RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

CRIMES CIBERNÉTICOS: ANÁLISE DA LEGISLAÇÃO CIVIL E PENAL VIGENTE NO BRASIL

CYBER CRIMES: ANALYSIS OF CIVIL AND CRIMINAL LEGISLATION IN FORCE IN BRAZIL

DELITOS CIBERNÉTICOS: ANÁLISIS DE LA LEGISLACIÓN CIVIL Y PENAL EXISTENTE EN BRASIL

Vanessa Cristina Dias Arruda[1], Marília Freitas Lima[2]

e4124578
https://doi.org/10.47820/recima21.v4i12.4578

PUBLICADO: 12/2023

RESUMO

A presente pesquisa avalia a regulamentação dos crimes cibernéticos, discorrendo acerca de algumas leis aprovadas no Brasil que tipificam atos como invadir computadores**,** roubar senhas**,** violar dados de usuários e divulgar informações privadas, discorrendo também acerca do moderno termo doutrinário, o estupro virtual. Desse modo, busca-se responder à seguinte questão: quais são as previsões jurídicas existentes no ordenamento jurídico brasileiro em relação aos crimes cibernéticos? Para tanto, foi utilizado o método de abordagem dedutivo, o método de procedimento monográfico e como técnica de pesquisa, a bibliográfica e a documental. A pesquisa tem como objetivo discutir as consequências dos crimes, perfil das vítimas, porcentagens dos crimes informáticos no Brasil e a proteção do direito de privacidade, com base nas alterações da legislação civil e penal vigente no nosso país, tendo como conclusão o dever de atualizações e modificações que assegurem o direito à privacidade e a prevenção de novos delitos virtuais, além da compreensão dos crimes cibernéticos e as leis que capacitam a proteção das vítimas.

PALAVRAS-CHAVE: Crimes Cibernéticos. Internet. Proteção de Dados. Legislação Brasileira.

ABSTRACT

The present research will evaluate the regulation of cyber crimes, discussing some laws passed in Brazil that typify acts such as breaking into computers, stealing passwords, violating user data and disclosing private information, also discussing the modern doctrinal term, virtual rape. In this way, we seek to answer the following question: what are the existing legal provisions in the Brazilian legal system in relation to cyber crimes? For this purpose, the deductive approach method, the monographic procedure method and the bibliographic and documentary research technique were used. The research will aim to discuss the consequences of crimes, profile of victims, percentages of computer crimes in Brazil and the protection of the right to privacy, based on changes in civil and criminal legislation in force in our country, having as a conclusion the duty of updates and modifications that ensure the right to privacy and the prevention of new cyber crimes, in addition to understanding cyber crimes and the laws that enable the protection of victims.

KEYWORDS: *Cyber Crimes. Internet. Data Protection. Brazilian Legislation.*

RESUMEN

Esta investigación evaluará la regulación de los delitos cibernéticos, discutiendo algunas leyes aprobadas en Brasil que tipifican actos como piratería informática, robo de contraseñas, violación de datos de usuarios y divulgación de información privada, discutiendo también el término doctrinal moderno, violación virtual. De esta manera, buscamos responder a la siguiente pregunta: ¿qué disposiciones legales existen en el ordenamiento jurídico brasileño en relación a los delitos cibernéticos? Para ello se utilizó el método de enfoque deductivo, el método del procedimiento monográfico y técnicas de investigación bibliográfica y documental. La investigación tendrá como objetivo discutir las consecuencias de los delitos, perfil de las víctimas, porcentajes de delitos informáticos en Brasil y la protección del derecho a la privacidad, a partir de cambios en la legislación

[1]Aluna do curso de Direito do 10° período do Centro Universitário de Goiatuba-UNICERRADO. Técnica em Investigação Forense e Perícia Criminal.
[2]Doutoranda no Programa de Pós Graduação em Sociologia e Direito - PPGSD/UFF. Mestre em Direito Público pela Faculdade de Direito da Universidade Federal de Uberlândia - UFU/MG. Docente no Centro Universitário de Goiatuba - UniCerrado/GO.

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

civil y penal vigente en nuestro país, siendo la conclusión la deber de actualización y modificaciones que garanticen el derecho a la privacidad y la prevención de nuevos delitos virtuales, además de la comprensión de los ciberdelitos y las leyes que posibiliten la protección de las víctimas.

PALABRAS CLAVE: *Delitos cibernéticos. Internet. Protección de Datos. Legislación brasileña.*

INTRODUÇÃO

A internet vem se mostrando bastante necessária, a comunicação acontece em questão de segundos, se tornando indispensável para vários meios, sejam eles o trabalho, estudo e até mesmo os crimes virtuais. Dessa maneira, a presente pesquisa analisa a legislação brasileira que versa sobre os crimes cibernéticos e a influência que essa legislação gerou sobre a criminalização dos crimes cibernéticos, analisando aqueles mais frequentes no Brasil, verificando a legislação criada e compreendendo a forma de reduzir e punir os crimes cibernéticos no Brasil. Dessa forma, busca-se responder ao seguinte questionamento: quais são as previsões jurídicas existentes no ordenamento jurídico brasileiro em relação aos crimes cibernéticos?

