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

O AVANÇO DOS CRIMES CIBERNÉTICOS E SEUS REFLEXOS NO ÂMBITO DO DIREITO BRASILEIRO

ORIENTANDA – ISABELA NEVES DA SILVA MARQUES
ORIENTADORA – PROFª. DRª. FÁTIMA DE PAULA FERREIRA

GOIÂNIA
2024/1

ISABELA NEVES DA SILVA MARQUES

O AVANÇO DOS CRIMES CIBERNÉTICOS E SEUS REFLEXOS NO ÂMBITO DO DIREITO BRASILEIRO

Artigo científico apresentado à disciplina Trabalho de Curso II, da Escola de Direito, Negócios e Comunicação da Pontifícia Universidade Católica de Goiás (PUC GOIÁS).
Prof. Orientador(a) – Dr.(a) Fátima de Paula Ferreira

GOIÂNIA

2024/1

ISABELA NEVES DA SILVA MARQUES

O AVANÇO DOS CRIMES CIBERNÉTICOS E SEUS REFLEXOS NO ÂMBITO DO DIREITO BRASILEIRO

Data da Defesa: ___ de maio de 2024

BANCA EXAMINADORA

_____

Orientador: Profª. Drª. Fátima de Paula Ferreira NOTA

_____

Examinador (a) Convidado (a): Profº. Dr.º Isac Cardoso das Neves NOTA

O AVANÇO DOS CRIMES CIBERNÉTICOS E SEUS REFLEXOS NO ÂMBITO DO DIREITO BRASILEIRO

ISABELA NEVES DA SILVA MARQUES[1]

RESUMO

Este trabalho abordará a questão dos crimes virtuais, conhecidos como cibercrimes, no ordenamento jurídico brasileiro, tendo em vista que o principal meio para prática de tais atos tem sido a internet, utilizada através de computadores, celulares, tablets, entre outros, pelos cibercriminosos. O objetivo deste estudo é compreender como o sistema jurídico brasileiro tem abordado esses delitos e quais são as medidas legais disponíveis para combatê-los, como por exemplo, a Lei Carolina Dieckmann e a lei 14.155/2021, que trata das invasões de dispositivos informáticos. Portanto, pelo trabalho exposto concluiu-se que há necessidade de um aperfeiçoamento no código penal e a criação de mais leis específicas para combate aos crimes virtuais, pois o índice de crimes na internet só vem se expandindo.

Palavras-chave: Cibercrimes, internet, cibercriminosos, lei Carolina Dieckmann.

INTRODUÇÃO

O presente trabalho procura abordar a problemática acerca dos crimes cibernéticos, tendo como foco a utilização da internet para a prática de tais crimes. Para isso, pretende-se analisar se as leis existentes possuem eficácia, bem como, punições adequadas para os infratores, além de meios para proteção para as vítimas. Os crimes cibernéticos, ou cyber crimes, ocorrem com maior intensidade, e ninguém está totalmente livre do risco de ser vítima, pois dados pessoais e bancários por exemplo, estão sendo hackeados e violados cada vez mais.

[1] Isabela Neves da Silva Marques Acadêmica do 10ª período do Curso de Direito da Pontifícia Universidade Católica de Goiás

Assim, este trabalho tem por objetivo problematizar o que leva o usuário a cair no golpe virtual, como os criminosos agem e os danos que podem ser causados as vítimas. Todavia, abordará alguns dos crimes mais comuns praticados na internet, como o estelionato, o crime contra a honra e a pornografia infantil, por exemplo. Objetivando os crimes que disparam na internet em razão dos avanços tecnológicos e meios criados pelos cibercriminosos para prática de tais condutas.

Acerca da problemática, várias pessoas estão sendo vítimas de roubos através de WhatsApp, sites enganosos, perfis falsos na internet, entre outros meios. Além disso, temos crimes que ferem a imagem e integridade das pessoas causando danos psicológicos e morais, como publicar fotos e vídeos sexuais de menores de idade na internet, na maioria das vezes com intuito de vender o conteúdo e se aproveitar disso para obter vantagem ilícita para si. Assim, esses diversos crimes vêm causando prejuízos tanto materiais, como psicológicos nas vítimas, tendo isso como um problema a ser resolvido.

Por fim, é preciso que todo crime mesmo que seja praticado na internet seja punido, aplicando as devidas normas e leis criadas para cada caso, como exemplo a Lei Carolina Dieckmann 12.737/2012, a Lei 14.155/2021 e a Lei de Stalking 14.132/21, e que o Código Penal Brasileiro venha se aprimorar junto com a evolução da tecnologia, para que todos os usuários possam utilizar a internet com mais segurança.

