet, caixas eletrônicos), sendo, em regra, crimes meios — ou seja, apenas a forma em que são praticados é que é inovadora. Têm como subespécie os crimes virtuais, informáticos ou cibernéticos (praticados pela internet), onde, apesar de se concretizarem em ambientes virtuais, os delitos trazem efeitos no mundo real. (BARRETO, 2016).

É cada vez mais comum ser noticiado na mídia de casos que nos levam a concluir que a prática desse tipo de crime aumentou significativamente nos últimos anos, principalmente devido ao desenvolvimento da Internet, com o uso contínuo das redes sociais. Como resultado, houve um aumento na prática de crimes contra o patrimônio dos usuários, como se pode verificar na figura a seguir, obtida do site https://stats.cert.br/incidentes/, que é um site da internet que reúne informações sobre ataques virtuais, estatísticas de notificações recebidas pelo CERT.br, relativas a incidentes reportados, entre outros, por CSIRTs, administradores de redes e usuários de Internet.

Figura 1 - Notificações de Ataques cibernéticos



Fonte: CERT.br/NIC.br - https://stats.cert.br/

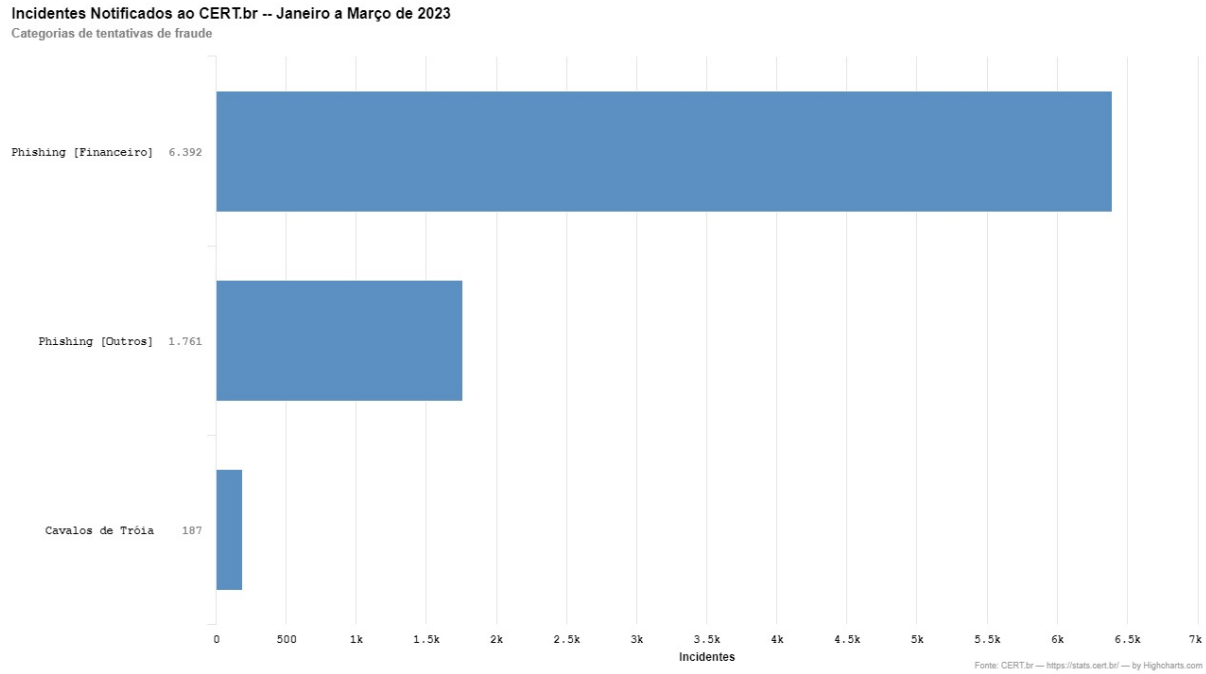
O Gráfico acima traz em números a quantidade de ataques cibernéticos notificados ao site em referência, onde pode-se verificar que foram mais 119 mil ataques do tipo *SCAN* que são do tipo varredura por vulnerabilidades, mais de 27 mil ataques do tipo *DOS* que são ataques a sites para tentativa de derrubar sites, mais de 8 mil ataques do tipo fraude para roubo de dados do usuário, mais de 3 mil ataques de outros tipos não especificados, mais de 2 mil ataques do tipo *web,* e por fim 250 ataques de invasão a computadores de usuários, isto no período de janeiro a março de 2023.

Em especial, observa-se que os ataques do tipo fraude ocupam o terceiro lugar na classificação acima, ataques estes que são a base para o cometimento dos crimes a que este trabalho se refere.

Estas notificações são voluntárias e refletem os incidentes ocorridos em redes que espontaneamente os notificaram ao CERT.br, mostrando a evolução de casos de ataques cibernéticos, conforme figura demonstrativa a seguir.

Neste portal estão disponíveis diversas estatísticas relacionadas com incidentes de segurança na Internet, sistemas mal configurados passíveis de serem abusados, ataques vistos em sensores (*honeypots*) e reclamações de *spam*. Algumas estatísticas possuem atualização diária e outras atualização mensal.

Figura 2 - Notificações de Ataques do tipo phishing



- "Fonte: CERT.br/NIC.br -https://stats.cert.br/**."**

Este segundo Gráfico acima traz em números a quantidade de ataques cibernéticos, especificados nos das espécies de *Phishing*, que são aqueles em que o criminoso se utiliza de meios informáticos para obter os dados pessoais do usuário, como por exemplo senhas, número de cartão de crédito. Neste caso, os atacantes se passam por entidades legítimas, como bancos, instituições financeiras ou empresas, e tentam induzir as vítimas a revelarem informações pessoais. Para isso os meios utilizados são por exemplo o envio de *webmail*, mensagens de SMS

para celulares ou mensagens com links em redes sociais, e como pode- se ver foram mais de 6 mil ataques do tipo phishing financeiro, mais de 1700 ataques de outros tipos de phishing, e mais de 180 ataques do tipo cavalo de troia, que inserem um programa malicioso no equipamento da vítima. Estes dados foram coletados no período de janeiro a março de 2023.

Além disso, as mudanças nos hábitos de consumo da população levaram a maior utilização da internet para transações bancárias on-line e compras no comércio eletrônico. Essa situação atrai criminosos buscando formas de enganar pessoas, obtendo ganhos e benefícios indevidos.

Diante dessa realidade, torna-se muito importante o estudo sobre os tipos de crimes virtuais existentes, para, a partir desse conhecimento, poder-se tomar as medidas necessárias para nos protegermos e também ao nosso patrimônio.

2.3 - LEGISLAÇÃO BÁSICA SOBRE CRIMES VIRTUAIS

À medida que a Internet se desenvolveu e o cibercrime aumentou, o Estado sentiu a necessidade de promulgar leis que protegessem os usuários de abusos. Foi aí que surgiram várias leis para lidar com esta questão.

2.3.1 – Lei de Carolina Dieckmann

A Lei nº 12.737/2012, popularmente conhecida como Lei Carolina Dieckmann, dispõe sobre a separação entre crime virtual e crime informático, além de acrescentar ao Código Penal os artigos 154-A e 154-B.

O objetivo da legislatura era dar mais privacidade aos usuários da rede e evitar que suas informações pessoais fossem violadas por terceiros, protegendo assim sua privacidade e intimidade.

Esta é a primeira lei que determinou a política de maior segurança no ambiente virtual e simboliza claramente o crime cibernético, principalmente no que diz respeito a ataques a computadores, e-mails e outras contas virtuais, sem o devido consentimento do titular.

Nesse sentido, a Lei contempla os seguintes casos, como atacar o computador de outra pessoa, violando indevidamente o mecanismo de segurança e

com o objetivo de obter, interferir ou destruir dados ou informações, além de arriscar para ganho ilegal, fabricar, oferecer para distribuir, vender ou distribuir um dispositivo ou programa de computador com a finalidade de praticar interferência de computador, divulgação, negociação ou transmissão a outra pessoa, a qualquer título, dos dados ou informações obtidas, interceptação ou interrupção de informações telegráficas, telefônicas, informáticas, ou de serviço público, falsificação de documento particular, falsificação de cartão de crédito ou débito.

2.3.2 - Marco Civil da Internet

O Marco Civil da Internet, Lei n° 12.965/2014, é a lei que regulamenta o uso da Internet no Brasil. Nesse sentido, este diploma legal traz diversos princípios, garantias, direitos e deveres dos usuários da rede, e estabelece diretrizes que permitem a atuação da União, Estados, Distrito Federal e Municípios nesta matéria.

O objetivo é garantir o direito à privacidade e à liberdade de expressão nas comunicações. Portanto, a violação de dados e informações confidenciais só será conhecida por ordem judicial.