Diante disso, o objetivo geral é analisar a legislação brasileira que versa sobre os crimes cibernéticos e a influência que essa legislação gerou sobre a criminalização dos crimes cibernéticos. Já o objetivo específico do presente trabalho é expor os crimes cibernéticos mais comuns e a respectiva legislação brasileira, compreendendo como é possível punir os criminosos, bem como, qual é o juízo competente para analisar esses crimes no ambiente virtual.

O trabalho está dividido em três capítulos, o primeiro visa esclarecer a origem da Internet e como ela se tornou uma ferramenta tecnológica veloz e eficiente, mas, traz como ponto negativo a contribuição para novos e ardilosos crimes virtuais, exemplificando também a nomenclatura e a classificação dos crimes cibernéticos.

O segundo capítulo analisa os aspectos gerais dos crimes no âmbito virtual, sendo eles o perfil das vítimas, competência, finalidade do crime, tempo e lugar do crime e, a Teoria Dualista. Já o terceiro capítulo visa analisar a evolução da legislação brasileira com aprovação e edição das principais leis que punem os crimes virtuais, sendo elas a Lei Geral de Proteção de Dados e Lei do Marco Civil da Internet, bem como, a Lei Carolina Dieckmann.

A INTERNET E A POSSIBLIDADE DE CRIMES NO AMBIENTE DIGITAL

Ao ter um avanço significativo da tecnologia, especialmente em relação à Internet, foram predispostos progressos significativos para a integração social, da ciência, indústria e outros. Mas, simultaneamente, concorreu na origem de formas novas de degradação da população. Ao mesmo tempo que a internet executa um dos maiores transmissores da informação e do conhecimento, simultaneamente, gerou um ambiente de condutas desagregadoras e criminosas (Marra, 2019).

O surgimento da internet ocorreu em 1945-1991, na guerra fria. Os EUA produziram a primeira rede de internet, a Arpanet (*Advanced Research Projects Agency Network*), originada pelo Departamento de Defesa dos Estados Unidos (ARPA - *Advanced Research Projects Agency*), que ao

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

criar essa rede de comunicação, se prevenia dos ataques soviéticos, e proporcionava novas táticas de guerra. O primeiro e-mail enviado foi em 1965. O Brasil teve acesso à chegada da internet ao final da década de 80 (Diana, 2019).

A internet se originou e avançou apressadamente no meio social, originando novas áreas de pesquisas na área jurídica, requerendo do direito recursos que não estavam aptos a encarar (Cavalcante, 2011). Há pontos positivos e negativos sobre a tecnologia. O ponto positivo é a comodidade que a internet trouxe, e o ponto negativo são as condutas censuráveis ou condenáveis (Castro, 2003).

De certa forma, a Internet traz lados positivos e negativos, porém, à falta de denúncias pode ser um dos fatores que originarão mais crimes, pois, a partir disso os criminosos terão a sensação de facilidade em cometer crimes virtuais, devido à falta de punição. Segundo Santos *et al.,* (2017, p. 3) “Os crimes virtuais são cada vez mais comuns, porque as pessoas cultivam a sensação de que o ambiente virtual é uma terra sem leis”. Ainda segundo Santos *et al.* (2017, p. 7) “encontramos nos principais crimes virtuais: a pornografia infantil, fraude e golpes, estelionato, ameaça, entre outros, como aborda uma pesquisa feita pelo site Safernet”.

Devido à falta de denúncia e a demora de criações de leis especificas que incluam todos os crimes cibernéticos, e por muitas vezes sendo complicado identificar esses criminosos, a quantidade de crimes cibernéticos aumenta, sendo extremamente necessário para combater esse problema, a criação de mais leis especificas que tragam proteção e a diminuição desses crimes, e, um maior número de investimentos nos recursos de perseguição penal desses infratores.

De acordo com Matsuyama *et al.* (2017, p. 2), os crimes cibernéticos são condutas que contrariam a lei e que acontecem por meio de dispositivos eletrônicos que podem estar ou não conectados à internet, além de outras atividades criminosas em face de “equipamentos tecnológicos, sistemas de informação ou banco de dados”.

Há uma necessidade de mudança na legislação brasileira em relação aos crimes cibernéticos, pois, não havendo legislação específica para punir esse crime, há um aumento dos casos, como exposto por de Sousa Neto *et al.* (2014, p. 235) “A jurisprudência brasileira apoia a responsabilização de pessoas que efetuam crimes virtuais, porém, existem lacunas na lei e alguns criminosos poderão não ser condenados”.

Na doutrina não existe concordância sobre a nomenclatura adequada para descrever crime cibernético, havendo vários termos, entre eles está o e-crimes, crime digital, crimes eletrônicos, crimes virtuais, crimes informáticos, dentre outros (Matsuyama *et al*, 2017). Qualquer ato ilegal que se utiliza da tecnologia para práticas delituosas em sistemas, ou obtenção de dados não autorizados, podem ser consideradas crimes cibernéticos (Matsuyama *et al,* 2017).