1. OS CIBERCRIMES

1.1. Conceito

A palavra cibercrime surgiu após uma reunião em Lyon, na França, de um grupo de nações denominada G8. Nessa reunião foram discutidos os crimes praticados via aparelhos eletrônicos, ou pela disseminação de informações através da internet. Esse grupo havia se reunido para estudar os problemas da criminalidade surgidos e promovidos pela internet (PERRIN, 2006, p.01).

A internet, por ser um instrumento de muita importância em toda globalização, tornou-se o meio de prática desses crimes, que são os seguintes: estelionato, crimes

contra a honra, pornografia infantil, fraude de identidades (onde informações pessoais são roubadas e usadas), roubo de dados financeiros ou de pagamento com cartão, entre outros.

De acordo com CASSANTTI:

> Toda atividade onde um computador ou uma rede de computadores é utilizada como uma ferramenta, base de ataque ou como meio de crime é conhecido como cibercrime. Outros termos que se referem a essa atividade são: crime informático, crimes eletrônicos, crime virtual ou crime digital. (CASSANTI, 2014, p. 03).

O autor, ao tratar do assunto, acrescenta: “Crimes virtuais são delitos praticados através da internet que podem ser enquadrados no Código Penal Brasileiro resultando em punições como pagamento de indenização ou prisão.” (CASSANTI, 2016).

Desse modo, os crimes virtuais ferem a dignidade das pessoas, e causam danos materiais, como roubos de dados pessoais e de dinheiro, além dos danos psicológicos.

O doutrinador ROSSINI, aduz que:

> [...] o conceito de “delito informático” poderia ser talhado como aquela conduta típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, praticada por pessoa física ou jurídica, com o uso da informática, em ambiente de rede ou fora dele, e que ofenda, direta ou indiretamente, a segurança Informática, que tem por elementos a integridade, disponibilidade a confidencialidade. (ROSSINI, 2004, p. 110.).

Portanto, os crimes cibernéticos são praticados através de todas as plataformas moveis, como celulares, tablets, computadores, e todas as formas digitais, e o criminoso pode ser qualquer um, basta que tenha o conhecimento tecnológico necessário.

1.2 A INTERNET NA GLOBALIZAÇÃO E NA PRÁTICA DE CIBERCRIMES

A internet mudou a vida dos seres humano, fazendo com que todos ficassem dependentes desse meio, sendo possível se comunicar a distância, realizar estudos, fazer pagamentos de cartões e boletos de forma online, dentre várias outras coisas, todos pelo meio digital.

A porcentagem de usuários que acessam a internet para seu uso pessoal e para o benefício próprio sempre foi grande. Todavia, não podemos nos esquecer daqueles que navegam esse meio para entrar na cabeça dos usuários e aplicar seus devidos golpes.

Todavia, destaca SILVA:

> O primeiro registro de delito com o uso de computador data de 1958, no qual um empregado do Banco de Minneapolis, nos Estados Unidos da América, havia alterado os programas de computador do banco, de modo a depositar para si as frações de centavos resultantes de milhões de movimentações financeiras. A primeira condenação por uma corte federal norte-americana deu-se em 1966, por alteração de dados bancários (SILVA, 2012, p. 28).

Computadores, celulares, tablets, sites, dentre outros recursos tecnológicos possuem os dados de todos que usufruem desses aparelhos tecnológicos, e, sabendo disso, os criminosos recorrem a estratégias de roubar seus dados, provocando possíveis assédios, falsidades ideológicas, chantagens, dentre outros crimes que competem a difícil identificação de quem cometeu o crime ou do que fazer após passar por uma situação dessas.

1.3. OS SUJEITOS NO CIBERCRIME

1.3.1. O CIBERCRIMINOSO – SUJEITO ATIVO

O cibercriminoso é todo aquele que pratica ações antijurídicas, através da internet, contra os usuários, e é julgado e sentenciado como qualquer outro criminoso. Essas pessoas não tem um certo perfil de padrão, e pode ser um formado em tecnologia da computação que geralmente chamamos de hackers ou de crackers, ou um usuário comum que, ao longo do tempo foi adquirindo recursos e experiências próprias para prática de tais atos.

Vale ressaltar que, apesar de qualquer pessoa poder praticar esse tipo de crime, os hackers são os que estão em maior porcentagem de prática, pois eles possuem uma experiência maior nesse ramo.