A lei prevê que o acesso à internet é essencial para o exercício da cidadania, e nesse sentido, são garantidos ao usuário diversos direitos, como por exemplo a não violação da intimidade e da vida privada sob pena de indenização por danos materiais ou morais, a inviolabilidade e sigilo das comunicações feitas pela internet, a inviolabilidade e privacidade das comunicações feitas pela Internet, a impossibilidade de interromper a conexão com a Internet, exceto por suspensão, não fornecer informações pessoais a terceiros, a menos que expressamente autorizado, e o consentimento expresso para a coleta, uso, armazenamento e processamento de dados pessoais.

2.3.3 - Lei Geral de Proteção de Dados Pessoais (LGPD)

A Lei Geral de Proteção de Dados Pessoais (LGPD) representada pela Lei nº. 13.709/2018, versa sobre do tratamento de dados pessoais, inclusive meios digitais, por pessoas físicas ou jurídicas. A intenção do legislador era dar maior proteção aos direitos fundamentais de liberdade e privacidade e ao livre desenvolvimento da personalidade da pessoa natural.

Por conta disso, a Lei introduz diversos fundamentos, como respeito à privacidade, liberdade de expressão, informação, comunicação e ideias, desrespeito à intimidade, honra e imagem, direitos humanos, livre desenvolvimento da personalidade, dignidade e exercício da cidadania.

Em suma, de acordo com o art. 6 da Lei Geral de Proteção de Dados, podemos determinar 10 (dez) princípios, que são avaliados durante os procedimentos sobre os dados pessoais, vejamos:

I – finalidade:

II – adequação:

III - a necessidade:

IV - acesso livre:

V - qualidade dos dados:

VI – transparente:

VII – segurança:

VIII – prevenção:

IX - não discriminação:

X - demonstrar prestação de contas e responsabilidade, (STF, 2021).

Além disso, empresas que fizerem uso indevido de dados de clientes podem ser multadas em até 2% do faturamento total do negócio legítimo, com limite de R$ 50 milhões. Além das multas, os dados organizacionais podem ser bloqueados ou perdidos.

Estes princípios, para além de serem compatíveis com as leis de outros países que utilizam princípios semelhantes, garantem a uniformidade e eficácia das normas à facilidade de comunicar o seu conteúdo tanto aos titulares dos dados como aos que tratam os dados pessoais e a transferência internacional de dados.

Os princípios de proteção de dados incluem, por exemplo, o princípio da finalidade, segundo o qual o processamento de dados nunca é feito de forma genérica, mas deve ser feito para uma finalidade específica, que também deve ser suficiente e necessária para atingir sua finalidade.

Os princípios de transparência e de livre acesso, dos quais os titulares dos dados devem ser sempre cientificados quando tratam de informações sobre si próprios e têm amplo acesso às suas informações.

O princípio da qualidade, que garante a exatidão e atualização das informações.

O princípio de segurança que garante que o controlador de dados deve protegê-los.

O princípio da prevenção, que promove a implementação de medidas avançadas no desenvolvimento de sistemas de processamento de dados para evitar problemas futuros para os dados.

E, por fim, o princípio da não discriminação, importante para que a proteção de dados não seja apenas considerada do ponto de vista da privacidade do indivíduo, mas também considere que o uso de dados pessoais não deve incentivar práticas discriminatórias.

3 - PRINCIPAIS TIPOS DE CRIMES VIRTUAIS

Alguns crimes são cometidos por pessoas comuns, especialmente no caso de crimes contra a honra. Eles são caracterizados por insultos, fofocas infundadas e acusações de atos criminosos. Todos esses comportamentos lesam a integridade moral e prejudicam a dignidade e a honra das vítimas.

Por outro lado, alguns cibercriminosos participam de organizações criminosas e usam técnicas avançadas para obter benefícios financeiros. É o caso de ataques a bancos e sistemas financeiros de grandes empresas, por exemplo.

Alguns exemplos de crimes cibernéticos são, o *stalking*; casos de difamação; distribuição de mercadorias; violação da lei de propriedade intelectual; fraude de identidade, através do uso indevido de informações pessoais de outras pessoas; e roubo de dados financeiros relacionados a cartões de crédito.

3.1 CRIMES CONTRA A HONRA

Injúria, difamação e calúnia são crimes contra a honra que já estavam consagrados no Código Penal antes do advento da Internet. No entanto, esses crimes também podem ser cometidos no mundo virtual. Esses processos criminais tratam de crimes que atentam contra a honra de um indivíduo, como ofensa à sua reputação pessoal ou profissional.

Nesse aspecto, adentramos à questão da honra e da imagem, e neste sentido José Miguel Garcia Medina afirma:

> A constituição também protege a imagem. A honra de uma pessoa pode ser atingida quando indevidamente usada sua imagem, bem como, p.ex. em face do mau uso do seu nome [...] A inviolabilidade da honra e imagem diz respeito não apenas a atos que causem transtorno, mas, também, ao uso indevido. (MEDINA, 2014, pg. 85)

Podemos perceber assim que o uso indevido da imagem de alguém, mesmo existindo o limite da proteção da intimidade e da vida privada, pode resultar em danos morais e materiais. Desta forma, a internet, principalmente com as redes sociais, é um campo muito amplo, com fluxo de informações muito rápido, propiciando assim condutas danosas. A principal dificuldade é a de identificar o

autor, uma vez que o compartilhamento de imagens e informações possui um fluxo intenso, dificultando assim achar a fonte da conduta ilícita.

Logo adiante será tratado o conceito e as diferenças entre cada um desses casos.

3.1.1 - Calúnia

O crime de Calúnia está previsto no art. 138 do Código Penal, que afirma: “Caluniar uma pessoa, mentir é definido como crime”. A pena é de reclusão de seis meses a dois anos, além de multa.

A conduta consiste em imputar à vítima uma prática falsa, de fato considerado crime. É uma forma de prejudicar a honra da vítima. Qualquer pessoa pode ser sujeito ativo do crime, ainda permitindo coautoria e participação.

Da mesma forma, as pessoas que propagam e divulgam alegações falsas, mesmo que entendam que a informação é verdadeira, podem enfrentar as penalidades da Lei. É sobre disseminação e distribuição de informações. Assim fixa a lei: "A mesma punição é dada a quem, sabendo que as alegações são falsas, as divulga pela denúncia verbal ou as divulga relatando de qualquer outra forma".

Utilizando o crime no mundo virtual, uma pessoa que, por meio de suas redes sociais, fala palavras ofensivas a outra, e divulga que essa pessoa cometeu um crime, que de fato, ela não cometeu, comete um crime de calúnia. O crime é um ato livre e pode ser cometido por palavras escritas ou verbais, por ações e gestos.

O crime tipificado ocorre apenas quando a prática criminosa é conhecida por outras pessoas. Nesse sentido, se a calúnia escrita não chegar ao conhecimento de um terceiro por qualquer motivo, não houve crime completo.

Neste crime não deve haver certeza ou suspeita, ainda que equivocada, da existência de crime cometido por sujeito passivo. Isso significa que alguma intenção é necessária, o criminoso deve agir em consciência e por sua própria vontade para caluniar a vítima.

Podemos exemplificar este tipo de crime citando a seguinte jurisprudência:

> PROCESSUAL PENAL. RECURSO ORDINÁRIO EM HABEAS CORPUS. CALÚNIA, DIFAMAÇÃO E INJÚRIA MAJORADAS. ALEGAÇÃO DE INÉPCIA DA INICIAL. FALTA DE INDICAÇÃO DO LOCAL DOS FATOS. INCOMPETÊNCIA TERRITORIAL. PRECLUSÃO. EQUÍVOCO NA CAPITULAÇÃO JURÍDICA. NÃO OCORRÊNCIA. RÉU SE DEFENDE DOS

> FATOS. INVIABILIDADE DE INCURSÃO NO ACERVO PROBATÓRIO. NULIDADES. PRECLUSÃO PARA APRESENTAR RESPOSTA À ACUSAÇÃO. INOCORRÊNCIA. CERCEAMENTO DE DEFESA. NOMEAÇÃO DE DEFENSOR AD HOC SEM ANUÊNCIA DA PARTE. NÃO VERIFICAÇÃO. INTELIGÊNCIA DO ART. 44, DO CPC/1973. MATÉRIAS JÁ EXAMINADAS. REITERAÇÃO DE PEDIDO. RECURSO ORDINÁRIO DESPROVIDO. I - Os crimes contra a honra praticados pela internet são classificados como formais, ou seja, a consumação se dá no momento de sua prática, independente da ocorrência de resultado naturalístico, de forma que a competência deve se firmar de acordo com a regra do art. 70 do CPP
> ...
> Recurso ordinário desprovido. (STJ - RHC: 77692 BA 2016/0283021-4, Relator: Ministro FELIX FISCHER, Data de Julgamento: 10/10/2017, T5 - QUINTA TURMA, Data de Publicação: DJe 18/10/2017).

Logo, como visto, entende-se que a acusação deve ser falsa, ou seja, não corresponder à realidade dos fatos. Se a acusação for verdadeira, mesmo que seja prejudicial à reputação da pessoa, não será considerada calúnia.