No ano de 1960, infratores manipularam dados em computadores, os espionando e sabotando, assim cometendo abusos de forma ilegal nos seus sistemas, registrando os primeiros crimes cibernéticos, sendo difícil detectá-los pela tecnologia daquele tempo ser mais precária. Em 1980 foram descobertos e revelados vários atos criminosos com o uso da internet, sendo elas pirataria de programas, manipulação de valores nos caixas eletrônicos, abuso de telecomunicação, entre outros.

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

De acordo que as práticas dos crimes cibernéticos se intensificavam, ocasionaram as primeiras legislações que regularizavam a prática dos respectivos crimes (Nascimento, 2016).

Há várias nomenclaturas que reconhecem os *softwares* criminosos, como os *cookies*, que são pacotes pequenos de dados enviados de um *website* para o navegador do usuário, que registra informações das suas atividades, o criminoso ainda consegue dados como números de cartões de credito e senha; outra nomenclatura conhecida é o *Spywares,* que é um programa de espionagem que obtém informações sem o consentimento do computador do usuário, esses dados são enviados para outro usuário de rede anônimo (Nascimento, 2016).

Já os *Spammings* são programas que encaminham mensagens eletrônicas, principalmente publicitárias, que não foram solicitadas, havendo uma sobrecarga na caixa eletrônica, atacando a privacidade do utilizador do meio eletrônico, tendo grande potencial para ser instalados *cookies* espiões, que favorecem os crimes; os *Hoaxes* são *e-mails* que na maioria das vezes se passam por órgãos governamentais ou empresas, contendo conteúdos que provocam comoção, podendo eles serem religiosos, comovedor e sentimentais, sendo muito comum na internet, provocando o espalhamento das *Fake News*, sendo enriquecidos de vírus (Nascimento, 2016).

Os *Sniffer* são programas de espionagem semelhante ao *Spywares,* invadem os *hardwares* e coletam informações do usuário; o Cavalo de troia, um dos mais conhecidos é um programa de espionagem, que coleta informações, arquivos e senhas do computador do usuário, instalados ao abrirem arquivos recebidos, liberando para o criminoso controlar seu computador, dando a abertura para serem copiados ou excluídos quaisquer arquivos detectados no aparelho (Nascimento, 2016).

Já os *Backdoors* são objetos de projetos de programas defeituosos ou com falhas de fabricação enviados de forma culposa ou dolosa, tendo uma similaridade ao Cavalo de Troia; já os Vírus são doenças contagiosas que danificam todos os programas e configurações do computador. Depois de instalados, o criminoso terá acesso especificamente a todas as informações disponíveis no computador, podendo infectar outras repartições. Eles são encaminhados por *e-mails*, vídeos, músicas, CDs, USB, entre outros; e por fim, o *Worm* é um programa que se prolifera de um sistema para outro sem a interferência do usuário infectado; esse programa elimina arquivos do dispositivo (Nascimento, 2016).

ASPECTOS GERAIS DOS CRIMES

Os crimes cibernéticos têm sua classificação como puros e impuros. O crime cibernético puro invade o sistema computacional e seus componentes, como o *hardware* ou o *software*, bem como, os bancos de dados e o sistema informático (Matsuyama *et al,* 2017). No crime cibernético impuro o delito não é direcionado aos sistemas ou componentes, a utilização da internet é a ferramenta principal para execução do crime (Nascimento, 2016).

A outras especificações, sendo eles os crimes puros que o objetivo alvejado é o sistema e dados; os mistos que não visam atingir o sistema informático nem seus componentes, mas, a informática é a ferramenta essencial para a consumação do ato criminoso; e os comuns que também não visam atingir o sistema informático nem seus componentes, mas utiliza a informática como uma

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

ferramenta, porém, esse não é um meio indispensável, poderia utilizar outro para efetuar a ação (Castro, 2003).

A competência dos crimes cibernéticos, na grande parte dos casos, e também os crimes de racismo e pedofilia no ambiente virtual, são de responsabilidade da Justiça Federal, já os crimes contra a honra praticados virtualmente, são de competência da Justiça Estadual (Nascimento, 2016).

Quando uma pessoa é vítima de racismo ou ofensas, é preciso preservar todas as provas do ocorrido, pois no campo virtual as páginas podem ser alteradas a qualquer momento, o que pode gerar dificuldades nas investigações. Quando o crime virtual deixa indícios que fortificam em ilícitos materiais, é necessário a realização de uma perícia que analise todas as provas para comprovar a autoria e materialidade do crime (Nascimento, 2016).

Identificar os autores dos crimes cibernéticos é um trabalho árduo pelas autoridades policiais. Na maioria das vezes os autores são providos de experiência e intitulados pela comunidade cibernética como agentes delituosos na prática desses crimes. Tendo várias determinações, como: *Hacker* que para benefício próprio invade sistema do dispositivo, mas esses não comete conduta delituosa; *Cracker*, que utiliza sua experiência para prejudicar outrem, quebrando uma segurança invadindo; *Phreaker* que modificam internamente linhas telefônicas, fazendo ligações gratuitas e escutas clandestinas, sendo cometidas em anonimato dificultando que a polícia identifique tais agentes; *Carder* que são estelionatários que aproveitam de erros de segurança das administradoras de cartão de credito, criando programas para fazer compras com cartão de credito alheio (Rocha, 2013). Após o criminoso obter os dados dos cartões de créditos, ele os distribui no IRC's[3], com propósito de não ser localizado, possibilitando muitas pessoas terem acesso a esses dados, dificultando descobrir quem os subtraiu (Crespo, 2011).