Contudo, conforme ANANIAS e WANDERLEY (2014, p.38), *hacker* não é o termo mais adequado, haja vista que a expressão inicialmente era usada pra se referir a um indivíduo com grande habilidade com computadores. Ainda, os autores trazem

que tanto para os especialistas no meio como a doutrina preferem se referir aos cibercriminosos como *crackers*, termo este que teria sido criado pelos hackers, para não serem confundidos com aqueles.

Os crackers possuem claramente intenções ilícitas, como roubo de senhas e espionagem (ANANIAS e WANDERLEY, 2014, p.38).

DIAS (2010, p.9) realiza uma colocação muito oportuna quanto ao sujeito ativo deste crime, dizendo que embora o perfil do cibercriminoso tenha sido romantizado e descrito como um gênio na área da informativa, computadores e afins, com um Q.I. acima da média, introvertido, antissocial, movido pelo desejo de superação da máquina, esse perfil evoluiu, fazendo surgir novas modalidades criminológicas de delinquentes, não tão jovens ou inteligentes, desprovidos de tecno-ética e movidos com o objetivo de extrair informações, usa-la ou vende-la.

1.3.2. VÍTIMA – SUJEITO PASSIVO

Assim como o sujeito ativo do cibercrime, o sujeito passivo não possui condições especiais. Desta maneira, qualquer pessoa pode ser vítima, seja ela uma pessoa física ou jurídica, individual ou coletiva, públicas ou privadas, bastando estar conectado a um sistema ou à rede mundial de computadores (DIAS, 2010, p. 12).

Dessa maneira, devemos nos atentar ao inserir nossos dados na internet, e procurar maiores conhecimentos e informações a tudo o que vamos fazer, pois qualquer um está sujeito a cair nesses golpes.

MOURA (2012, p.24) afirma que pesquisas sobre as vítimas dos cibercrimes são unânimes quanto a não confiabilidade de estatísticas. Acrescentando, MOURA (2012, p.24) aduz que:

> Na maioria dos casos a vítima sequer sabe que está sendo atingida pelos agentes. Quando descobrem – observe-se que há uma parcela que continua sem perceber que os crimes estão ocorrendo – preferem calar-se, arcando com os prejuízos sofridos, a estampar páginas de jornais e revistas, admitindo sua vulnerabilidade e perdendo credibilidade, como nos casos de grandes empresários e bancos.

Desta forma, como quaisquer pessoas podem cometer crimes no ambiente cibernético, qualquer indivíduo usuário da rede está sujeito a ser alvo e consequentemente poderá ser vítima (MOURA, 2012, p.24).

2. EXEMPLOS DE CRIMES CIBERNÉTICO

2.1 ESTELIONATO

O crime de estelionato se caracteriza quando uma pessoa tem o intuito de enganar alguém ou induzi-lo a cometer um erro, usando argumentos enganosos, para ter vantagem para si ou para outra pessoa.

Vejamos o que está disposto no artigo 171 do Código Penal:

> Art. 171. 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**.**

Todavia, o crime de estelionato tem como alvo o patrimônio das vítimas, podendo ser praticado tanto em contato pessoal no mundo físico, como virtualmente, que são os casos que mais vem crescendo no mundo, devido a facilidade que temos de acesso as tecnologias e a internet.

Vejamos o que nos ensina BITENCOURT (2019, p.1369): No estelionato, há dupla relação causal: primeiro, a vítima é enganada mediante fraude, sendo está a causa e o engano o efeito; segundo nova relação causal entre o erro, como causa, e a obtenção de vantagem ilícita e o respectivo prejuízo, como efeito**.**

Portanto, neste crime qualquer pessoa pode ser o criminoso e a vítima, já que não há um perfil padrão para ambos, basta que a pessoa aplique o golpe e a outra caia, gerando prejuízos e vantagens ilícitas sobre tal meio.

2.1.1. CLONAGEM DE CARTÃO

Um dos vários crimes de estelionato mais conhecido e comum atualmente tem sido a clonagem do cartão, onde basicamente o criminoso consegue roubar os dados do cartão, através de compras online em sites desconhecidos por exemplo, e assim obter acesso ao nome do cliente, data de validade e código de segurança, e com essas informações, ele pode criar a clonagem desses cartões, e utilizá-los para em qualquer loja tanto física quanto online, para realização de compras de produtos.

Conforme citado por NAKAMURA (2007, p.22):

> A transação eletrônica segura, utilizado no comercio de eletrônico, faz com que as lojas virtuais não tenham acesso ao número do cartão de crédito, o que poderia ser aproveitado para uma base de dados de seus clientes. Essa, na realidade, é uma característica importante para a segurança, pois o maior perigo dos incidentes envolvendo cartões de crédito está relacionado ao seu armazenamento.

