doi.org/10.51891/rease.v8i11.7554

CRIMES VIRTUAIS: O AVANÇO DOS CRIMES ELETRÔNICOS E A EVOLUÇÃO DAS LEIS ESPECÍFICAS NO BRASIL

VIRTUAL CRIMES: THE ADVANCE OF ELECTRONIC CRIMES AND THE EVOLUTION OF SPECIFIC LAWS IN BRAZIL

Haian de Assis Lopes de Almeida[1]
Tamar Ramos de Oliveira[2]

RESUMO: Este presente artigo apresenta diversas informações, baseadas em artigos científicos, doutrinas e legislações vigentes no Brasil, sobre o tema de cibercrimes ou crimes virtuais. O estudo sobre o tema justifica-se na medida em que os crimes virtuais se tornaram cada vez mais frequentes na nossa sociedade, uma vez que a maioria da população mundial tem acesso à internet. A metodologia aplicada possui um aspecto descritivo e a abordagem utilizada será qualitativa. Têm como objetivo principal verificar os tipos de crimes virtuais no Brasil, suas possibilidades e limitações, demonstrando a dificuldade para punir e verificar os indivíduos que realizam tal conduta, por conta da dificuldade na obtenção de provas e na competência territorial. Busca evidenciar as legislações vigentes sobre o tema, como por exemplo a lei 12737/2012, também conhecida como lei Carolina Dieckmann, que trata das invasões de dispositivos informáticos e outros crimes como a falsificação de documentos particulares. para que assim a sociedade civil, tendo acesso, possa saber como reagir e quais cuidados tomar para ao menos minimizar os danos. Esclarecer a questão de um crime muito comum, porém pouco perceptível, que é o crime de stalking, onde recentemente foi publicada a Lei do Stalking (Lei nº 14132/2021), que tipifica o crime de perseguição, também conhecida pelo termo estrangeiro "stalking", alterando o dispositivo do Código Penal com a inclusão de penalidade de reclusão de seis meses a dois anos e multa. Infelizmente, o que ocorre de fato no Brasil é a extrema dificuldade de fazer uma subsunção do fato com a norma, ficando impunes a maioria dos criminosos virtuais.

Palavras-chave: Direito penal. Cibercrime. Direito Digital.

ABSTRACT: This article brings a lot of information, based on scientific articles, doctrines and legislation in force in Brazil, on the topic of cybercrimes or virtual crimes. Their main objective is to investigate the types of virtual crimes in Brazil and the possibilities and limitations of their regulation, demonstrating the difficulty in punishing and verifying individuals who carry out such conduct, due to the difficulty in obtaining evidence and territorial jurisdiction. To highlight the few legislations in force on the subject, such as the law 12737/2012, also known as the Carolina Dieckmann law, which deals with the invasion of computer devices and other crimes such as the falsification of private documents. so that civil society, having access, can know how to react and what precautions to take to at least minimize the damage. To clarify the issue of a very common, but barely perceptible crime, which is the crime of stalking, where the Stalking Law (Law nº 14132/2021) was recently published, which typifies the crime of stalking, also known by the foreign term "stalking", amending the provision of the Penal Code with the inclusion of a penalty of imprisonment from six months to two years and a fine. Unfortunately, what actually happens in Brazil is the extreme difficulty of subsuming the fact with the norm, leaving most cyber criminals unpunished.

Keywords: Criminal Law. Cybercrime. Digital Law.

[1]Discente do curso de Direito da Faculdade de Ilhéus, Centro de Ensino Superior, Ilhéus, Bahia
[2]Discente do curso de Direito da Faculdade de Ilhéus, Centro de Ensino Superior, Ilhéus, Bahia.

1 INTRODUÇÃO

Este presente artigo apresenta diversas informações, baseadas em artigos científicos, doutrinas e legislações vigentes no Brasil, sobre o tema de cibercrimes ou crimes virtuais. O estudo sobre o tema justifica-se na medida em que os crimes virtuais se tornaram cada vez mais frequentes na nossa sociedade, uma vez que a maioria da população mundial tem acesso à internet. A metodologia aplicada possui um aspecto descritivo e a abordagem utilizada será qualitativa. Têm como objetivo principal verificar os tipos de crimes virtuais no Brasil, suas possibilidades e limitações, demonstrando a dificuldade para punir e verificar os indivíduos que realizam tal conduta, por conta da dificuldade na obtenção de provas e na competência territorial.

Acredita-se que o aumento da prática criminosa virtual esteja diretamente relacionado ao aumento do uso da Internet pelas pessoas. Portanto, é fundamental para o bom desenvolvimento da "sociedade digital" compensar os prejuízos causados por esses criminosos.

Para que essa ideia se torne realidade, leis mais rígidas devem estar em vigor. É necessária uma regulação efetiva do crime virtual, levando-nos a refletir sobre as medidas de contingência que podem tornar a sociedade mais segura.