3.1.2 - Difamação

A difamação envolve imputar à outra pessoa, um fato que ofenda sua reputação. A pena prevista no Código Penal é de reclusão de três meses a um ano, além do pagamento de multa. Este é um crime que degrada a dignidade da vítima. Isso porque se faz interpretação indecente da verdade, e por isso, é considerado crime.

Nesse sentido, a acusação não deve ser falsa. Por ser verdade, os crimes de difamação acontecem com mais ênfase a atacar a honra da vítima. Portanto, há necessidade de o agente estar plenamente ciente de que não há falsidade na acusação.

A difamação é muito comum na Internet, especialmente nas redes sociais. É o caso de publicar fotos de um adúltero, por exemplo, prejudicando a imagem e a reputação de outra pessoa.

Exemplifica ainda, uma jurisprudência sobre o assunto:

> JUIZADOS ESPECIAIS CRIMINAIS. DIREITO PENAL. QUEIXA-CRIME. DIFAMAÇÃO. CRIMES CONTRA A HONRA. GRUPO DE WHATSAPP. INEXISTÊNCIA DE IMPUTAÇÕES DE FATOS DETERMINADOS CAPAZES DE CONSUBSTANCIAR, POR SI, A OCORRÊNCIA POTENCIAL DE LESÃO OU MÁCULA À HONRA OBJETIVA OU SUBJETIVA DOS APELADOS. CRIMES CONTRA HONRA NÃO CARACTERIZADOS. RECURSO CONHECIDO E PROVIDO. 1) Cuida-se de recurso inominado interposto pelo apelante em face da r. sentença que

> julgou procedente a pretensão deduzida na queixa-crime para condená-lo como incursa a sanção do art. 139 do CP. 2) O apelante, a priori, suscita a incompetência do juízo em razão da necessidade de prova pericial. Segundo ele, as conversas que embasaram sua condenação foram extraídas de um grupo privado do whatsapp, do qual o recorrido embora participante, não ficou demonstrados nos autos que este foi quem postou as mensagens à ordem 7. No mérito, alega a atipicidade do crime de difamação, por ausência de comprovação de materialidade.
> ...
> Recurso conhecido e provido. 8). Sentença reformada. (TJ-AP - APL: 00564548020168030001 AP, Relator: MARIO EUZEBIO MAZUREK, Data de Julgamento: 07/08/2018, Turma recursal).

Compreende-se então que na Difamação da reputação, a imputação deve ser capaz de causar dano à reputação da pessoa envolvida. A reputação refere-se à opinião que terceiros têm sobre a honra, integridade ou moralidade da pessoa acusada.

3.1.3 - Injúria

O crime de injúria descreve a prática de crimes destinados a lesar a dignidade ou a honra de outrem. Muitas vezes, o comportamento criminoso ocorre por meio de ofensas, insultos e agressões verbais ou escritas à vítima. A pena será de reclusão de 01 a 06 meses, ou pagamento de multa.

Um crime de honra afeta a condição física, intelectual, moral e social da vítima. Trata-se do que uma pessoa pensa sobre si mesma, ou seja, está diretamente relacionada à sua autoestima. O crime é resolvido quando cessa a distribuição da injúria e divulga-se a verdade.

Se o dano for cometido em crimes relacionados à raça, cor, nacionalidade, religião e procedência, e referentes à condição de idoso ou de pessoa com deficiência, a pena será de reclusão de um a três anos e multa, sendo essas injúrias relacionadas à discriminação.

Um juiz não pode aplicar uma pena em um crime de injúria se o agente ativo, de forma culposa, causar diretamente a lesão, ou seja, esse crime somente é cometido na forma dolosa.

Esses tipos de crimes cometidos no ciberespaço que são considerados muito comuns.

> AGRAVO DE INSTRUMENTO. DECISÃO MONOCRÁTICA. AÇÃO COMINATÓRIA. RESPONSABILIDADE CIVIL. FACEBOOK. REDE DE RELACIONAMENTOS. POSTAGEM OFENSIVA PROVIMENTO

> ANTECIPATÓRIO DE TUTELA VISANDO EXCLUIR O PERFIL DO INDIGITADO AGRESSOR. DEFERIMENTO PARCIAL PELO JUÍZO SINGULAR COM BASE EM DISPOSITIVO DA LEI DO MARCO CIVIL DA INTERNET. LEI Nº 12.965/2014, ART. 22. DECISÃO MANTIDA POR SEUS PRÓPRIOS FUNDAMENTOS. RECURSO DESPROVIDO LIMINARMENTE, COM FULCRO NO ARTIGO 557, "CAPUT", DO CPC. (Agravo de Instrumento Nº 70064449457, Nona Câmara Cível, Tribunal de Justiça do RS, Relator: Miguel Ângelo da Silva, Julgado em 28/04/2015).
>
> (TJ-RS - AI: 70064449457 RS, Relator: Miguel Ângelo da Silva, Data de Julgamento: 28/04/2015, Nona Câmara Cível, Data de Publicação: Diário da Justiça do dia 12/05/2015).

Desta forma, pode-se concluir que o presente crime se resume em proferir palavras ou realizar ações que violem a dignidade ou ataquem a honra de uma pessoa, causando-lhe constrangimento, humilhação ou desprezo perante terceiros.

3.2 – AMEAÇA

O crime de ameaça está previsto no art. 147 do Código Penal. Veja a redação do dispositivo: “Ameaçar uma pessoa, pela voz, escrita ou toque, ou qualquer outro meio simbólico, a fim de prejudicá-la injusta e gravemente”. A pena aplicada será de prisão, de um a seis meses, ou o pagamento de multa.

Obtém-se o conceito de Ameaça conforme Alessandro Goncalves Barreto preceitua:

> Comete o crime de ameaça o indivíduo que envia mensagens eletrônicas à vítima, prometendo difamá-la gravemente em redes sociais e, ainda, sugerindo males indeterminados que poderiam acometer sua família. (BARRETO, 2016).

É o comportamento de intimidar, ameaçar e assustar a vítima, com palavras, textos e gestos. No caso do crime virtual, o comportamento ocorre por meio de comentários ameaçadores nas redes sociais. O crime é aperfeiçoado pela declaração da promessa do mal injusto, ou seja, especificar o ato a ser cometido. Com o advento das redes sociais, a ameaça tornou-se um crime comum.

Assim, pode-se exemplificar este crime com uma jurisprudência sobre o assunto:

> CONFLITO DE COMPETÊNCIA Nº 156.284 - PR (2018/0008775-5) RELATOR : MINISTRO RIBEIRO DANTAS SUSCITANTE : JUÍZO DE DIREITO DO JUIZADO DE VIOLÊNCIA DOMÉSTICA E FAMILIAR CONTRA A MULHER DE CURITIBA – PR SUSCITADO : JUÍZO DE DIREITO DA VARA CRIMINAL DE NAVIRAÍ – MS INTERES. : EVERTON APARECIDO DE LIMA SILVA INTERES. : JUSTIÇA PÚBLICA EMENTA

> CONFLITO DE COMPETÊNCIA. CRIME DE AMEAÇA PRATICADO POR *WHATSAPP* E *FACEBOOK*. ÂMBITO DE APLICAÇÃO DA LEI MARIA DA PENHA. DELITO FORMAL. CONSUMAÇÃO NO LOCAL ONDE A VÍTIMA CONHECE DAS AMEAÇAS. CONFLITO DE COMPETÊNCIA CONHECIDO. DECLARADA A COMPETÊNCIA DO JUÍZO SUSCITADO.1. O crime de natureza formal, tal qual o tipo do art. 147 do Código Penal, se consuma no momento em que a vítima toma conhecimento da ameaça. 2. Segundo o art. 70, primeira parte, do Código de Processo Penal, "A competência será, de regra, determinada pelo lugar em que se consumar a infração". 3. No caso, a vítima tomou conhecimento das ameaças, proferidas via *Whatsapp* e pela rede social *Facebook,* na Comarca de Naviraí, por meio do seu celular, local de consumação do delito e de onde requereu medidas protetivas. 4. Independentemente do local em que praticadas as condutas de ameaça e da existência de fato anterior ocorrido na Comarca de Curitiba, deve-se compreender a medida protetiva como tutela inibitória que prestigia a sua finalidade de prevenção de riscos para a mulher, frente à possibilidade de violência doméstica e familiar. 5. Conflito conhecido para declarar a competência do Juízo da 1º Vara Criminal da Comarca de Naviraí/MS, ora suscitado.

Conclui-se então que o crime de ameaça consiste em expressar ou comunicar de forma verbal, escrita, gestual ou por meio de outros meios uma ameaça de prejudicar a integridade física, a vida, a liberdade, a honra, o patrimônio ou qualquer outro interesse legítimo da pessoa ameaçada.