As vítimas geralmente só percebem a tal conduta ilícita quando chega a fatura do cartão, ou quando chega as notificações de compras que não foram feitas por elas mesmo.

Outro método que os criminosos usam para clonar as vítimas é por meio de links enviados no e-mail ou então ligações solicitando informações pessoais ou financeiras, e que muitas vezes o cidadão acredita ser alguém do banco responsável da sua conta que esteja ligando, e fornece todos os dados que eles precisam.

Por isso que devemos ficar atentos onde inserimos os nossos dados bancários, se o site é seguro, se o link e4m que você abre é seguro, e se alguém com quem você conversa e passa seus dados é de confiança.

2.1.2. CLONAGEM DE WHATSAPP

A clonagem do whatsapp funciona assim: o criminoso entra em contato com a vítima, seja por ligação, ou por mensagem mesmo, se passando por alguma empresa conhecida ou por um organizador de eventos, ou ainda então por um parente da vítima, e oferece propostas ou pede um favor, solicitando que o mesmo indique um código de verificação que chega em seu SMS. A partir do momento que a pessoa informa seu código de verificação, o whatsapp já está clonado.

Diante de tais fatos, com a clonagem feita, o criminoso tem acesso a toda a vida da vítima, e pode fazer contato com todos seus parentes e amigos. A partir daí, eles começam a mandar mensagens pedindo empréstimos de dinheiro, seja para pagar contas, ou para comprar algo que extrema urgência.

A vítima confiando que tal pessoa é seu parente, ou amigo/conhecido, acaba caindo no golpe e mandando o dinheiro.

Atualmente, este crime virtual vem crescendo bastante, causando malefícios a sociedade, em que rege seus patrimônios e bens.

2.1.3. EMPRÉSTIMOS FALSOS

O golpe começa quando o criminoso entra em contato com a vítima, seja através de ligação, mensagem de whatsApp, e-mail ou por outras redes sociais. Geralmente, eles colocam anúncios divulgando seus empréstimos com juros baixíssimos, para atrair a atenção da vítima, e se passam como agentes do banco central ou como pessoas de alto padrão que tem capacidades financeiras de realizar todo tipo de empréstimo.

Os golpistas sempre miram em pessoas com baixas rendas mensais, e que não conseguem um crédito com o banco, e estão dispostas a qualquer acordo que vier para se livrar das suas dívidas.

Quando a pessoa aceita o empréstimo, os criminosos agem da mesma forma que os bancos, e coletam os dados da pessoa para cadastro e enviam um contrato para ser assinado por elas.

Assim que assinado, eles alegam que há um impedimento na liberação do dinheiro, e que é preciso pagar uma taxa de IOF (imposto sobre operações financeiras), para liberar o dinheiro. Ou então usam outros argumentos, como solicitar o pagamento do seguro antes de liberarem o crédito. Ademais, assim que é feito a transação da vítima para o autor, eles desaparecem e nunca mais se vê rastros do dinheiro novamente.

2.2. CRIMES CONTRA A HONRA

Com o avanço do mundo virtual, os indivíduos, através de exposições de imagens pessoais e privacidades violadas, passaram a tornar-se alvo e ter sua honra violada.

Podemos definir crimes contra a honra a calúnia, a injúria e a difamação. Eles estão contidos nos artigos 138 (calúnia), 139 (difamação) e 140 (injúria), do Código Penal.

No crime de calúnia, o autor atribui falsamente um crime a alguém, sendo essa informação falsa, e ferindo sua honra e reputação diante da sociedade. Isso acontece através da exposição na internet, com fotos, comentários, vídeos, entre outros.

Vejamos o que diz o art. 18 do código penal: “Caluniar alguém, imputando-lhe falsamente fato definido como crime: Pena - detenção, de seis meses a dois anos, e multa.’’

Além disso, o código prevê que, a calúnia contra pessoas já falecidas também está sujeita a punição, pois os parentes da pessoa caluniada, acabam se tornando as vítimas.

Portanto, qualquer pessoa pode ser o sujeito ativo e o passivo deste crime, já que não há perfil padrão para que se possa cometer estas ações.

Já no crime de difamação, não há necessidade direta de acusação associada a algum crime cometido, basta que seja uma acusação que atinja a sua honra. Todavia, a acusação pode ser verdadeira ou não, só é preciso que a pessoa que sofreu as ofensas se sinta atingido.