A teoria dualista foi aplicada pelo legislador infraconstitucional, que separa o delito dos autores dos partícipes. O *login* e senha são mecanismos de proteção, que ao serem violados caracterizam elemento normativo do tipo. O crime dessa lei é considerado crime doloso (Scarmanhã *et al.,* 2014).

Assim, há uma dual finalidade não cumulativa. A primeira finalidade não cumulativa é a conduta da invasão de dispositivos informáticos, que viola indevidamente o mecanismo de segurança, para que os dados sejam destruídos, obtidos ou adulterados. Já a segunda conduta é a instalação de vulnerabilidades para obtenção de vantagens ilícitas, sendo ela efetuada também por meio da invasão. Se o agente dolosamente invade, analisa dados da vítima, mas não danifica, o fato é considerado atípico. Para cometer o fim especial do tipo, o agente deveria "quebrar" alguma segurança do aparelho, caso o aparelho não tenha essa segurança, a conduta não refletirá efeitos ao enquadramento penal (Rocha, 2013). A exibição do verbo invadir refere-se ao sentido de acessar, violar sem consentimento do proprietário do aparelho (Scarmanhã *et al,* 2014).

Em relação ao tempo e o lugar do crime cibernético, o Código Penal aborda a teoria da atividade para indicar o momento do crime, no campo virtual é completamente complicado examinar o exato

[3] IRC(Internet Relay Chat) é um protocolo de comunicação que foi utilizado para bate papo em tempo real e que permitia tanto conversas públicas quanto privadas. (ULTRADOWNLOADS, 2017).

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

momento da prática do crime, haja que no meio virtual há uma dissociação temporal, tendo capacidade de programar a execução de um crime virtual no tempo, podendo ser executados após um determinado e longo período depois de sua programação, pois cada sistema possui um relógio interno.

No campo virtual não há um espaço físico determinado nem geográfico delimitado, sendo necessário para constatar o crime efetuado constatar o local da informação para gerar uma ideia de território. O espaço virtual é denominado como ciberespaço", indicando a localização que gerou todo caminho de informações através da internet, podendo ultrapassar territórios, devido ao mundo estar se usufruindo da internet (Nascimento, 2016).

Em 2017, uma faixa de 978 milhões de consumidores de 20 países teve US$ 172 bilhões roubados por *hackers*, segundo *Norton Cyber Security* (Norton, 2018, p. 13). As vítimas sempre tendem a compartilhar perfis parecidos, sendo entusiastas de tecnologia que são rodeados de dispositivos mobile em casa e fora dela, porém, há um ponto cego quanto à segurança cibernética, usando quase sempre a mesma senha em diversas contas ou compartilhar suas senhas com outras pessoas (Convergencia Digital, 2018). Segundo um relatório da *Norton Cyber Security* o Brasil teve um prejuízo de US$22 bilhões após 62 milhões de pessoas serem afetadas pelos ataques cibernéticos em 2017, considerado o segundo maior país com grande número de casos de crimes cibernéticos, ficando somente atrás da China (UOL, 2018).

Cerca de 84% foram afetadas pelo crime cibernético em 12 meses. Em uma pesquisa com brasileiros, 34% de brasileiros dizem escrever suas senhas em papéis, 59% compartilham suas senhas, 24% usam as mesmas senhas, 83% se encontram preocupados que suas informações de dados bancários sejam roubadas, 18% compartilham suas senhas *online* de suas contas bancárias. Senhas que tem com frequência grande distribuição são de aparelhagens ligados a Internet domésticas, sendo 38% *laptops* com 36% e por fim, *desktops* com 37%. Proteção contra ameaças maliciosas é a maior preocupação sobre segurança *online* no Brasil, ficando em segundo lugar a proteção de identidade e privacidade (Convergencia Digital, 2018). No ano de 2018, o Brasil esteve no *ranking* de ataques cibernéticos em terceiro lugar, em relação à dispositivos conectados à internet, encontrando-se atrás da China e Estados Unidos, segundo Symantec (Jornal do Comercio, 2019).

A gravidade da pornografia infanto-juvenil é um grande problema no Brasil, precisando ser tratado de forma correta. Esse crime aumentou grandemente na internet, sendo que em 2009 era considerado um dos crimes mais cometidos no ambiente virtual (Pinheiro, 2009 *apud* MPF, 2018). Os arts. 240 e 241 do ECA – Lei nº 8.069/1990, alterados pela Lei nº 11.829/2008, tipifica esse crime de compartilhamento, posse, produção ou reprodução de pornografia infanto-juvenil (MPF, 2018).