Não há dúvida de que a Internet é uma das maiores invenções do século XX. Desde o seu surgimento, abriu as portas para o desenvolvimento de novas tecnologias, e essas evoluções continuam até os dias de hoje, mudando nossas vidas e a forma como interagimos. Esse crescimento tecnológico, no entanto, além de proporcionar diversos benefícios, também facilitou a prática de delitos.

Os chamados crimes virtuais, ou crimes cibernéticos. Durante o enfrentamento da pandemia pela COVID-19, os ataques cibernéticos se tornaram constantes.

O Brasil está no epicentro de uma onda global de crime cibernético, ou cibercrime. O país é uma das maiores vítimas das fraudes bancárias online e malware financeiro, e o problema continua a se agravar. O número de ataques cibernéticos no país e as fraudes bancárias online cresceram muito ao longo dos últimos ano Todavia, grande parte da população brasileira ainda ignora a escala do problema. Os formuladores de políticas públicas começam só agora a reagir às ameaças, mas apenas de forma fragmentada. Para combater o crime cibernético de maneira eficaz, o Brasil necessita ampliar a discussão pública sobre o tema e principalmente capacitar os profissionais responsáveis pela perícia dos crimes virtuais, uma vez que em grande maioria são despreparados, somado ao fato de

que existe uma grande deficiência de ferramentas investigativas para esclarecer o que de fato ocorre no mundo virtual. Os legisladores, as agências de segurança, as empresas, as organizações da sociedade civil e os cidadãos precisam levar a questão muito mais a sério.

2 DESENVOLVIMENTO

2.1 Conceito, classificações e tipificações dos crimes virtuais

Da mesma maneira que surgiram diversos benefícios com a evolução dos computadores e da internet, surgiram também diversos crimes e criminosos especializados na linguagem informática, espalhados por todo o mundo. Tais crimes são chamados de crimes virtuais, digitais, informáticos, telemáticos, de alta tecnologia, dentre outras nomenclaturas.

É importante também citar o conceito de crimes virtuais talhado pela Organização para a Cooperação Econômica e Desenvolvimento da ONU: O crime de informática é qualquer conduta ilegal não ética, ou não autorizada que envolva processamento de dados ou transmissão de dados.

Se tratando da doutrina, alguns autores classificam os crimes virtuais como puros e impuros ou mistos. Os puros são as condutas que ainda não foram tipificadas, ou seja, necessitam de uma lei que crie os tipos penais específicos para a persecução das condutas. Já os impuros ou mistos são os tipos penais já existentes e que podem ocorrer no ambiente virtual.

Sendo assim, percebemos que não há um consenso sobre o que é considerado crime virtual, nem mesmo uma denominação aceita pela maioria, assim como não há legislação específica definindo o que é crime na rede. Desta forma, o Código Penal é utilizado como base para condenações que envolvam os crimes cibernéticos.

Os crimes virtuais podem ser classificados como próprios ou puros, e ainda podem ser classificados como impróprios ou impuros.

Nos crimes virtuais próprios, o sujeito ativo usa o sistema de computador do sujeito passivo e usa o computador como sistema técnico, como objeto e meio de cometer o crime. Tais crimes incluem não apenas o hacking de dados não autorizados, mas também toda interferência em dados informatizados, como hacking de dados armazenados em um computador, com ou sem a intenção de modificar, alterar, inserir dados falsos, ou seja, tocar diretamente no software do computador ou hardware que só pode ser executado por ou contra um computador e seus periféricos.

O chamado crime virtual impróprio refere-se ao crime cometido pelo uso de computadores, ou seja, o uso de máquinas como ferramenta para realizar atos ilícitos que afetem todos os interesses legítimos que foram protegidos. Crimes que já são tipificados, agora são realizados através de um computador e da rede, utilizando o sistema virtual e seus componentes como mais um meio para a realização do crime. Aqui não é essencial o uso do computador para a concretização do ato ilícito que pode se dar de outras formas para chegar ao fim desejado, como por exemplo a pedofilia.

A Internet passou a ser um dos meios de celebração de contratos, atualmente os contratos que são fechados desta forma, obedecem a alguns princípios como: Publicidade, vinculação, veracidade e não abusividade.

Por exemplo, no caso de contratos firmados por meio digital, o Brasil não possui legislação específica contra atos ilícitos cometidos por meio do mundo virtual, o que mostra os desafios no combate ao cibercrime. Há momentos em que se faz o uso do princípio da analogia como a única maneira disponível para impedir que os cibercriminosos fiquem impunes.