Sobre a difamação, o STF[2] define:

> A tipicidade do crime contra a honra que é a difamação há de ser definida a partir do contexto em que veiculadas as expressões, cabendo afastá-la quando se tem simples crítica à atuação de agente público, revelando-a fora das balizas próprias.
>
> (STF, Inq. 2.154/DF, Tribunal Pleno, rel. Min. Marco Aurélio, j. 17.12.2004).

E por fim, o crime de injúria, este se refere ao agente que atribui algo negativo em relação a vítima, ofendendo suas qualidades físicas e morais.

Um dos casos que mais ocorrem de injúria, é quando alguém insulta a mãe, esposa, ou filho de alguém, ferindo bastante a honra e o psicológico da pessoa.

Desse modo, dispõe o art. 140 do código penal:

> Art. 140 – Injuriar alguém, ofendendo-lhe a dignidade ou o decoro:
> Pena – detenção, de um a seis meses, ou multa.
> § 1º – O juiz pode deixar de aplicar a pena:
> I – quando o ofendido, de forma reprovável, provocou diretamente a injúria;
> II – no caso de retorsão imediata, que consista em outra injúria.
>
> § 2º – Se a injúria consiste em violência ou vias de fato, que, por sua natureza ou pelo meio empregado, se considerem aviltantes:
> Pena – detenção, de três meses a um ano, e multa, além da pena correspondente à violência.

[2] (STF, Inq. 2.154/DF, Tribunal Pleno, rel. Min. Marco Aurélio, j. 17.12.2004).

> § 3º Se a injúria consiste na utilização de elementos referentes a religião ou à condição de pessoa idosa ou com deficiência: (Redação dada pela Lei nº 14.532, de 2023).
> Pena – reclusão, de 1 (um) a 3 (três) anos, e multa. (Redação dada pela Lei nº 14.532, de 2023).

2.3. PORNOGRAFIA INFANTIL

A pornografia infantil é qualquer exposição relacionada a uma criança ou adolescente (de até 18 anos), para fins primordiais sexuais. É um ato criminoso que vem crescendo primordialmente na internet e está descrito no Estatuto da Criança e do Adolescente (ECA), no Código Penal, e na Convenção dos Direitos da Criança da ONU, de 1989.

O artigo 240 do Estatuto da Criança e do Adolescente, dispõe as seguintes condutas:

> Art. 240. Produzir, reproduzir, dirigir, fotografar, filmar ou registrar, por qualquer meio, cena de sexo explícito ou pornográfica, envolvendo criança ou adolescente: Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa. Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa.

Com o aprimoramento da internet, esse crime veio ganhando forças, principalmente com a criação da deep web, que é uma plataforma não muito comentada e conhecida pelas pessoas, e de complicado acesso, que possibilita a exposição desse crime por meio de sites relatados de “invisíveis”.

É por isso que as autoridades têm dificuldade em romper e acabar de vez com esse crime, já que o acesso a deep web é difícil e os réus se ocultam, por meio do anônimo.

Vale ressaltar que esse crime não é praticado somente por aqueles que sentem prazer em ver os conteúdos sexuais, más temos também aqueles que compram e vendem esses materiais pornográficos, para fins lucrativos.

Vejamos o artigo 241 do ECA: “Vender ou expor à venda fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente: Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa.”

A jurisprudência é bastante rigorosa quando se refere a condutas que envolvem a disseminação pela internet, assim entendeu o STJ:

> **Compete à Justiça Federal processar e julgar as ações penais que envolvam suposta divulgação de imagens com pornografia infantil em redes sociais na *internet*.** A jurisprudência do STJ entende que só a circunstância de o crime ter sido cometido pela rede mundial de computadores não é suficiente para atrair a competência da Justiça Federal. Contudo, se constatada a internacionalidade do fato praticado pela internet, é da competência da Justiça Federal o julgamento de infrações previstas em tratados ou convenções internacionais (crimes de guarda de moeda falsa, de tráfico internacional de entorpecentes, contra as populações indígenas, de tráfico de mulheres, de envio ilegal e tráfico de menores, de tortura, de pornografia infantil e **pedofilia** e corrupção ativa e tráfico de influência nas transações comerciais internacionais). O Brasil comprometeu-se, perante a comunidade internacional, a combater os delitos relacionados à exploração de crianças e adolescentes em espetáculos ou materiais pornográficos, ao incorporar, no direito pátrio, a Convenção sobre Direitos da Criança adotada pela Assembleia Geral das Nações Unidas, por meio do Decreto Legislativo n. 28/1990 e do Dec. n. 99.710/1990. A divulgação de imagens pornográficas com crianças e adolescentes por meio de redes sociais na internet não se restringe a uma comunicação eletrônica entre pessoas residentes no Brasil, uma vez que qualquer pessoa, em qualquer lugar do mundo, poderá acessar a página publicada com tais conteúdos pedófilo-pornográficos, desde que conectada à internet e pertencente ao sítio de relacionamento. Nesse contexto, resta atendido o requisito da transnacionalidade exigido para atrair a competência da Justiça Federal. Precedentes citados: CC 112.616-PR, DJe 1º/8/2011; CC 106.153-PR, DJ 2/12/2009, e CC 57.411-RJ, DJ 30/6/2008. CC 120.999-CE, Rel. Min. Alderita Ramos de Oliveira (Desembargadora convocada do TJ-PE), julgado em 24/10/2012.”