Crianças e jovens são as vítimas que mais tem facilidade de sofrer ataques cibernéticos, pesquisa feita com estudantes de Curitiba-PR e região de 13 e 15 anos mostra que a maioria navega na internet sem acompanhamento dos pais, entrando em conteúdos privados a adultos e se encontrando com indivíduos que apenas conheceram de forma virtual (Drechsel, 2016). Houve uma alta de 109,5% no ano de 2018, de acordo com a associação SaferNet Brasil de denúncias de crimes na internet, havendo aumento nas queixas de crimes em relação as mulheres. Foram 133.732 queixas de crime em 2018, sendo os principais crimes cibernéticos registrados: pornografia infantil; apologia e

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

incitação a crimes contra a vida; violência contra mulheres; xenofobia; racismo; LGBTfobia; neonazismo; maus tratos contra animais; intolerância religiosa e tráfico de pessoas (Poder 360, 2019).

LEGISLAÇÃO ESPECÍFICA DO ORDENAMENTO JURÍDICO BRASILEIRO ACERCA DOS CRIMES CIBERNÉTICOS

Em 2018 foi aprovada a Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709, trazendo um item importante, que é o consentimento da pessoa, sendo possível requerer que sejam apagados determinados dados, bem como, haver a desistência da vítima em relação ao seu consentimento, compartilhar dados para outro produtor de serviços etc. A abordagem dos dados deve respeitar certas normas, sendo elas a finalidade e a necessidade, devendo esses serem acertados e comunicados a pessoa, antes de acessar os dados (Barbosa, 2020).

Além disso, a Lei n.º 12.695/2014, também chamada Marco Civil da Internet, foi editada. Ela regulamenta o uso da internet estipulando princípios e normas que garante uma elevada proteção aos seus usuários. Essa lei foi originada por meio de uma incorporação de diversos projetos semelhantes**,** que se fortaleceram principalmente pelas identificações de espionagem do Governo Norte Americano contra alguns países incluindo o Brasil (Nascimento, 2016).

A Lei nº 12.737/2012, lei Carolina Dieckmann como é referida, foi sancionada no dia 02 de dezembro de 2012. Essa lei alterou o Código Penal Brasileiro, tipificando os chamados delitos ou crimes informáticos, foi uma lei elaborada com a finalidade de solucionar os problemas ocasionados pela lacuna legislativa envolvendo o uso de meio cibernético (FMP, 2019).

A Lei Carolina Dieckmann ganhou esse nome após fotos da atriz serem expostas em maio de 2012, tendo uma grande discussão nacional (Caleffi, 2015). O grupo especializado da Delegacia da Repressão aos Crimes de Informática (DRCI) em conjunto com a Polícia Civil do Rio de Janeiro, com a ajuda de programas desenvolvidos encontraram os suspeitos, descobrindo que eles furtaram 60 arquivos do computador da atriz. Ao enviarem um *spam* para o computador, Carolina abriu, os criminosos, por meio de um programa específico mascarado enviado para o e-mail da atriz, permitiu que eles subtraíssem fotos, essas que possivelmente estavam localizadas na caixa de e-mail que foram enviadas pela atriz (Garcia, 2017).

Carolina Dieckmann teve 36 fotos pessoais de cunho íntimo divulgadas após *hackers* invadirem seu computador, além de ser chantageada pelo autor do crime que pediu R$ 10 mil reais para não expor suas fotos, ao negar pagar determinada quantia, suas fotos foram divulgadas (FMP, 2019). Suas imagens foram divulgadas por quatro *crackers* de São Paulo e Minas Gerais (GARCIA,2017).

No Brasil as leis demoram anos para serem aprovadas, mas pela pressão da mídia, após a ocorrência de fotos pessoais de cunho íntimo da atriz Carolina Dieckmann serem publicadas, após um *hacker* invadir seu computador, fez com que o processo de aprovação levasse apenas um ano para sua sanção. Subtrair dados pessoais já era crime antes desse acontecimento, porém, não havia norma que tratasse especificamente sobre o assunto (FMP, 2019). O MP paulista considera a origem da legislação como uma lei que avança amplamente na tipificação dos crimes cibernéticos, pois, antes da

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

lei ser originada havia uma interpretação livre no que se refere a punição dos contraventores (Caleffi, 2015).

A Lei nº 12.737/2012, acrescentou os artigos 154-A e 154-B ao Código Penal Brasileiro. O artigo, 154-A, estabeleceu o crime chamado “Invasão de dispositivo informático”, compreendendo a invasão de qualquer dispositivo informático de outrem. Sendo praticado quando violado o mecanismo de segurança, tendo objetivo de instalar vulnerabilidades para vantagens ilícitas, adulterar, destruir ou obter dados sem autorização do proprietário. Quem produz, oferece, vende ou envia dispositivos que permite a prática, também responderá pelo crime, a ação desse crime procederá mediante representação. Essa lei também alterou a redação dos artigos 266, em que os parágrafos 1º e 2º traz consequências para quem interromper, impedir ou dificultar os serviços de informação que sejam públicos e 298 que equipara cartões de crédito ou débito como documentos particulares, bem como, nas hipóteses de crimes de falsificação de documento, essas mudanças impactou o direito penal (FMP, 2019).