Podemos citar alguns exemplos de crimes que são utilizados como forma de analogia aos crimes virtuais, sendo eles: O crime de Calúnia, art.138 do Código Penal; Pedofilia, art. 247 da Lei nº 8.069/90 (Estatuto da Criança e do Adolescente); Difamação, art. 139 do Código Penal; Injúria, art.140 do Código Penal; Ameaça, art. 147 do Código Penal; Violação ao direito autoral, art. 184 do Código Penal; Estelionato, art. 171 do Código Penal; Apropriação indébita, art.168 do Código Penal; Dano, art.163 do Código Penal; Furto, art.155 do Código Penal; Crimes contra a propriedade industrial, art. 183 da Lei nº 9.279/96; Interceptação de comunicações de informática, art. 10 da Lei nº 9.296/96; Interceptação de E-mail Comercial ou Pessoal, art. 10 da Lei nº 9.296/96; Crimes contra software, Pirataria, art.12 da Lei nº 9.609/98.

No entanto, existem normas específicas que tratam desse tema, de forma que não abrange todo o campo de atuação dos cibercriminosos, o que representa mais um desafio à aplicabilidade do direito penal. Portanto, a estrutura dos tipos de crimes no ordenamento jurídico nacional ainda não é perfeita.

A Lei nº 12.737/2012 – Lei dos Crimes Cibernéticos, ou, também conhecida como, a Lei "Caroline Dieckmann", trouxe importantes alterações ao Decreto-Lei 2.848/40 – Código Penal brasileiro, ao passo que realizou a formalização e a tipificação de condutas delituosas no âmbito informático, constituindo os chamados "crimes cibernéticos.

A Lei nº 12.737/12 afeta o direito penal, pois acrescenta os artigos 154-A e 154-B ao Código Penal Brasileiro. Além disso, altera a redação dos artigos 266 e 298. A norma aborda a segurança em ambientes virtuais.

Atitudes como o uso indevido de informações pessoais e materiais, envolvendo a privacidade de pessoas na internet, sendo elas fotos ou vídeos, estão previstas na redação da Lei nº 12.737/12.

O artigo 154-A, nos remete a um crime chamado invasão de equipamentos de informática, que inclui hackear qualquer outro dispositivo virtual, como computador, smartphone, tablet, etc., conectado à Internet ou não.

Esta ação deve ser realizada em violação de um mecanismo de segurança com o objetivo de adulterar, obter ou destruir dados sem a autorização do proprietário do dispositivo. Esta regra também se aplica a qualquer instalação de uma vulnerabilidade (como um vírus) no dispositivo para explorar.

Quem produzir, oferecer, distribuir, vender ou divulgar programas de computador ou equipamentos que permitam essa prática também sofrerá as consequências do crime. A ação do delito será mediante representação, ou seja, o Ministério Público (MP) só fará denúncia a pedido do ofendido, a menos que o delito tenha sido cometido (direta ou indiretamente) contra a administração pública, ou seja, o município, governo estadual ou federal, e quaisquer empresas concessionárias de serviços públicos.

O texto acrescenta ainda os parágrafos 1º e 2º ao artigo 266, sujeitando às mesmas consequências do artigo a quem interromper, impedir ou dificultar os serviços públicos de informação. Além disso, a pena é dobrada quando o ato é realizado durante uma calamidade pública (circunstâncias excepcionais, como desastres naturais).

A pena para o crime de invasão de dispositivos é a detenção, de 3 meses a 1 ano e multa. Mas se forem causados prejuízos económicos à vítima, a pena é aumentada em 1/6.

Se o crime resultar na aquisição de conteúdos de comunicações privadas, segredos comerciais ou industriais, controle remoto de equipamentos ou dados confidenciais, se o fato não constituir crime mais grave, é punível com pena de reclusão de 6 meses a 2 anos e multa.

Neste último caso, a multa ainda é aumentada em 2/3 se os dados adquiridos forem transmitidos, divulgados ou comercializados. Por fim, a pena pode ser aumentada de um terço a metade se houver infração cometida contra as seguintes autoridades: o prefeito, governador ou presidente da república; o presidente do Supremo Tribunal Federal (STF); presidentes dos órgãos legislativos municipais, estaduais ou da União, como Senado Federal,

Câmara, Municipal, Câmara Legislativa; dirigentes máximos da administração municipal, estadual ou federal.

Em 2014, foi publicada a Lei Marco Civil da Internet (Lei nº 12.965/2014) que dispõe sobre os deveres e os direitos das pessoas que utilizam a internet, com objetivo de proteção do uso de dados pessoais dos titulares. A lei em destaque prevê como princípios que regulam o uso da internet no Brasil, enumerados no artigo 3º, dentre outros, o princípio da proteção da privacidade e dos dados pessoais, e asseguram, como direitos e garantias dos usuários de internet, no artigo 7º, a inviolabilidade e sigilo do fluxo de suas comunicações e inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial.