Assim, a pornografia infantil é um crime extremamente doloso, que não tem como intenção o dano material, tão somente, a exposição de fotos, vídeos, e conteúdos sexuais maliciosos, que envolvem a imagem das crianças e dos adolescentes.

3. O DIREITO BRASILEIRO E SUAS APLICAÇÕES PENAIS NO ÂMBITO CIBERNÉTICO

Como sabemos, o direito é um dos únicos meios para se combater o avanço dos crimes sejam físicos ou virtuais. Está contido no Ordenamento Jurídico Brasileiro várias normas e leis que são aplicadas em favor da internet e das redes sociais. Assim, podemos conscientizar-se que a internet não é um meio onde não há lei.

Porém, a legislação brasileira precisa ainda também evoluir bastante, pois há lacunas no âmbito judicial que precisam ser criadas, como leis específicas ao crime cibernético.

Contudo, é importante que o direito penal esteja sempre acompanhando os avanços tecnológicos e criando métodos para combate dos cibercrimes.

Pois, o meio virtual nunca deixa de se expandir, e os criminosos estão sempre procurando novos meios para cometerem novos crimes, e esperando brechas para acessarem e roubarem, sejam informações ou sejam dinheiro.

Como entende o autor ALEXANDRE ATHENIENSE (2004, p. 1):

> Entendo que as soluções legais a serem buscadas deverão objetivar a circulação de dados pela internet, controlando a privacidade do indivíduo sem cercear o acesso à informação. Neste sentido é necessário aprimorar nossas leis de proteção de dados, inclusive com a regulamentação da atividade dos provedores que controlam a identificação do infrator, bem como um maior aparelhamento das delegacias especializadas.

Portanto, é preciso que o ambiente virtual esteja regulamentado de leis penais, que regem ao combate do cibercrime. Vejamos a seguir algumas leis específicas contra alguns dos mais populares crimes virtuais.

3.1. Lei Carolina Dieckmann 12.737/2012

A Lei Carolina Dieckmann foi criada pela ex-Presidente da República Dilma Russeff, e foi dado esse nome em referência a atriz de televisão que teve seu computador violado e seus arquivos e dados roubados e vazados na internet, inclusive fotos íntimas suas foram espalhadas simultaneamente.

Por esta razão foi criada a referente lei, para proteção de dados de todos os usuários que ultilizam o meio eletrônico.

Ademais, muitos brasileiros dependem de seus celulares, tablets e computadores para armazenarem e guardarem dados, fotos, senhas de acessos e informações relacionadas a vida profissional e pessoal. E a partir disso, os cibercriminosos aproveitam para hackearem e terem acesso a esses dados.

Por isso é preciso que haja barreiras para garantia da privacidade dos indivíduos, como a criação dessa lei.

Assim destaca CARDOSO (2017, p. 09):

> A Lei 12.737/2012 criou, assim, novos tipos incriminadores, além de se caracterizar como a primeira lei a funcionar “como instrumento normativo destinado especificamente à tutela do bem jurídico no mundo virtual”. No entanto, alega que suas normas textuais não produziram grandes reformas no ordenamento jurídico, nem tampouco resolveram os problemas que o Direito enfrenta no cabível à temática.

Tal lei foi então, a primeira a punir crimes cibernéticos que destacam sobre a invasão de dispositivos informáticos, acrescentada no Código Penal Brasileiro nos artigos 154-A e 154-B, e altera a redação dos artigos 266 e 298.

Vejamos o que dispõe o artigo 154-A do Código Penal:

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
>
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.
>
> § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no **caput.**
>
> § 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
>
> § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
>
> Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.
>
> § 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidas.
>
> § 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:
>
> I - Presidente da República, governadores e prefeitos;
>
> II - Presidente do Supremo Tribunal Federal;

> III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou
>
> IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.