Para que seja configurado o crime de ameaça, é necessário que três elementos estejam presentes, sendo a conduta ameaçadora, onde o autor deve realizar uma conduta que tenha caráter ameaçador, seja por meio de palavras, gestos, escritos, mensagens eletrônicas, telefonemas, entre outros. Essa conduta deve demonstrar a intenção de prejudicar ou causar medo à vítima.

Também deve estar presente o potencial de causar medo ou insegurança: a ameaça deve ser capaz de causar temor, apreensão, insegurança ou coagir a vítima. É importante destacar que o medo causado pela ameaça deve ser justificado, ou seja, a ameaça deve ser crível o suficiente para que uma pessoa razoável a considere como uma ameaça real.

Por fim, o dolo, onde o autor da ameaça deve agir intencionalmente, consciente de que suas palavras, gestos ou ações são ameaçadoras e destinadas a causar medo ou coagir a vítima.

3.3 - IDENTIDADE FALSA

O crime de identidade falsa envolve dar a si mesmo ou a outra pessoa uma identidade falsa com a finalidade de obter uma vantagem injusta ou prejudicar

alguém. A pena é de reclusão de três meses a um ano, além do pagamento de multa.

Esse crime é comum na internet, onde criminosos criam perfis falsos para se passar por outra pessoa e cometer atos de má-fé. É o mesmo para uma pessoa que usa o nome e fotos de uma terceira pessoa para pedir dinheiro de forma inadequada, fingindo ser essa pessoa.

O crime se consuma no momento da falsa identificação. Desde então, o agente pode ser punido. Portanto, a obtenção de resultados é considerada como exaustão criminal.

De qualquer forma, é importante mencionar que criar perfis falsos nas redes sociais é considerado comportamento criminoso apenas se for baseado em uma pessoa real. No caso do perfil falso, onde são usadas fotos de coisas ou lugares, por exemplo, sem mencionar uma identidade falsa, pretendendo apenas manter a identidade do usuário oculta nas redes não constitui crime.

Assim como nos outros itens elencados, pode-se observar jurisprudência sobre o assunto:

> CRIME CIBERNÉTICO - FUNCIONÁRIO PÚBLICO - DELITO SEM COMPLEXIDADE - ESSÊNCIA DOS CRIMES DE ALTERAÇÃO DE SISTEMA INFORMATIZADO - CIRCUNSTÂNCIAS JUDICIAIS FAVORÁVEIS - PENA BASE FIXADA NO MÍNIMO. Funcionário da CEEE que transfere no sistema, débito de fornecimento de energia para pessoa fictícia. Crime cibernético tipificado no art. 313-A do Código Penal. Sendo favoráveis todas as circunstâncias judiciais, a pena base deve situar-se no mínimo. Não se pode entender como complexa, conduta de agente nessas condições, já que a alteração de dados em sistema informatizado é da própria...(TJ-RS - ACR: 70043570068 RS, Relator: Gaspar Marques Batista, Data de Julgamento: 06/10/2011, Quarta Câmara Criminal, Data de Publicação: Diário da Justiça do dia 13/10/2011).

Desta forma, o principal objetivo do criminoso é assumir uma identidade falsa ou utilizar documentos falsificados com o intuito de obter vantagens indevidas, enganar outras pessoas ou cometer outras atividades ilícitas. Resumidamente, consiste em usar uma identificação falsa, seja ela um nome fictício, documentos falsificados ou informações fraudulentas relacionadas à identidade pessoal, a fim de enganar, ludibriar ou cometer fraudes.

3.4 - CRIMES CONTRA O PATRIMÔNIO

A definição do que é patrimônio pode ser expressada como sendo um conjunto de bens, direitos e obrigações com valor econômico, que pertencem a uma pessoa, ou conjunto de pessoas ou ainda a uma empresa. Desta forma, o patrimônio envolve um complexo conjunto de ações jurídicas apreciáveis em dinheiro, ou seja, que tem valor econômico, que de uma forma direta, é concebido para a sociedade, como uma universalidade de direitos, ou seja, como uma unidade abstrata distinta dos elementos que a compõem, sendo este um conceito que é próprio do direito privado.

Então, pode-se determinar que não há crime patrimonial sem que haja uma lesão de interesse economicamente apreciável. Neste sentido, há a possibilidade de furto, de apropriação indébita e de roubo em relação a certos papéis que representam valores, como, por exemplo, ações ou letras de câmbio ou mesmo dinheiro em espécie.

De forma mais prática, podemos conceituar que No Brasil, os crimes contra o patrimônio são delitos que atentam contra a propriedade. Esses tipos de crimes estão previstos no Código Penal Brasileiro, que têm como objetivo a proteção dos bens materiais e imateriais das pessoas físicas e jurídicas de nossa sociedade.

Os crimes contra o patrimônio podem ser descritos como sendo:

Roubo, caracterizado pela subtração de algo mediante ameaça, violência ou grave ameaça. Nesse crime, o agente usa a força física ou psicológica para conseguir o que deseja, podendo ocasionar lesões ou morte à vítima. O roubo é uma conduta grave e é punido de forma rigorosa pela legislação brasileira.

Furto, que diferente do roubo, consiste na subtração de algo sem o emprego de violência ou grave ameaça. Nesse caso, o agente age de forma dissimulada, aproveitando-se da distração ou desatenção da vítima para praticar o delito. O furto é uma conduta considerada menos grave do que o roubo, mas ainda assim é punida pelo ordenamento jurídico.

Estelionato que é uma modalidade de crime contra o patrimônio que ocorre quando alguém obtém vantagem ilícita em prejuízo de outra pessoa, utilizando-se de artifícios, ardil, fraude ou outros meios fraudulentos. Essa conduta está relacionada à enganação, com o intuito de obter benefícios financeiros indevidos.

Dano, esse crime de dano ocorre quando alguém destrói, inutiliza ou deteriora coisa alheia, sem o consentimento do proprietário. Pode ser tanto um ato de vandalismo, como pichar um prédio, quanto uma ação negligente, como danificar um veículo por imprudência. O dano pode ser material ou imaterial, afetando não apenas o patrimônio, mas também a tranquilidade e a integridade emocional da vítima.

Apropriação indébita, este é um crime contra o patrimônio que ocorre quando alguém se apropria de forma indevida de um bem móvel que lhe foi confiado, seja por empréstimo, depósito, aluguel ou qualquer outra forma de guarda. O agente, ao invés de devolver o bem, passa a se beneficiar dele, causando prejuízo ao proprietário legítimo.

É importante ressaltar que cada um desses crimes possui suas particularidades, sendo necessário analisar as circunstâncias e os elementos presentes em cada caso específico. Além disso, as penas para essas infrações podem variar de acordo com a gravidade do delito, podendo incluir medidas restritivas de liberdade, multas e outras sanções previstas em lei.

3.4.1 - Patrimônio Digital

O patrimônio digital refere-se ao conjunto de ativos e informações digitais que uma pessoa ou organização possui. Esses ativos podem incluir conteúdos digitais, como arquivos de mídia (fotos, vídeos, músicas), documentos eletrônicos, e-mails, perfis em redes sociais, blogs, sites, entre outros.

O patrimônio digital é uma extensão do patrimônio tradicional e tornou-se cada vez mais relevante com o avanço da tecnologia e da sociedade digital. Ele representa não apenas um valor monetário, mas também um valor emocional e pessoal para os indivíduos.

Esse tipo de patrimônio pode incluir informações pessoais, registros de atividades, dados financeiros, comunicações importantes, entre outros conteúdos digitais que são armazenados e acessados por meio de dispositivos eletrônicos, como computadores, smartphones, tablets e servidores online.

É importante ressaltar que, assim como o patrimônio físico, o patrimônio digital também precisa ser protegido contra possíveis ameaças, como roubo de

identidade, invasões de privacidade, acesso não autorizado ou perda de dados. A segurança e a preservação do patrimônio digital tornaram-se preocupações essenciais para os indivíduos, empresas e instituições, que adotam medidas de segurança cibernética, backups regulares e outras práticas para garantir a integridade e a disponibilidade de seus ativos digitais.

Além disso, o patrimônio digital também levanta questões legais, como a sucessão digital, que envolve a transferência ou a preservação do patrimônio digital após o falecimento de uma pessoa. Muitos países estão desenvolvendo leis e regulamentações para lidar com essas questões, a fim de proteger os direitos e as necessidades dos indivíduos em relação ao seu patrimônio digital.

Em suma, o patrimônio digital abrange todos os ativos e informações digitais de uma pessoa ou organização, exigindo cuidados especiais para a sua segurança, preservação e tratamento legal adequado.

3.4.2 - Estelionato e Fraudes Virtuais

O estelionato é um crime comum, ou seja, pode ser praticado por qualquer pessoa, não sendo restrito a determinadas profissões, cargos ou qualidades específicas. Ele não é considerado um crime de mão livre, uma vez que exige ações fraudulentas e dolosas por parte do autor para obter vantagem financeira indevida.