Nessa lei pode haver concurso de agentes, é considerado unilateral quando utilizam somente um computador e plurilateral quando usam dois ou mais computadores para a prática do crime, tendo a coautoria no caso da atriz já que foram 4 agentes de locais distintos. A tipicidade subjetiva é de dolo genérico, não admitindo modalidade culposa, já que os agentes têm a vontade livre e consciente de acessar dados das vítimas. A invasão de dispositivos informáticos é crime comum, podendo o sujeito ativo ser qualquer pessoa, e o sujeito passivo é qualquer pessoa física ou jurídica que possui dados informáticos. (Garcia, 2017).

O Código Penal não foi muito alterado pela Lei nº 12. 737/2012, especificamente, somente o que tipifica estabelecida conduta como crime é o art. 154-A. Assim, não há precisão da vítima ser dona do aparelho informático, exemplo disso, é a utilização de equipamentos em *lan house* pelas vítimas, constituindo um indiferente penal pelo que o aparelho deve estar ou não conectado à internet (Rocha, 2013).

A tutela do bem jurídico da liberdade individual e do direito a descrição profissional, bem como a pessoal é a finalidade dessa referida lei. Em seus efeitos o que mais contribuiu para surgimento de novos casos foi a vulnerabilidade das leis brasileiras, a criação dessa lei trouxe maior segurança jurídica e rigor penal. Há possibilidades de melhora da lei, quanto mais amplitude a lei tiver mais aplicável ela será. Um dos pontos negativos da lei é a punição, não sendo rígida o suficiente para evitar novos crimes (Garcia, 2017).

A agilidade da internet trouxe elevados benefícios se tornando um meio obrigatório para certa parte da população mundial. Essa facilidade, por vez, traz um risco desconhecido por diversos usuários, que ao utilizar impropriamente a internet e algumas vezes fazendo postagens e exposições desnecessárias, não observam o risco que pode surgir, acabam se tornando vítimas de diversos crimes, até mesmo contra a dignidade sexual (Nunes *et al,* 2019).

O primeiro crime caracterizado contra a dignidade sexual virtual, conhecido como estupro virtual ocorrido no Brasil foi no ano de 2017, no Estado do Piauí, onde uma vítima de 32 anos teve um termino não aceito pelo seu ex companheiro, na ocasião, este utilizou de imagens feitas quando a

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

vítima dormia para realizar o crime, exigindo a ela por meio de perfis falsos que o enviasse imagens e vídeos íntimos onde a vítima praticasse atos libidinosos, não se conformando com os registros**,** o ex companheiro obteve informações da vítima e de sua família, além de imagens com o filho da vítima para efetuar ameaças. Após toda a perturbação, a vítima procurou a Delegacia para declarar o ocorrido, o caso acarretou a prisão do indivíduo, que gerou uma grande repercussão, já que o tema estupro virtual é inédito aqui no país (Nunes *et al,* 2019)

Estupro virtual é um tema recente, conhecido doutrinariamente como sextorsão, tratando-se de atos que constrange alguém mediante a extorsão, adquirindo pornografia ou algum registro relacionado ao sexo, com o uso de chantagem psicológica afirmando expor informações ou registros íntimos das vítimas. Os tormentos provocados nas vítimas fazem que muitas vezes elas pratiquem as ações pedidas em troca da não exposição de sua intimidade, a grande parte dessas vítimas são mulheres. Surge assim diversos atos sexuais não desejáveis pelo medo da exposição, não sendo denunciado muitas vezes, trazendo exaustão psicológico e físico a vítima.

O conceito de estupro trazido no artigo do código penal 213°, só considera estupro os crimes que tragam intervenção do sujeito ativo, constrangendo a vítima para praticar ou aceitar que seja praticado o ato libidinoso, podendo ou não consistir em conjunção carnal. No crime de estupro virtual, há uma participação direta do agente sobre a vítima, mesmo não sendo de modo presencial, tendo a vítima realizado os atos libidinosos em si mesma, devido às ameaças, porém, há uma intervenção do sujeito ativo direto em relação a vítima. Há como provar se houve o consentimento da vítima pelo contexto das mensagens. Se os atos praticados forem feitos sem o consentimento da vítima será considerado constrangimento (Nunes *et al,* 2019).

Há uma necessidade analógica nesse tema, pois a análise estrita da lei não é suficiente para amparo de crimes recentemente gerados, sendo esses novos crimes frequentes no cotidiano. Porém, para o estupro virtual é indispensável a criação de um tipo penal ou aceitar a classificação desses crimes virtuais no crime de estupro, caso não tenha esse encerramento, esse ambiente de crimes continuará tendo a liberdade para criar versões de tudo que é exposto nas redes e compartilhar o que quiser, não tendo barreiras para pesquisas ou controle do que é exposto, ofendendo a liberdade de outrem (Nunes *et al,* 2019).

MÉTODO

Nessa pesquisa foi utilizada a técnica de pesquisa de documentação indireta, sendo ela bibliográfica, o método de abordagem foi dedutivo e o método de procedimento utilizado foi o monográfico, possibilitando a análise de dados confiáveis e atuais, tendo seu embasamento em doutrinas, legislação, artigos, livros e reportagens.