Portanto, a lei Carolina Dieckmann surgiu para punir os cibercrimes, como por exemplo a fraude e a invasão de privacidade, sendo um marco primordial civil da internet, e possuindo ferramentas suficientes para combates desses crimes digitais.

Por fim, ressalta ESTEFAM, (2020, p. 440):

> Com a tipificação do crime de invasão de dispositivo informático previsto no artigo 154-A do CP, a Lei nº 12.737/2012 reconheceu de forma pioneira a tutela de um novo bem jurídico-penal, a segurança informática, ladeando outros valores fundamentais que merecem a proteção do Direito Penal.

De modo pelo acima exposto, percebe-se que a criação dessa lei foi essencial para a segurança dos usuários em questão da sua privacidade, para que ela não seja violada.

3.2. Lei 14.155/2021

A lei 14.155/21 alterou o código penal em que diz respeito a invadir o dispositivo de outrem, situado no art. 154-A do Código Penal. Além disso, houve também alteração nos crimes de furto relacionados a fraude eletrônica, situados no art. 155, § 4º-B do Código Penal, e somente de fraude eletrônica no art. 171, § 2º-A do Código Penal.

Todavia, relata Alexandre Gonçalves Barreto:

> Destacamos a importância de bem diferenciar o crime de furto mediante fraude do delito de fraude eletrônica. A melhore maneira para isso é analisar o elemento comum a ambos: a fraude. No furto ela é utilizada pelo cibercriminioso com o fito de burlar a vigilância da vítima, facilitando a subtração. Desse modo, a vítima não entrega o bem por espontânea vontade. Já na fraude eletrônica, modalidade de estelionato, a fraude visa obter o consentimento da vítima que, ludibriada, entrega voluntariamente o bem. (BARRETOS, 2021, p.136).

Esta lei representou um marco muito importante ao combate dos crimes cibernéticos, além da lei Carolina Dieckmann.

Ela foi criada no intuito de tornar as penas mais graves que se direcionam ao crime de estelionato cometido de forma online, através da internet.

Assim, invadir um dispositivo eletrônico passou de um crime relativamente menos ofensivo, para um crime com penas relativamente mais severas. Vejamos como ficou o artigo 154-A do CP, após a criação da lei 14.155/21:

> 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.

Assim, não é preciso que haja a violação do mecanismo de segurança para ter acesso ao dispositivo. Todavia, é preciso somente a não autorização do responsável e o dolo para obter ou adulterar dados da vítima para que se configure um cibercrime.

3.3. Lei de Stalking 14.132/21

A lei 14.132/21 é conhecida como stalking, e foi sancionada pelo ex-Presidente da República Jair Bolsonaro em 31 de março de 2021.

Tal lei foi inserida no art. 147-A do Código Penal, para combater as perseguições através da internet, que interfiram na liberdade e privacidade das pessoas.

Para o italiano Marcello Adriano Mazzola, na obra em que analisa os “novos danos” da sociedade globalizada e pós-moderna:

> stalking é o comportamento de quem (stalker ou ‘caçador à espreita’) molesta um sujeito (vítima) por meio de atos persecutórios e/ou intimidadores, de forma obsessivamente repetitiva, deixando a vítima em estado de alerta e relevante preocupação, quando não em profunda angústia.

O crime é considerado comum, poise pode ser praticado por um. Quando a vítima for criança, adolescente, idoso ou mulher perseguida por razões do sexo feminino, a pena é aumentada a metade de 50%.

Este crime consiste em perseguir alguém, invadindo sua liberdade e colocando em risco sua integridade física e psicológica.

Segundo Zaniolo, a conduta de *stalkear* a vítima poderá ser:

> Um modo de violência no qual o sujeito ativo invade a esfera de privacidade da vítima, reiteradamente repetindo a mesma ação por maneiras e atos variados, empregando táticas e meios diversos: ligações telefônicas (celular, residência ou comercial), mensagens amorosas, telegramas, ramalhetes de

> flores, presentes não solicitados, assinaturas de revistas não desejáveis, recados em faixas afixadas nas proximidades da residência da vítima, permanência na saída da escola ou do trabalho, espera de sua passagem em determinado lugar, frequência no mesmo local de lazer, entro outros. (Zaniolo. 2021; p.299).

Portanto, a conduta do stalkear que cause um incomodo a vítima, já é considerada crime.