O artigo 10º, § 1º, que trata de forma específica da proteção aos registros, dados pessoais e comunicações privadas, é bem claro quanto à possibilidade de fornecimento de dados privados, se forem requisitados por ordem de um juiz, e diz que o responsável pela guarda dos dados será obrigado a disponibilizá-los se houver requisição judicial. Caso o responsável se recuse a fornecer os dados solicitados pelo juiz, poderá responder pelo crime de desobediência, previsto no artigo 330 do Código Penal.

Recentemente, a Lei de Perseguição (Lei nº 14.132/2021), que trata do crime de perseguição, também conhecido como termo estrangeiro "stalking", altera as disposições do Código Penal para incluir multa e 6 meses a 2 anos de reclusão.

As infrações relacionadas às leis de stalking abrangem ambientes físicos e digitais (cyber stalking), incluindo ameaças à integridade física e psicológica da vítima, invasão de privacidade e liberdade. A nova lei é oriunda do PL 1.369/2019, de autoria da senadora Leila Barros (PSB-DF).

Leila destaca que o avanço das tecnologias e o uso em massa das redes sociais trouxeram novas formas de crimes. Ela acredita que o aperfeiçoamento do Código Penal era necessário para dar mais segurança às vítimas de um crime que muitas vezes começa on-line e migra para perseguição física.

Antes, a prática era enquadrada apenas como contravenção penal, que previa o crime de perturbação da tranquilidade alheia, punível com prisão de 15 dias a 2 meses e multa.

De acordo com a nova lei, o crime de perseguição terá pena aumentada em 50% quando for praticado contra criança, adolescente, idoso ou contra mulher por razões de gênero. O acréscimo na punição também é previsto no caso do uso de armas ou da participação de duas ou mais pessoas.

2.2 Os crimes mais praticados

2.2.1 Pedofilia

A pedofilia é considerada crime e sempre causa muita agitação social, mas não é difícil de encontrar na internet fotos mostrando conteúdo pornográfico envolvendo menores e muitas vezes crianças, diante disso, um dos poucos delitos que possui sua ação na internet devidamente tipificada é a pedofilia, disposto no art. 241, II, do ECA.

O ECA, no art. 241, previa apenas a divulgação e publicação, por Internet, de imagens e fotos de crianças e adolescentes, cenas eróticas e explícitas. A Lei 11.829/08 ampliou muito os núcleos do tipo de penal, para abranger entre outras coisas, o ato de armazenar, oferecer, expor a venda e transmitir.

> Assim, o ECA estabelece que: Art. 241-A. Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático (como Internet), fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfico envolvendo criança ou adolescente (BRASIL,1990).

É importante observar que redes de computadores podem vincular vítimas a redes de pedofilia. Quando as crianças compartilham fotos com seus amigos ou colegas de escola, uma imagem pode acabar em uma rede de pedofilia. Alguém que visualiza a foto pode ser conectado a uma rede por meio da pessoa que a compartilhou ou quando a imagem foi postada publicamente em um blog.

Devido ao anonimato proporcionado pela internet, é difícil identificar os infratores. É importante notar que esse anonimato não é absoluto; é possível identificar criminosos escondidos atrás de uma tela de computador. Uma possibilidade é encontrar o endereço IP de dispositivos conectados à internet, como um roteador ou computador. Essas informações podem ser usadas para rastrear o computador que criou a atitude criminosa e identificar o criminoso.

No que diz respeito à prática da pedofilia virtual, vemos os pedófilos utilizarem ambientes virtuais para exteriorizar fantasias sexuais por meio de menores. A partir de então, cometerá infrações penais típicas do ECA.

2.2.2 Invasão de Privacidade

Muitas pessoas revelam prontamente informações pessoais na internet pensando que são privadas. No entanto, isso não é verdade, pois tudo na internet pode ser acessado por qualquer pessoa que saiba como fazê-lo. Essas informações podem ser usadas indevidamente

por criminosos cibernéticos para enganar pessoas inocentes. Muitos internautas criam perfis falsos nas redes sociais para coletar informações sobre pessoas sem o seu conhecimento. Essas, informações são posteriormente vendidas a pessoas com intenções maliciosas que podem colocar em risco a vida das pessoas. A comunicação on-line precisa de mais segurança, pois atualmente vivemos em uma época em que tudo pode acontecer devido à invasão virtual de privacidade.

Os dados e informações publicados na Internet são difíceis controle por causa da estrutura em que se baseia (interconexão entre computadores ao redor do mundo), é basicamente libertário. A informação se espalha extremamente rápido e atinge a maioria da população, por isso, a divulgação de informações é cada vez mais frequente, dados e fatos que precisam ser mantidos dentro dos limites da privacidade dos indivíduos.

Agravando a situação, o cibercrime é um dos negócios promissores na economia, por conta da negociação de dados privados.