Quanto à classificação jurídica do estelionato, é um crime próprio, ou seja, requer uma particular qualidade ou relação específica entre o autor e a vítima. No caso do estelionato, o autor deve induzir ou manter a vítima em erro por meio de fraude.

Quanto à ação penal, o estelionato é um crime de ação penal pública incondicionada, ou seja, a persecução penal pode ser iniciada pelo Ministério Público, independentemente de autorização ou representação da vítima. O Ministério Público é responsável por oferecer a ação penal, levando o caso aos tribunais e buscando a punição do autor do crime.

Em relação à suspensão condicional do processo (também conhecida como transação penal) e à aplicação da ANPP (Acordo de Não Persecução Penal), existe a possibilidade de aplicação no ordenamento jurídico brasileiro, desde que aplicados os devidos requisitos legais.

A suspensão condicional do processo está prevista no artigo 89 da Lei de Execução Penal (Lei nº 9.099/1995) e no artigo 89 da Lei de Drogas (Lei nº 11.343/2006). Essa medida possibilita a suspensão do processo criminal por um determinado período, mediante o cumprimento de certas condições pelo acusado. Se o acusado cumprir essas condições estabelecidas, ao final do prazo fixado, o processo é extinto e não há condenação. No entanto, caso o acusado descumpra as condições, o processo é retomado.

Acordo de Não Persecução Penal (ANPP): O ANPP foi introduzido no ordenamento jurídico brasileiro pela Lei nº 13.964/2019, conhecida como Pacote Anticrime. Trata-se de um instrumento que permite a aplicação de medidas alternativas à persecução penal em determinados casos de crimes de menor potencial ofensivo ou crimes com pena mínima inferior a quatro anos. O acordo é firmado entre o Ministério Público e o acusado, com o objetivo de evitar o processo judicial. Para que o ANPP seja aplicado, é necessário que o acusado confesse formal e circunstancialmente a prática do crime e concorde com a proposta apresentada pelo Ministério Público.

É importante ressaltar que tanto a suspensão condicional do processo quanto o ANPP estão sujeitos a critérios legais e decisão discricionária do Ministério Público, que analisará a viabilidade e a conveniência de aplicar essas medidas em cada caso específico. Além disso, a legislação pode sofrer alterações ao longo do tempo, sendo fundamental consultar a legislação atualizada e buscar orientação jurídica específica para compreender como essas medidas são aplicadas no contexto atual do ordenamento jurídico brasileiro.

Estudo realizado pela Federação do Banco do Brasil (Febraban) mostra que o número de tentativas de fraudes financeiras contra brasileiros aumentou durante a covid19. Nesse período, a agência registrou um aumento de 80% no crime cibernético (fraude na Internet). As principais infrações incluem roubo de identidade, roubo e venda de dados comerciais, fraude por terceiros em sites de varejo online, fraude em seguros, caridade e arrecadação de fundos. Existem créditos fraudulentos e roubos de cartão que vêm com ele (TIBURSKI, 2020).

De acordo com a interpretação da Suprema Corte, transações fraudulentas no ciberespaço são características de peculato. No entanto, não é fácil definir padrões precisos para atividades cibercriminosos, especialmente para comércio.

O Direito Penal no artigo 171 define estelionato como “obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento: Pena – reclusão, de 1 (um) a 5 (cinco) anos, e multa.

Ao inserir a cláusula acima no contexto de estelionato, o mesmo de acordo com Gil:

> Ação intencional e prejudicial a um ativo intangível causada por procedimentos e informações (software e bancos de dados), de propriedade de pessoa física, ou jurídica, com o objetivo de alcançar benefício, ou satisfação psicológica, financeira e material. GIL (2000. P. 114).

Conclui-se, então, que o crime em questão é definido como forma de crime que ilude a vítima visando a sua situação de vulnerabilidade e a leva ao erro, normalmente, o criminoso envia um e-mail falso para a vítima, que contém um link que redireciona a vítima para a página de compra. Este é o mecanismo usado para obter os dados bancários.

Segundo matéria publicada no site da internet do órgão Serasa, um tipo de golpe, de fraude, que se utiliza do estelionato para se concretizar, que ficou bem conhecido através das durante a pandemia, foi o “Golpe no Benefício do Governo”, que se trata de crime cometido no requerimento do benefício do Governo Federal Auxílio Brasil.

Desta forma, conclui-se que O crime de estelionato é a prática de enganar alguém, por meio de fraude, com o objetivo de obter vantagem financeira indevida para si ou para terceiros. Resumidamente, consiste em induzir ou manter alguém em erro, utilizando artifícios, ardil, falsidade, promessas falsas ou qualquer outro meio fraudulento, visando obter um benefício financeiro ilícito.

Para que seja configurado o crime de estelionato, é necessário que quatro elementos estejam presentes, sendo, a Fraude, onde o autor do crime utiliza algum tipo de artifício, ardil, falsidade, promessa falsa ou qualquer outro meio fraudulento para enganar a vítima, a Indução ou manutenção em erro, em que o autor induz ou mantém a vítima em erro, fazendo-a acreditar em uma situação falsa, omitindo informações relevantes ou utilizando de falsas representações, a Obtenção de vantagem ilícita, demonstrado pelo fato de que o objetivo do autor é obter uma vantagem financeira indevida para si mesmo ou para terceiros, causando prejuízo à vítima, e por fim, Dolo, no qual, o autor deve agir intencionalmente, consciente de

que suas ações são fraudulentas e com a intenção de obter benefícios financeiros ilegítimos.

Sendo assim, o crime de estelionato é tipificado no ordenamento jurídico brasileiro e pode acarretar consequências legais para o autor, como penas de prisão, multas ou outras penalidades. A gravidade do crime e suas circunstâncias específicas podem influenciar a determinação da pena.

4 - BENEFÍCIO DO GOVERNO FEDERAL – AUXÍLIO BRASIL

4.1 - ASSISTÊNCIA SOCIAL E A CONSTITUIÇÃO FEDERAL DE 1988

O respeito a dignidade da pessoa humana sempre foi um importante atributo das sociedades modernas. Trata-se de garantir ao indivíduo que suas necessidades vitais e básicas sejam respeitadas, mesmo que não esteja em um patamar de igualdade de direitos com os outros membros da sociedade. Desta forma, a busca por uma igualdade dos direitos fundamentais é o grande ensejo deste princípio.

Com a Constituição de 1988, o princípio da Dignidade da Pessoa Humana foi colocado como orientador para todo o ordenamento jurídico, por estar elencado como Fundamento da República Federativa, no artigo 1º do referido diploma legal. Assim, todos os atos, decisões e orientações devem sempre levar em conta, que em hipótese alguma tal princípio possa vir a ser desrespeitado.

Porém o Estado, além de apenas respeitar esta dignidade, se viu na obrigação de intervir na sociedade, levando assistência aos que dela necessitassem. A política assistencialista do Estado, através da Assistência Social, busca exatamente esta concretização, promovendo o bem estar da população, oferecendo aos marginalizados condições mínimas que garantam sua dignidade.

A Constituição Federal, em seu artigo 203, inciso V, instituiu um benefício que tem como característica levar aos idosos e aos deficientes que não tivessem meios de prover sua subsistência nem de tê-la provida por suas famílias, a percepção de 1 (um) salário mínimo, garantindo assim a respeitabilidade de direitos.

4.2 – AUXÍLIO BRASIL

O Auxílio Brasil é um programa do Governo Federal, de Assistência Social, que é administrado pelo Ministério da Cidadania. Este programa substitui o programa anterior, que é o benefício do Bolsa Família, instituindo o pagamento de um valor, de natureza assistencial, para famílias em situação de extrema pobreza e pobreza.

Segundo o portal do Governo Federal na internet, este programa contribui no combate à pobreza extrema garantindo renda básica para a população, integrando políticas públicas, que visam simplificar a cesta de benefícios sociais e assistenciais

do governo, além de estimular a emancipação destas famílias para que alcancem autonomia e superarem situações de vulnerabilidade social.

O Auxílio Brasil visa alcançar os cidadãos brasileiros em situação de vulnerabilidade através de critérios como, Primeira Infância: para famílias com crianças de até 3 anos incompletos. Composição Familiar: para famílias com gestantes, nutrizes ou pessoas de 3 a 17 anos, ou de 18 a 21 anos matriculados na educação básica. Superação da Extrema Pobreza: para famílias cuja renda mensal per capita continuar abaixo da linha de extrema pobreza (R$ 105), mesmo após a soma dos critérios 1 e 2, não havendo limitações quanto ao número de integrantes da família.

É necessário ao cidadão candidato ao benefício se inscrever no Cadastro Único (CadÚnico) e aguardar a análise de um sistema informatizado, que avalia todas as regras do Programa, no entanto, a entrada no programa não é automática, pois o Governo Federal analisa o limite orçamentário do programa.