CONSIDERAÇÕES

Portanto, com a obtenção desses dados do artigo, torna-se possível a compreensão dos crimes cibernéticos e as leis que capacitam a proteção das vítimas. A internet trouxe não somente benefícios de uma melhor comunicabilidade, mas um grande aumento de criminalidade, a internet nem sempre

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

dá a capacidade de identificar e aplicar as medidas cabíveis aos agentes ativos que praticam os delitos virtuais, já que a maioria dos autores trabalha de forma anônima e cuidadosa, mas, algumas vezes são deixados rastros do criminoso, podendo processar e julgar o agente.

Desse modo, com a tecnologia que vem avançando rapidamente, o direito se encontra cada vez mais induzido a se modificar e arquitetar medidas que assegurem os direitos e dados dos cidadãos devido os novos obstáculos que se refletem com a imersão célere do ciberespaço na sociedade.

A internet gerou uma construção tanto no meio intelectual quanto na vida das pessoas, fazendo com que seu uso proporcione formas de organização social inesperados. Sem distinção de classe social ou econômica, as leis trazem em seus dispositivos a prevenção de novos delitos e eventuais novas técnicas de invasão e conturbação na navegação dos consumidores da rede mundial de internet.

Para proteger o sistema de invasões, é necessário proteção com algum programa antivírus atualizado, pois ele dificulta a invasão do sistema por terceiros, sendo ágil na hora de detectar e eliminar os vírus que forem encontrados no sistema. É preciso atenção nas visitas dos *sites*, principalmente analisar se é de confiança (Nascimento, 2016).

Graças às modificações na nossa legislação, há possibilidade de punição, que amparados por determinadas leis ou analogia utilizada para determinados casos, torna possível uma punição específica para criminosos que praticam crimes cibernéticos.

Destaca-se, ainda que a legislação garante o direito à privacidade, se tratando de direito fundamental pela Constituição Federal, sendo assim, toda atualização que amplie a legislação brasileira em face dos crimes cibernéticos contribuirá para responsabilização dos danos digitais causados pelos infratores, o incremento das leis citadas no trabalho prevê a defesa dos consumidores da internet, podendo assim utilizar e obter mercadorias e serviços de forma segura.

REFERÊNCIAS

BARBOSA, Mateus Israel Alves Cruvinel. **Crimes Virtuais a Evolução dos Crimes Cibernéticos e os Desafios no Combate.** Orientadora: Takeda, Tatiana de Oliveira**.** 2020. 24 f. TCC (Graduação) - Curso de direito, Escola de Direito e Relações Internacionais, PUC Goiás, 2020. Disponível em: https://repositorio.pucgoias.edu.br/jspui/handle/123456789/105. Acesso em: 14 mar. 2022.

CALEFFI, Renata. **Estratégias políticas de comunicação:** O papel do telejornal na construção legislativa brasileira (Lei Carolina Dieckmann, Lei Seca e Projeto de Emenda Constitucional para Redução da maioridade penal). Orientador: SOMMA NETO, João. 2015. 126 f. Dissertação (Mestrado) – Curso de Comunicação, Setor de Artes, Comunicação e Design, Universidade Federal do Paraná. Curitiba, 2015. Disponível em: http://hdl.handle.net/1884/37292.Acesso em: 16 mar. 2022.

CASTRO, Aldemario Araujo. A internet e os tipos penais que reclamam ação criminosa em público. **Revista de Direito Eletrônico**, Petrópolis, v. 1, n. 2, p. 41-51, 2003.

CAVALCANTE, Andrea de Fátima Araújo. **A atipicidade dos crimes cibernéticos no Brasil e a impunidade:** uma análise crítica. Orientadora: LIMA, Henriqueta Fernanda Chaves A. Ferreira. 2011. 76 f. TCC (Graduação) – Curso de Direito, FAVIP, Faculdade do Vale do Ipojuca. Caruaru. 2011. Disponível em: https://silo.tips/download/sociedadede-educaao-do-vale-do-ipojuca-sesvale-mantenedora-da-faculdade-do-vale--3. Acesso em: 10 mar. 2022.

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

CONVERGENCIA DIGITAL. Sessenta e dois milhões de brasileiros foram vítimas do cibercrime. **Convergência Digital**, 22 jan. 2018. Disponível em: https://www.convergenciadigital.com.br/Seguranca/Sessenta-e-dois-milhoes-de-brasileiros-foram-vitimas-do-cibercrime-47117.html?UserActiveTemplate=site. Acesso em: 19 set. 2022

CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. São Paulo: Saraiva, 2011.

DE SOUSA NETO, Cícero Alves; SANTOS, Matheus. **Crimes Cibernéticos**: Generalidades e Perspectiva da Legislação Brasileira. **Revista TRANSGRESSÕES CIÊNCIAS CRIMINAIS EM DEBATE**, v. 2, n. 1, p. 225-238, 2014.