Isso acontece, pois, as instituições estatais e privadas produzem redes de trocas precisas de informações, para ações de marketing direcionadas, ações de combate ao crime, criação de perfis na internet, dentre outros.

Então a lei precisa se adaptar as novas ideias criminosas que a intimidade das pessoas, a vida privada e as informações pessoais dos indivíduos suportam com o surgimento da internet e das novas ferramentas que toleram a troca de informações.

A inviolabilidade constitucional da residência pessoal e da esfera privada do indivíduo já não garante amplas proteções no tocante a autoridade sobre informações privadas.

A disseminação da Internet; a expansão da era da comunicação e da informação; proporcionou uma vantagem para o surgimento de métodos que tornaram o abuso de privacidade algo fácil e acessível. Portanto, há a necessidade de uma reorganização desse direito.

2.2.3 Crimes contra a honra

Honestidade e respeito são essenciais para os relacionamentos. Cada pessoa tem a obrigação de ser honesta com os outros e respeitar os direitos dos outros. Honestidade e respeito são valores importantes no mundo tradicional, mas são cada vez mais difíceis de manter na era digital moderna. A internet deu a muitas pessoas uma plataforma para espalhar fofocas e calúnias. Também deu a muitas pessoas uma plataforma para o bullying,

o que é uma forma de desrespeito. Além disso, as mídias sociais deram às pessoas uma maneira fácil de assediar outras online. As pessoas precisam aprender a ser mais respeitosas ao interagir na internet para que todos possam ficar felizes e confortáveis.

Cyberbullying é uma das formas mais comuns de desrespeitar os outros online. As pessoas costumam usar as mídias sociais ou e-mail para espalhar rumores e insultos sobre os outros. Isso faz com que o remetente e o destinatário se sintam melhor consigo mesmos às custas dos sentimentos de outra pessoa. Os caluniadores geralmente justificam suas ações com base em sentimentos feridos, mas isso não é desculpa para o cyberbullying. Todos merecem se sentir respeitados online, assim como na vida real. Infelizmente, algumas pessoas gostam de infligir dor emocional a outras por meio do cyberbullying, o que torna difícil parar sem leis mais fortes contra isso.

As plataformas de mídia social são outra maneira comum de desrespeitar outras pessoas online. As pessoas postam comentários negativos sobre outras pessoas ou tiram fotos delas e depois postam essas fotos online para que todos vejam. Muitos sites de mídia social têm regras contra esse tipo de comportamento, mas não há garantia de que todos seguirão essas regras ou que os sites as aplicarão contra todos que as violarem. Alguns usuários chegam ao ponto de criar contas falsas com o nome de outra pessoa para que possam interagir com seus próprios perfis e causar problemas para seus alvos sem revelar sua identidade. Não há limite para o quão longe algumas pessoas irão em sua busca de entretenimento às custas de outra pessoa, mas é preciso haver maneiras melhores de prevenir esses comportamentos do que confiar em usuários individuais e mods de sites para se policiar.

Honestidade e respeito são valores essenciais em qualquer sociedade, mas podem ser difíceis de manter online. As pessoas muitas vezes desconsideram suas obrigações morais ao interagir umas com as outras online; espalham mentiras e desrespeitam-se constantemente. Eles também tendem a ser menos autocontrolados ao interagir com formas digitais de entretenimento em comparação com formas tradicionais de entretenimento como literatura, teatro, arte e assim por diante, o que também adiciona outra camada de problemas para nossa sociedade.

A inviolabilidade da honra é direito fundamental protegido pela Constituição Federal em seu artigo 5°, inciso X. A honra é um patrimônio pessoal, está relacionada a qualidades físicas, morais e intelectuais de uma pessoa e sua proteção se justifica, vez que está

diretamente relacionada com o respeito, a aceitação e bom convívio social em um determinado grupo. (BRASIL, 1988)

Por se tratar de um crime virtual improprio, as condutas penais estão previstas nos artigos 130, 139 e 140, do Código Penal, sendo estes crimes comuns, que estipularam 8 tipos que são praticados pela Internet.

É o ato de difamar, caluniar ou injuriar alguém, ferindo a sua dignidade ou atribuindo um fato ofensivo a sua reputação.

Nesses crimes, os agentes utilizam diversos meios virtuais, como e-mail e redes sociais. Tais crimes estão se proliferando muito em ambientes sociais, especialmente em redes sociais que recentemente ganharam poder, devido ao ódio gratuito, preconceitos, preconceitos relacionados a gênero, cor e religião. É importante ressaltar que são crimes onde muitas vezes os agentes os fazem usando o anonimato, o que dificulta sua identificação.

2.2.4 Estelionato

A realidade virtual é uma forma de promover produtos e serviços. De longe, é o desenvolvimento mais significativo no campo do entretenimento desde o advento do cinema. Além disso, é uma ótima ferramenta para educação e treinamento. No entanto, a realidade virtual também pode ser usada como uma oportunidade para cometer fraudes.