CONCLUSÃO

Concluímos que a internet vem sendo um meio em que os criminosos encontraram para aplicar golpes e ferirem a honra e integridade das pessoas. Com o avanço da tecnologia, vem ficando cada vez mais difícil combater esses crimes e identificar quem são os devidos autores. Por isso que é preciso que o código penal venha se aperfeiçoar juntamente com os avanços da internet, e seja criado mais leis específicas para o combate aos crimes cibernéticos.

O estelionato vem aumentando seu índice de vítimas cada vez mais, que caem no golpe do WhatsApp por exemplo, onde a pessoa acha que está conversando com algum parente e acaba enviando dinheiro para criminoso, ou então, a vítima coloca seus dados pessoais e bancários em sites criados especificadamente para golpes e acaba sendo clonado. O Sistema Penal Brasileiro deve ser mais rigoroso em razão desses golpes virtuais, tanto no âmbito judicial como policial, para que o número de vítimas usuárias da internet venha se diminuir.

Temos também a problemática dos crimes contra a honra, como exemplo acusar alguém a um crime que outro não cometeu, que está previsto no código penal artigo 138. A pornografia infantil também foi citada neste trabalho, que fere a honra e privacidade das crianças e dos adolescentes. Portanto, tais crimes não podem passar impunes, e a investigação da polícia deve sempre ser feita de maneira ágil e eficiente, para que os criminosos respeitem o direito que cada cidadão tem, de manter sua integridade e imagem diante da sociedade que vivemos.

Verifica-se, portanto, uma necessidade de uma legislação mais específica para tais crimes, como a criação de leis para cada crime citado de forma única, e o

aperfeiçoamento no sistema penal brasileiro, como punições mais graves e severas, a fim de evitar mais delitos, pois os crimes cibernéticos só crescem, juntamente com o avanço da tecnologia, causando danos morais, psicológicos e materiais nos usuários.

REFERÊNCIAS

ALEXANDRE JÚNIOR, J. C. **Cibercrime: um estudo acerca do conceito de crimes informáticos.** Revista Eletrônica da Faculdade de Direito de Franca, v. 14, n. 1, jun. 2019.

ANANIAS, Ricardo A. R. e WANDERLEY, Lucas F. **Delito Informático e a Lei 12.737/12 (Lei Carolina Dieckamnn)**. In: (Vários) Anais do IV Congresso De Ciências Jurídicas: Jurisdição, Estado e Cidadania e VII Encontro Científico do Curso de Direito. 2014. Disponível em: <consensusjuridico.com.br/anais/ANAIS2014.pdf>

ATHENIENSE, A. R. **Crimes virtuais, soluções e projetos de Lei**. DNT. [s.l.]. 29 out. 2004. Disponível em: <http://www.dnt.adv.br/noticias/direito-penal-informatico/crimes-virtuais-solucoes-e-projetos-de-lei/>. Acesso em: 27 nov. 2021.

BITENCOURT, Cezar Roberto. **Código Penal Comentado**. 10ª edição. Editora Saraiva Jur. 2019.

CASSANTI, Moisés de Oliveira**. Crimes Virtuais, Vítimas reais**. Rio de Janeiro: Brasport, 2014.

DIAS, Vera Elisa M. **A Problemática da Investigação do Cibercrime**. 2010. Disponível em <www.verbojuridico.net/doutrina/2011/veradias_investigacaocibercrime.pdf>.

MOURA, PÂMELA A. R. **Crime Cibernético E Seus Aspectos No Universo Jurídico**. 2012. Disponível em: <http://ftp.unipac.br/site/bb/tcc/tcc388a1273480aa73d54b0c9bb36ffff.

Nakamura, E. T.; Geus, P. L. **Segurança de Redes em Ambientes Cooperativos**. 1ª ed. São Paulo: Novatec, 2007.

ROSSINI, Augusto Eduardo de Souza. **Informática Telemática e Direito Penal**. São Paulo: Memória Jurídica 2004.

SANTOS, A. F. C. **O cibercrime: desafios e respostas do direito**. Dissertação (Mestre em Direito) – Universidade Autónoma de Lisboa, Lisboa 2015.

SILVA, Marcelo Mesquita. **Ação internacional no combate ao cibercrime e sua inflência no ordenamento jurídico brasileiro**. 2012. 107f. Dissertação (Mestre em Direito) – Universidade Católica de Brasília, Brasília 2012.

Zaniolo, Pedro Augusto. Crimes Modernos: **O impacto da tecnologia no direito**. - 4 ed. Salvador: Editora Juspivm, 2021.