4.2.1 - Etapas para a solicitação de benefício do Governo Federal

4.2.1.1 - Fazer a inscrição no Cadastro Único

A primeira etapa da solicitação do benefício é solicitar a sua inscrição no Cadastro Único, que nada mais é do que a porta de entrada para os programas sociais dos Governos Federal, Estaduais, Distrital e Municipais. Esse Cadastro é realizado presencialmente em qualquer parte do Brasil, e para permanecer inscrito é necessário que o solicitante mantenha as informações de toda a sua família sempre atualizadas.

O cadastro é realizado em um Centro de Referência da Assistência Social (CRAS), que é o Posto de Atendimento do Cadastro Único e Setor Responsável pelo Programa Auxílio Brasil. O atendimento ocorre nas gestões descentralizadas dos municípios e cada um tem autonomia para definir seus protocolos de atendimento.

4.2.1.2 - Receber o Cartão do Auxílio Brasil

Ao ser selecionado para o Programa, o requerente receberá um cartão emitido pelo banco Caixa Federal, em nome do(a) responsável familiar. O Cartão é

enviado pelos Correios no endereço informado no Cadastro Único. Acompanha o cartão um panfleto com explicações importantes, por exemplo, como receber o benefício, datas de recebimento do benefício e outras informações.

4.2.1.3 - Receber Benefício Financeiro

O solicitante passará a receber mensalmente uma quantia em dinheiro, com valor dependente da renda mensal por pessoa da família, da quantidade de pessoas na família, se na família tem criança ou adolescente, ou se na família tem alguma grávida.

4.2.1.4 - Cumprir os compromissos de Saúde e Educação

Para permanecer inscrita no programa, as famílias devem cumprir compromissos com as políticas de Saúde e Educação, como por exemplo a frequência escolar mensal mínima de 60% para crianças de 4 e 5 anos e de 75% para estudantes de 6 a 21 anos, bem como, cumprir o calendário nacional de vacinação, e fazer o acompanhamento nutricional, de peso e altura de crianças menores de 7 anos, e por fim, do pré-natal para as gestantes, para permanecerem cadastrados no CadUnico.

4.2.1.5 - Manter o Cadastro Atualizado

Será necessário que a família cadastrada atualize seu cadastro no CRAS no período máximo de dois anos, mas sempre que houver alguma mudança nas informações da família, será necessário o comparecimento do(a) responsável para efetuar a atualização.

4.3 - TENTATIVAS DE GOLPE NO BENEFÍCIO DO GOVERNO FEDERAL

Após ser implementado pelo governo federal o benefício do Auxílio Brasil, várias são as tentativas de aplicação de golpe, para fraudar o recebimento do benefício do Auxílio Brasil, sendo muitas dessas tentativas através de redes sociais que alcançam a população brasileira, como por exemplo, em mensagens que

circulam através do aplicativo de Celular WhatsApp, por mensagem de texto de celular, conhecida como SMS, e também por e-mail, que, segundo empresas de segurança em informática, ultrapassam a marca de 20 mil tentativas por dia, o equivalente a 13 tentativas por minuto. As informações são de recente levantamento da empresa especializada em segurança digital PSafe.

A fraude geralmente utiliza-se do nome do programa do Governo Federal, para induzir a vítima a acessar um link malicioso, enviado pelos meios supra citados, e solicita a vítima a realizar um cadastro em um banco de dados, que por exemplo, traz a promessa de que a vítima irá receber um valor de R$2.500,00, via Pix após conclusão do cadastro.

Durante o período verificado pela referida empresa de segurança digital, foram bloqueadas mais de 140 mil tentativas de golpe e descobertos 17 sites falsos na internet, que são muito similares aos sites do Benefício do Auxílio Brasil na internet, onde os criminosos tentam se passar pelo canal do governo e assim obter os dados das vítimas, que depois serão usados em solicitações reais dos benefícios do Auxílio Brasil, nos canais oficiais do Governo Federal.

A tentativa de golpe para obter os dados das vítimas, para fraudar os requerimentos do benefício do Auxílio Brasil ocorrem através de um meio chamado *Phishing*, que consiste na técnica de disseminação de *links* maliciosos, como dito anteriormente, via aplicativo de celular WhatsApp, SMS e e-mail, roubando os dados pessoais ou bancários da vítima. Essa referida mensagem é usada como uma espécie de isca para a vítima ter a possibilidade de consultar o direito ao benefício do governo, após fazer o cadastro, mencionado anteriormente pelo site indicado, que é uma cópia idêntica do site oficial, no entanto, trata-se de um site falso, que não direciona os dados nele inseridos para o cadastro do Governo Federal, mas que fornece esses dados aos *Hackers* que estão aplicando a tentativa de golpe.

Em alguns casos, o texto da mensagem maliciosa também instrui a vítima a compartilhar o referido link com outros contatos de seu telefone celular, como condição para recebimento do falso benefício. Tal estratégia faz com que mais pessoas recebam a mensagem de *Phishing*, ajudando a disseminar os links maliciosos e a aumentar a possibilidade de aplicação do golpe em proporções exponenciais, com um número de vítimas cada vez maior.

No entanto, existem formas de se proteger dessas tentativas de golpe do Auxílio Brasil, assim como de outros benefícios, e também de outros crimes

praticados no ambiente virtual. É fortemente recomendado por empresas de segurança digital cada pessoa usuária de sistemas de informática ter um programa de antivírus instalado no celular e também no computador que utiliza, pois o referido aplicativo de proteção pode bloquear os links maliciosos enviados, de forma imediata, além de poder fazer varreduras periódicas no sistema do smartphone e computador para identificar malwares e atividades suspeitas realizados por aplicativos instalados no celular ou computador da pessoa.

As empresas de segurança também orientam que é preciso o usuário dos aplicativos desconfiar de propostas muito atrativas, como promoções, sorteios, ganhos rápidos e brindes, que chegam via mensagens do aplicativo WhatsApp, ou por SMS contendo os links suspeitos.

Desta forma, o usuário deve, ao receber as referidas mensagens suspeitas, checar o endereço de site da internet a que o link enviado indica, utilizando para isso um endereço de internet, ou URL, em que um verificador faz a varredura do site antes do usuário abrir o link clicando nele. O analisador de links do site da internet pertencente a empresa dfndr lab (psafe.com/dfndr-lab/pt-br/), por exemplo, é capaz de informar se um site é seguro ou contem alguma irregularidade que possibilita ao hacker capturar os dados do usuário não.

Sabendo-se que o acesso ao benefício do Auxílio Brasil é restrito aos usuários que fazem parte do Cadastro Único, cuja inscrição é realizada somente de forma presencial em postos de atendimento, muitas vezes a tentativa de golpe não seria apenas para a obtenção irregular do Benefício, mas os dados capturados podem ser utilizados de todas as formas que os *hackers* descobrirem para tentar fraudar um requerimento e recebimento de benefícios do Governo.

Nesse sentido, é preciso que o usuário esteja atento às propostas enviadas nos referidos *links*, para perceber com antecedência que tratem-se de propostas falsas de benefícios do governo. Sendo assim é recomentado aos usuários que não forneçam dados pessoais sob hipótese alguma.

Mas, caso o usuário tenha acessado os referidos *links* fraudulentos e realizado cadastros em sites falsos, é altamente recomendado que o usuário mude todas as senhas, sobretudo de aplicativos bancários.

Além disso, é fundamental que os usuários ativem recursos nativos de proteção dos smartphones, como a autenticação de dois fatores. O procedimento

impede que terceiros tenham acesso às suas contas, mesmo que estejam em posse do seu login e senha.

Se tiver fornecido documentos pessoais, como CPF e RG, o usuário deverá fazer um boletim de ocorrência e comunique seu banco a respeito. Entre também em contato com as instituições envolvidas, como a Caixa Federal, para buscar soluções efetivas.

4.4 - GOLPE DO EMPRÉSTIMO CONSIGNADO

Segundo *Site* da empresa SERASA, no início de agosto de 2022 foi sancionada uma proposta de lei, que possibilita a modalidade de crédito consignado para o Auxílio Brasil, com empréstimo descontando até 40% do valor do benefício direto da fonte.

Essa possiblidade está sendo utilizada por *Hackers*, que estão se aproveitando a existência dessa nova modalidade de empréstimo para aplicar golpes.

Segundo o Site do SERASA, as vítimas relatam ter recebido ligações oferecendo o crédito consignado no valor de R$ 2.500, que seriam pagos no mesmo dia e descontados em parcelas de R$ 170 diretamente do Auxílio Brasil, no entanto, com essa ligação os criminosos estão novamente tentando obter os dados pessoais das vítimas para posteriormente fazer a realização de cadastros fraudulentos, utilizando os dados das vítimas em requerimentos oficiais de benefício do Governo Federal, já que os dados utilizados são válidos, contudo, dados como endereço são alterados, para que os criminosos, de posse do cartão benefício da vítima, possam se passar pelas vítimas, realizando saques dos valores referentes aos benefícios solicitados fraudulentamente.