Um sistema de realidade virtual cria um espaço virtual que dá aos usuários a impressão de que estão em um lugar diferente. Proporciona-lhes uma experiência longe de suas vidas reais. A realidade virtual é uma estratégia de marketing usada para fazer os produtos parecerem mais atraentes do que são. Também pode ser usado para treinar pessoas em situações perigosas sem colocá-las em risco. No entanto, existem alguns casos em que as pessoas foram enganadas pela realidade virtual e perderam seu dinheiro.

A tecnologia de realidade virtual tornou-se cada vez mais popular entre os jovens. O fato de ser acessível e fácil de usar torna a realidade virtual a escolha ideal para a cultura jovem de hoje. Os consumidores jovens tendem a confiar na realidade virtual sobre outros métodos de marketing por causa de seu realismo. Consequentemente, a RV ajudou a tornar muitos produtos mais atraentes para os consumidores jovens do que nunca.

O conceito de realidade virtual é tão poderoso que pode mudar a forma como os consumidores veem certos produtos e serviços. Por exemplo, quando lançados pela primeira vez, os cassinos adotaram a realidade virtual como um método para trazer jogadores para seus estabelecimentos para jogar online, mesmo que morassem longe de um no mundo real.

A capacidade de criar experiências virtuais permitiu que os cassinos criassem jogos que permitem que os jogadores experimentem jogos de azar sem arriscar dinheiro. Essa estratégia foi tão bem-sucedida que gerou enormes lucros para cassinos em todo o mundo, bem como opções de jogo mais seguras para jogadores que precisam de ajuda com problemas de dependência. No entanto, essa abordagem também permitiu que os cassinos enganassem os jogadores a apostar muito mais do que pretendiam.

A realidade virtual pode ser usada para fins educacionais e programas de treinamento de negócios, bem como entretenimento propósitos. No entanto, também pode ser usado para

atividades criminosas, como peculato e crimes cibernéticos. Alguns criminosos exploram vulnerabilidades em sistemas virtuais para roubar dinheiro ou dados de vítimas inocentes. Em alguns casos, os hackers criaram mundos virtuais inteiros preenchidos com bots de inteligências artificiais controlados por eles, essencialmente transformando seus sistemas em bancos onde ninguém pode acessar seu dinheiro a menos que siga suas regras.

A realidade virtual é uma ferramenta poderosa que pode ser usada para o bem ou para o mal, dependendo do como ele é implementado por usuários e criadores. Ela permite que os usuários experimentem coisas além do que eles atualmente têm acesso no mundo real, permitindo que as empresas ganhem novos clientes e cortem custos por meio de programas de treinamento e esquemas de desfalque.

Os estelionatários encontraram na internet um grande campo de atuação, pois é possível cometer os mais diversos crimes sem aparecer, ou correr o risco de ser preso em flagrante. Os criminosos inteligentes exploram o seu anonimato para enganar as vítimas e assim ganhar dinheiro, propriedades e ganhos pessoais com facilidade.

Uma das formas mais comuns de fraude no mundo virtual é Hackear os e-mails das vítimas, especialmente aqueles que têm o costume de verificar saldos e extratos em seus computadores.

Em tal situação, o criminoso encontra uma maneira de clonar uma página bancária online do usuário e forçá-lo a tentar acessá-la, saber que os dados inseridos serão interceptados por um terceiro mal-intencionado.

Dessa forma, os hackers podem subtrair valores altos em minutos sem sair de casa simplesmente hackeando o dispositivo ou clonando os dados bancários dos indivíduos.

Vale ressaltar que para que se configure estelionato, deve haver o emprego de um artifício ardiloso, obter vantagem ilícita, induzir a vítima ao erro.

2.3 Aspectos históricos

À medida que a tecnologia se desenvolveu após a Segunda Guerra Mundial, o mundo se viu na necessidade de comunicações mais rápidas e globais. Assim nasceu a Internet: um sistema que se desenvolveu e se aperfeiçoou nas últimas décadas para facilitar a comunicação e o acesso à informação. Portanto, qualquer pessoa com acesso a um dispositivo de internet pode usufruir dessa ferramenta. Devido a uma série de fatores, o mundo se vê como parte integrante do uso diário da tecnologia. Hoje, ingressamos em uma nova fase conhecida como a "Era da Informação", na qual os meios de comunicação atuais continuam apresentando enormes, avanços tecnológicos, conferindo importância e extrema relevância nas esferas social, econômica e política. No entanto, ao mesmo tempo em que a internet nos uniu e facilitou o dia a dia da população mundial, ela também possui suas próprias deficiências que abrem espaço para o cibercrime.