DIANA, Daniela. História da Internet. **Toda Matéria**, 10 mar. 2019. Disponível em: https://www.todamateria.com.br/historia-da-internet/. Acesso em: 17 mar. 2022

DRECHSEL, Denise. Crianças e jovens são as principais vítimas dos crimes cibernéticos. **Gazeta do Povo**, 17 maio 2016. Disponível em: https://mwww.gazetadopovo.com.br/educacao/criancas-e-jovens-sao-as-principais-vitimas-dos-crimes-ciberneticos-8z9ydeu4llc4b9m0xmogg6o3o. Acesso em: 18 mar. 2022

EPSTEIN, Lee; KING, Gary. **Pesquisa empírica em direito**: as regras de inferência. São Paulo: Direito GV, 2013.

FMP. Lei Carolina Dieckmann: você sabe que o essa lei representa? **FMP**, 16 ago. 2019. Disponível em: https://blog.fmp.edu.br/lei-carolina-dieckmann-voce-sabe-que-o-essa-lei-representa/. Acesso em: 12 mar. 2022

GARCIA, Aline Tavares. **O direito à intimidade e a frágil privacidade da era digital:** uma análise sobre os crimes cibernéticos e a eficácia da lei Carolina Dieckmann. Orientador: CUNHA, Gláucio Fernando Barros. 2017. 63 f. Monografia (Graduação) – Curso de Direito, Universidade Federal do Maranhão. São Luís, 2017. Disponível em: http://hdl.handle.net/123456789/1651 Acesso em: 18 mar. 2022.

GIL, Antônio Carlos. **Métodos e técnicas de pesquisa social**. 6. ed. São Paulo: Atlas, 2008.

JORNAL DO COMERCIO. Brasil é o 3° em ranking de ataques cibernéticos. **Jornal do Comercio**, 27 fev. 2019. Disponível em: https://www.jornaldocomercio.com/conteudo/economia/2019/02/672396-brasil-e-o-3-em-ranking-de-ataques-ciberneticos.html. Acesso em: 10 mar. 2022

MARRA, Fabiane Barbosa. Desafios do Direito na Era da Internet: Uma Breve Análise Sobre os Crimes Cibernéticos. **Rev. Campo Jurídico**, barreiras-BA, v.7, n.2, p.145-167, jul./dez. 2019.

MATSUYAMA, Keniche Guimarães; Lima, João Ademar de Andrade. **Crimes Cibernéticos**: Atipicidade dos Delitos. UNIFACISA, Campina Grande, 2017.

NASCIMENTO, Natália Lucas. **Crimes Cibernéticos**. Fundação Educacional do Município de Assis – FEMA – Assis, 2016.

NORTON. **2017 Norton Cyber Security Insights Report - Global Results**. [S. l.]: Norton, 2018, p.13. Disponível em: https://www.nortonlifelock.com/us/en/newsroom/press-kits/ncsir-2017/Acesso em: 18 fev. 2022

NUNES, Karine Lopes; COSTA, Larissa Aparecida. O Surgimento de Um Novo Crime: Estupro Virtual. In: ETIC 2015: Encontro de Iniciação Científica do Centro Universitário Antônio Eufrásio de Toledo - ISSN 21-76-8498. Presidente Prudente, v. 15, n. 15, 2019. **Anais Eletrônicos [...].** Disponível em: http://intertemas.toledoprudente.edu.br/index.php/ETIC/article/view/7739. Acesso em: 09 mar. 2022.

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

PODER 360. ***Denúncias de crimes cibernéticos aumentaram 109,9% em 2018, diz associação.*** **Poder360,** 15 fev. 2019. Disponível em: https://www.poder360.com.br/justica/denuncias-de-crimes-ciberneticos-aumentaram-1099-em-2018-diz-associacao/. Acesso em: 20 fev. 2022

ROCHA, Caroline Borges. A evolução criminológica do Direito Penal: aspectos gerais sobre os crimes cibernéticos e a Lei 12. 737/2012. **Jus Navigandi,** Teresina, ano 18, n. 3706, 24 ago. 2013.

SANTOS, Liara Ruff dos; MARTINS, Luana Bertasso; TYBUCSH, Francielle Benini Agne. Os Crimes Cibernéticos e o Direito a Segurança Jurídica: Uma Análise da Legislação Vigente no Cenário Brasileiro Contemporâneo. UFSM-Universidade Federal de Santa Maria. *In:* 4° Congresso Nacional de Direito e Contemporaneidade, 8 a 10 de nov. 2017, Santa Maria, Rio Grande do Sul. 2017. **Anais eletrônicos [...].** Disponível em: http://coral.ufsm.br/congressodireito/anais/2017/7-7.pdf. Acesso em: 16 fev. 2022.

SCARMANHÃ, Bruna de Oliveira da Silva; NETO, Mário Furlaneto; SANTOS, Eduardo Lourenço. Invasão de dispositivo informático: aporte com a legislação espanhola. **Revista Em Tempo**, v. 13, p. 231-251, 2014.

ULTRADOWNLOADS. O que é IRC?. **Canaltech**, 26 jun. 2012. Disponível em: https://canaltech.com.br/entretenimento/O-que-e-IRC/. Acesso em: 19 fev. 2022

UOL. Brasil é o segundo país no mundo com maior número de crimes cibernéticos. **Uo**l, 15 fev. 2018. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2018/02/15/brasil-e-o-segundo-pais-no-mundo-com-maior-numero-de-crimes-ciberneticos.htm. Acesso em: 20 fev. 2022