Em alguns casos, os criminosos chegam até a cobrar dinheiro das vítimas, que teriam que fazer um depósito antecipado de quantia em adiantamento para liberação do benefício, prática ilegal para todas as modalidades de empréstimo.

4.4.1 - Formas de prevenção ao golpe

As informações pessoais não devem ser compartilhadas com desconhecidos, considerando que os dados pessoais do usuário são extremamente valiosos, e que

com eles em mãos, fraudadores podem cometer outras fraudes além do golpe do Auxílio Brasil, Deve-se tomar muito cuidado ao se preencher qualquer tipo de formulário online, principalmente em sites desconhecidos e não-oficiais.

Faz-se necessário desconfiar de ofertas online do benefício do Auxílio Brasil, o pagamento do benefício do Auxílio Brasil é feito exclusivamente pelo banco Caixa Econômica Federal, onde o usuário pode sacar o valor do benefício por meio de Poupança Social Digital, ou Poupança CAIXA Fácil, produtos oferecidos pelo referido banco, ou ainda via saque com o cartão do programa, desta forma, qualquer proposta de pagamento por outros canais deve gerar desconfiança no usuário do benefício.

Não se deve fazer quaisquer depósitos antecipados para liberação de contratos de empréstimos, essa prática é ilegal, e Instituições bancárias sérias não solicitam nenhum tipo de pagamento antecipado para liberação de empréstimos.

O usuário deve monitorar o seu CPF (Cadastro de Pessoa Física), utilizando - se de um aplicativo ou serviço do Serasa, que foi desenvolvido justamente para buscar aumentar a proteção dos dados do usuário. Com ele, usuário pode monitorar seus dados 24 horas por dia, também será alertado sempre houver vazamento de dados ou uma tentativa de fraude em seu CPF.

No entanto, caso o usuário já tenha clicado em um link suspeito, o mesmo deverá alterar todas as suas senhas, principalmente de aplicativos bancários, e procurar saber se o aplicativo utilizado oferece algum recurso de autenticação de segurança que use dois fatores para validação, ou seja, aumentando a segurança na utilização de aplicativos desenvolvidos para celular ou computador. Com esse recurso, terceiros não conseguem acessar as contas do usuário, mesmo que possuam login e senha da referida conta.

Caso o usuário tenha compartilhado documentos pessoais, como RG ou CPF, deverá ser comunicado imediatamente ao banco que o usuário utiliza os serviços, e deverá ser feito um boletim de ocorrência, informando ter sido vítima de uma tentativa de golpe.

No portal do órgão público Procon existe um alerta para golpes envolvendo repasses do governo federal a famílias, onde a recomendação do referido órgão é que as pessoas não entrem em links na internet que utilizam nomes não definitivos e com promessas de solução de endividamento.

O Procon ainda alerta a população para um novo golpe, desta vez relacionado a uma atualização ainda em discussão no programa do governo federal.

A eventual mudança está ligada ao repasse de recursos diretamente a famílias para quitação de empréstimos consignados.

Segundo Claudia Silvano, diretora do Procon-PR:

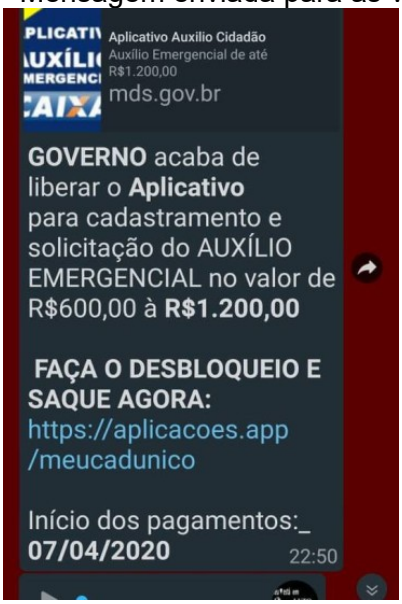
> “É importante destacar que a implementação de mudanças nos programas ainda está em estudo. Porém, os golpistas já começaram até mesmo a usar um nome, que sequer está definido, para atuar”.

Claudia Silvano ainda explicou:

> “Eles se aproveitam de um momento de fragilidade desses consumidores que, eventualmente, estão com nome em cadastro de inadimplentes ou que pretendem aumentar o score do seu CPF”.
> “Na ânsia de resolver a situação de um empréstimo que foi contraído e gerou uma dívida, a pessoa pode acabar formalizando um acordo que, na verdade, não existe de verdade, perdendo o dinheiro dessa falsa negociação e deixando sua condição financeira ainda mais complicada”.

Segundo o portal na internet do jornal “Extra”, o Golpe sobre falso cadastro no auxílio de R$ 600 já fez 6,7 milhões de vítimas, exibindo a imagem seguinte, contendo a seguinte mensagem:

Figura 3 – Mensagem enviada para as vítimas



Fonte: Site Jornal O Globo

Esta figura refere-se a Mensagem falsa, enviada para pessoas, versando sobre o benefício do Governo Federal, circulando nas redes sociais como Whatsapp por exemplo.

O Referido site do jornal traz ainda que no Estado do Rio de Janeiro, um outro tipo de golpe circula na internet, com falso link para que, supostamente, fosse feito o cadastramento na plataforma do benefício auxílio emergencial do Governo Federal de R$ 600,00. Tal cadastro fraudulento já fez cerca de 6,7 milhões de vítimas desde março, alertou o site com dados da empresa de segurança digital dfndr lab laboratório especializado em segurança digital da PSafe.

Ao clicar no link malicioso indicado, o usuário é levado um questionário com três perguntas: "Você recebe Bolsa Família?"; "Você é autônomo?"; "Você quer receber o auxílio?".

Após o usuário responder afirmativamente as questões, aparece uma outra mensagem informando o benefício ter sido aprovado, mas que, antes, seria necessário que o usuário enviasse o link para seus contatos no WhatsApp.

Segundo a referida empresa de segurança digital explicou, na voz de Emilio Simoni, diretor do dfndr lab.:

> “Para tornar o ataque mais verídico, alguns golpes se aproveitam de ações reais que grandes empresas e o governo estão realizando para enfrentar o coronavírus, como a doação de álcool em gel e pagamento de benefícios à população. E a tendência é que o número de ataques e de vítimas aumente, principalmente em decorrência do agravamento da situação do país neste momento de crise”.

A referida empresa PSafe, informou ainda que existem diversos links por onde o ataque de criminosos virtuais vem sendo disseminado, sendo alguns dos links auxilio-corona.info, auxiliocorona.com, auxiliocidadao.com, auxiliocidadao.archivezap.live/, e bit.ly/AuxilioCidadao.

Segundo a empresa, grande parte desses links de internet têm o objetivo de roubar dados pessoais e financeiros das vítimas ou levá-las a páginas falsas para visualizar publicidades excessivas.

No portal do Governo Federal pode-se encontrar a orientação de que o usuário deve denunciar ao Ministério da Cidadania fraude no Auxilio Emergencial, e informa ainda que para verificar se os dados do usuário foram indevidamente utilizados por terceiros para recebimento do Auxílio Emergencial, o cidadão deverá fazer a consulta no site https://consultaauxilio.dataprev.gov.br/ e consultar se houve solicitação e/ou pagamento do Auxílio Emergencial para o CPF do usuário.

Caso seja confirmado que os dados do cidadão foram utilizados

indevidamente, o mesmo deve ir pessoalmente em uma agência da Caixa Econômica Federal – CEF e proceder com o registro de contestação, informando sobre a utilização indevida dos seus dados por terceiros visando a obtenção fraudulenta do Auxílio Emergencial. A Caixa, em poucos dias, retornará ao cidadão o resultado da análise da contestação.

O Usuário, de posse dos documentos de registro de contestação e do resultado da análise da Caixa, deverá registrar uma denúncia de fraude no benefício do auxílio emergencial no ministério da cidadania no canal de atendimento do referido ministério no site da internet do mesmo.

Destaca-se que, caso o cidadão tenha emitido um documento de nome DARF, para efeitos da Declaração de Imposto de Renda 2021, mas não reconhece o requerimento do benefício, deve denunciar que seus dados foram utilizados fraudulentamente sem seu conhecimento ou anuência.

Para registrar ou acompanhar a manifestação o cidadão deverá acessar a Plataforma Integrada de Ouvidoria e Acesso à Informação do portal Fala.BR, na internet e que pertence ao Governo Federal.

Estes são os recursos e ferramentas disponíveis ao cidadão para poder não ser vítima de tentativas de golpe no benefício assistencial do Governo Federal, mas caso tenha sido vítima, os procedimentos supracitados são necessários para a defesa e regularização da situação do cidadão, bem como o resguardo para que o nome o cidadão não seja incluído no rol de pessoas protestadas nos órgãos de fiscalização e controle do Governo Federal.