A Internet aprimorou-se no período histórico de 1971 a 1991, a Guerra Fria, em que as duas superpotências envolvidas (Estados Unidos e União Soviética) se dividiram em um bloco socialista e um bloco capitalista, uma luta pelo poder e pela hegemonia. O advento da Internet foi baseado em facilitar a troca de informações entre pessoas geograficamente distantes, a fim de simplificar as táticas de guerra de ambos os lados. O nome por trás da criação desta ferramenta básica é Joseph Licklider.

O Departamento de Defesa dos EUA apoiou pesquisas sobre comunicações e redes que podem ser parcialmente interrompidas em uma guerra nuclear. O objetivo foi divulgá-lo de tal forma que, se os EUA forem bombardeados, tal rede permanecerá ativa porque não há um sistema central e a informação pode viajar por caminhos alternativos até chegar ao destinatário. Assim, em 1962, a ARPA encomendou ao Randcorporatino (um comitê estabelecido em 1948) a tarefa de apresentar seu primeiro plano em 1967. Em 1969, a rede de comunicações militares foi denominada ARPANET (Advanced Search Project Agent Network). No final de 1972, Ray Tomlinson inventou o e-mail, que ainda é o aplicativo mais usado na NET. Em 1973, o Reino Unido e a Noruega foram conectados à rede, tornando-a um fenômeno global. Nesse mesmo ano, outra aplicação fundamental na Internet, a especificação do protocolo de transferência de arquivos FTP, foi publicada. Então, naquele ano, qualquer pessoa conectada à ARPANET poderia fazer login.

Originalmente, o crime cibernético se referia ao uso de um computador para cometer um crime. O termo foi usado pela primeira vez em 1960 e descreveu atos de espionagem e sabotagem baseados em computador. Ganhou popularidade na década de 1990 com o

aumento dos serviços bancários on-line, comércio eletrônico, mídia social e mensagens instantâneas. Hoje, o cibercrime é um fenômeno global potencialmente mais prejudicial do que os crimes tradicionais. É considerado o quinto maior negócio do mundo, depois das indústrias de armas e petróleo.

Para entender como o cibercrime afeta nossas vidas diárias, é importante saber quais tipos de crimes se enquadram nessa categoria. Os golpes de phishing são um método que os criminosos usam para obter suas informações pessoais. Os golpes de phishing ocorrem quando criminosos se passam por empresas respeitáveis criando sites falsos onde você insere suas informações de login. Outro exemplo é o malware, programas que exploram vulnerabilidades, no sistema operacional ou navegador do seu computador, para obter acesso aos seus dados. O malware então envia esses dados de volta ao servidor do criminoso para que eles usem como quiserem. Outras formas de crime cibernético incluem ataques de negação de serviço e ransomware, criptografando os dados de um usuário e exigindo um resgate por sua chave de descriptografia.

O crime cibernético pode causar danos em muitos níveis diferentes. Por exemplo, criminosos podem danificar sistemas de computador pertencentes a indivíduos ou organizações. Eles também podem afetar os mercados de ações adulterando determinados dados ou programas. Eles também podem ameaçar a segurança nacional ao comprometer sistemas governamentais que contêm informações confidenciais. Além disso, fraudes em jogos de azar online e lavagem de dinheiro também são exemplos de crimes cibernéticos que têm sérias repercussões para a sociedade em geral.

Para cometer crimes cibernéticos, os criminosos usam muitos métodos e ferramentas diferentes, incluindo computadores, dispositivos móveis, plataformas de mídia social e criptomoedas como Bitcoin. Além disso, eles usam spyware e várias ferramentas de hackers, como cavalos de Troia e keyloggers, para obter acesso não autorizado ao sistema de alguém. Métodos de engenharia social, como phishing, são essenciais para a maioria dos cibercriminosos, pois permitem obter informações cruciais sem a necessidade de conhecimentos técnicos. Além disso, alguns governos contratam hackers, conhecidos como hackers patrocinados pelo Estado para obter acesso a sistemas pertencentes a outros países.

Embora estejamos cada vez mais dependentes da tecnologia, devemos estar cientes dos diferentes tipos de crimes cibernéticos que existem hoje. Isso nos ajudará a tomar decisões informadas ao usar dispositivos e plataformas eletrônicos que possam colocar nossos dados em risco.

2.4 Dificuldades na obtenção de provas e competência

Crimes no ciberespaço tornaram-se cada vez mais comuns à medida que a internet se tornou uma ferramenta popular para comunicação e negócios. No entanto, a prevalência de crimes cibernéticos também dificultou a obtenção de provas nesses casos. Muitos criminosos aprenderam a evitar deixar rastros de seus crimes. Os desafios de investigar crimes cibernéticos são consideráveis. Para combater crimes virtuais, muitos países criaram agências de crimes cibernéticos. Um exemplo é a Europol, uma organização que é composta por 28 países europeus e é usada para combater o crime cibernético transnacional. A Europol também fornece aos países informações sobre grupos internacionais de crime organizado.