Diante de todo o exposto é possível constatar que, diante de todos os crimes cibernéticos, o Código Penal Brasileiro aborda diversas condutas relacionadas ao ambiente digital, porém, suas penalidades são consideradas brandas e não são efetivas o suficiente para desencorajar a prática dessas ações. Por exemplo, o "golpe do benefício do governo", que pode ser enquadrado no Código Penal como fraude do tipo *phishing*, e é considerado crime de acordo com o artigo 154-A.

No entanto, essa falta de penas mais rígidas na legislação em relação aos crimes cibernéticos contribui para a percepção de que a internet é um ambiente sem lei. Sendo assim, é imprescindível que sejam promulgadas outras leis, mais específicas para lidar com os delitos cometidos em ambientes virtuais, uma vez que esses crimes são comuns e podem causar danos reais às vítimas. A imposição de penas proporcionais é uma forma de controlar esses comportamentos criminosos,

pois ao saberem que podem sofrer consequências significativas, os infratores, pensarão duas vezes antes de praticar tais atos.

Assim, é necessário um fortalecimento da legislação no que diz respeito aos crimes cibernéticos, a fim de garantir a proteção adequada das vítimas e estabelecer um ambiente digital mais seguro. Medidas mais rigorosas e proporcionais às infrações cometidas servirão como uma importante ferramenta de dissuasão, ajudando a conter essas práticas criminosas e incentivando a responsabilidade individual de todos os usuários da internet.

5 - CONCLUSÃO

A evolução digital transformou o cotidiano, o modo de agir e pensar de toda sociedade, e isto foi de tal maneira, que essa mudança trouxe benefícios para a resolução das demandas diárias, mas também trouxe o lado obscuro de toda essa facilidade, com a expansão dos índices de criminalidade digital.

Neste trabalho foram apontados os crimes cibernéticos mais comuns, bem como o modus operandi dos criminosos, com ênfase no crime cometido na obtenção de dados de forma ilegal e o requerimento de forma fraudulenta do benefício do Governo Federal Auxílio Brasil.

Foram analisadas as principais leis específicas brasileiras voltadas para coibir os crimes virtuais, a Lei 12.737/12 conhecida como a “Lei Carolina Dieckmann”, a Lei 12.965/14 oficialmente chamada de Marco Civil da Internet, a importância da Lei 13.709/18 – Lei Geral de Proteção de Dados, e o entendimento dos tribunais sobre os meios de barrar as condutas criminosas, que na maioria dos casos empregam a analogia para o julgamento desses crimes.

Ao se tratar do Brasil, mesmo com leis anteriores que abordavam a temática de privacidade, proteção de dados como, por exemplo, a Lei de acesso à informação, o Marco civil da internet, a Lei Carolina Dieckmann, dentre outras, as leis ainda não abrangiam totalmente os tipos de crimes, sendo então necessária a criação da Lei Geral de Proteção de Dados, gerando impactos positivos na sociedade.

Quando se trata de dados pessoais de pessoa física, o titular agora possui total direito ao acesso e exclusão, ou anonimização de seus dados em instituições, ou bases de dados a qualquer momento que desejar.

Desta forma, o presente trabalho contribui para o conhecimento do leitor bem como para o debate sobre a temática de Proteção de Dados no contexto e no campo da Internet no Brasil, abordando ainda uma lista de cuidados e procedimentos para que o leitor possa se precaver e não sofrer com golpes aplicados pelas redes sociais

Ante todo o exposto, é notável a importância de serem trabalhadas as leis para a proteção dos dados dos cidadãos, bem como a tipificação dos crimes cibernéticos e a fixação de penas para os criminosos. Mas Também deve-se ser observados os tipos de comportamentos necessários aos cidadãos para se proteger

e não sofrerem com dissabores oriundos da captura e mau uso de seus dados por hackers e outros criminosos.

REFERÊNCIAS

BARRETO. Alessandro Gonçalves. Manual de Investigação Cibernética à luz do Marco Civil da Internet. Rio de Janeiro. Ed Brasport, 2016.

BRASIL. Lei Geral de Proteção de Dados. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 25 set. 2022.

BRASIL. Portal. Disponível em https://www.gov.br/pt-br/servicos/receber-o-auxilio-brasil-pab#:text=Esse%20Cadastro%20%C3%A9%20realizado%20presencialmente a%20sua%20fam%C3%ADlia%20sempre%20atualizadas.&text=Presencial%20%3A Respons%C3%A1vel%20pelo%20Programa%20Bolsa%20Fam%C3%ADlia. Acesso em: 13 mai. 2023.

BRASIL. Portal. Disponível em https://www.gov.br/cidadania/pt-br/servicos/auxilio-emergencial/denunciar-fraude-no-auxilio-emergencial-1. Acesso em: 10 mai. 2023.

BRASIL. Presidência da República. Constituição Federativa do Brasil 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 12 nov. 2021.

BRASIL. Presidência da República. Lei 12.737, de 30 de novembro de 2012. Disponível em:

http://www.planalto.gov.br/ccivil_03/_ato2011014/2012/lei/l12737.htm. Acesso em: 25 set. 2022.

BRASIL. Presidência da República. Lei 12.965, de 23 de abril de 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 25 set. 2022.

BRASIL. Presidência da República. Lei 13.709, de 14 de agosto de 2018. Disponívelem:http://www.planalto.gov.br/ccivil_03/_ato2015-018/2018/lei/l13709.htm. Acesso em: 25 set. 2022.

CASTRO, Aldemario Araujo. A internet e os tipos penais que reclamam ação criminosa em público. Disponível em: http://egov.ufsc.br/portal/sites/default/files/anexos/13308-13309-1-PB.pdf. Acesso em: 25 set. 2022.

EXTRA, Jornal. Disponível em https://m.extra.globo.com/economia-e-financas/golpe-do-auxilio-emergencial-faz-vitimas-em-todo-brasil-veja-como-identificar-fraude.html. Acesso em: 21 mai. 2022.

GIL, Antônio de Loureiro. Fraudes Informatizadas. 2ª edição, 1ª tiragem, 2000.

MEDINA. José Miguel Garcia. Constituição Federal comentada. 3. ed. rev., atual. e ampl. São Paulo: Editora Revista dos Tribunais, 2014.

O GLOBO, Jornal. Disponível em https://oglobo.globo.com/economia/defesa-do-consumidor/golpe-sobre-falso-cadastro-no-auxilio-de-600-ja-fez-67-milhoes-de-vitimas-saiba-como-se-proteger-24356996. Acesso em: 10 mai. 2023.

PROCON. Portal. Disponível em https://www.aen.pr.gov.br/Noticia/Procon-PR-alerta-para-golpes-envolvendo-repasses-do-governo-federal-familias. Acesso em: 10 mai. 2023.

SANTOS, Regiane Martins dos Santos. Comentários à Lei Geral de Proteção de Dados. Disponível em https://modeloinicial.com.br/artigos/crimes-virtuais. Acesso em: 25 set. 2022.

SERASA. Portal. Disponível em https://www.serasa.com.br/premium/blog/golpe-do-auxilio-brasil-como-identificar/. Acesso em: 10 mai. 2023.

TECHTUDO, Segurança. Disponível em https://www.techtudo.com.br/listas/2022/07/golpe-do-auxilio-brasil-tem-20-mil-tentativas-diarias-veja-como-funciona.ghtml. Acesso em: 10 mai. 2023.

GLOSSÁRIO DE TERMOS TÉCNICOS

Cavalos de Tróia: notificações sobre códigos maliciosos hospedados *online* e utilizados para furtar informações e credenciais.

Malware: termo abreviado para "software malicioso", refere-se a programas de computador desenvolvidos para causar danos, roubar informações ou obter acesso não autorizado a sistemas e dispositivos.

DOS: é uma forma de ataque que visa tornar um serviço ou recurso indisponível para os usuários legítimos, sobrecarregando ou saturando os sistemas ou infraestruturas alvo.

Phishing: técnica utilizada por criminosos para obter informações confidenciais, como senhas, números de cartão de crédito, por meio do envio de mensagens falsas que se passam por entidades confiáveis, como bancos ou empresas.

Phishing: [Financeiro]: notificações de casos de páginas falsas com intuito de obter vantagem financeira, em geral envolvendo bancos, cartões de crédito, meios de pagamento e *sites* de comércio eletrônico;

Phishing: [Outros]: notificações de páginas falsas sem objetivo financeiro direto, em geral envolvendo serviços de *webmail*, acessos remotos corporativos, credenciais de serviços de nuvem, entre outros.

Ransomware: um tipo de malware que criptografa os arquivos de um sistema, tornando-os inacessíveis ao usuário. O criminoso exige um resgate (ransom) para descriptografar os arquivos e restaurar o acesso.

Scan: engloba além de notificações de varreduras em redes de computadores (*scans*), notificações envolvendo força bruta de senhas, tentativas mal sucedidas de explorar vulnerabilidades e outros ataques sem sucesso contra serviços de rede disponibilizados publicamente na Internet.

Spyware: software projetado para monitorar atividades em um sistema, coletando informações pessoais.