Muitos crimes cibernéticos são difíceis de investigar porque as evidências são intangíveis. Além da dificuldade em localizar criminosos, os investigadores também devem descobrir como obter as provas de que precisam para o seu caso. Alguns casos requerem equipamentos especializados para acessar e recuperar dados armazenados no espaço virtual. Esse equipamento pode ser caro e difícil acesso, portanto, a coleta de dados pode levar muito tempo.

As investigações acerca do tema, também enfrentam desafios porque os crimes cibernéticos transcendem as fronteiras geográficas. Como tal, muitas vezes estão sob a jurisdição de outros Estados. Esses Estados, na maioria das vezes, não podem compartilhar informações entre si ou coordenar seus esforços para investigar um crime. Consequentemente, os criminosos podem facilmente escapar da detecção, passando por brechas jurisdicionais.

O processo de investigação também é mais difícil porque os criminosos estão se tornando cada vez mais experientes em tecnologia, às vezes até mais do que as agências de investigações dos crimes cibernéticos. A aplicação da lei deve acompanhar os avanços tecnológicos para ficar a par das atividades criminosas online. Os Estados também precisam trabalhar muito para recrutar indivíduos com experiência em tecnologia que possam ajudá-los em seus esforços de investigação.

Em alguns casos, testemunhas e vítimas também não estão dispostas a cooperar, especialmente em casos onde ocorrem crimes cibernéticos públicos, como assédio online ou esquemas de fraude que afetam muitas pessoas ao mesmo tempo. A maioria dos indivíduos não querem se envolver em processos judiciais porque temem represálias do perpetrador ou repercussões na mídia em relação aos seus casos, tornando ainda mais difícil a obtenção de provas para consequentemente punir os criminosos antes que eles causem mais danos.

O crime online é um perigo sempre presente que ameaça constantemente a segurança de todos. No entanto, investigar esses crimes é difícil, pois as evidências são intangíveis e os criminosos experientes em tecnologia parecem estar sempre um passo à frente da lei. A maioria dos países ainda estão aprendendo a lidar com esses desafios, porém, sempre será necessária a ajuda das vítimas e testemunhas para determinar e punir os criminosos antes que causem danos em grande escala.

CONSIDERAÇÕES FINAIS

O presente artigo abordou acerca dos crimes virtuais, das suas tipificações e classificações, as dificuldades na obtenção de provas para o combate a este crime e na competência para julga-los, bem como os seus aspectos históricos. Como os demais tipos de crimes, os crimes virtuais foram aperfeiçoados com o passar do tempo, ao passo que a tecnologia evoluiu, os cibercrimes também evoluíram.

Em contrapartida, foram surgindo também legislações com o objetivo de punir os cibercriminosos, como por exemplo a Lei nº 12.737/2012, também conhecida como a Lei "Carolina Dieckmann", que tratou dos crimes de invasão de dispositivos informáticos, punindo atitudes como o uso indevido de informações pessoais e materiais, envolvendo a privacidade de pessoas na internet, sendo elas fotos ou vídeos. Não é possível deixar de citar também o Marco Civil da Internet, que dispõe sobre os deveres e os direitos das pessoas que utilizam a internet, com objetivo de proteção do uso de dados pessoais dos titulares. A lei em destaque prevê os princípios que regulam o uso da internet no Brasil.

Observou-se os crimes virtuais mais praticados, como por exemplo o crime de estelionato, que consiste na obtenção de vantagem ilícita, induzindo a vítima ao erro no ambiente virtual, muitas vezes hackeando os e-mails das vítimas, especialmente aqueles que têm o costume de verificar saldos e extratos em seus computadores. Outro crime bastante praticado no ambiente virtual são os crimes contra a honra, consistindo em difamar, caluniar ou injuriar alguém, ferindo a sua dignidade ou atribuindo um fato ofensivo a sua reputação na internet, sendo as redes sociais o principal meio de propagação desses crimes.

Além disso, foi destacado as dificuldades na obtenção de provas dos crimes virtuais, uma vez que muitos crimes cibernéticos são difíceis de investigar porque as evidências são intangíveis. Além da dificuldade em localizar os criminosos, os investigadores também devem descobrir como obter as provas de que precisam para o seu caso, onde na maioria das vezes, não contam com a colaboração das vítimas. Outra dificuldade apontada está na

Competência para julgar tais crimes, porque os crimes cibernéticos transcendem as fronteiras geográficas. Como tal, muitas vezes estão sob a jurisdição de outros Estados. Esses Estados, na maioria das vezes, não podem compartilhar informações entre si ou coordenar seus esforços para investigar um crime. Consequentemente, os criminosos podem facilmente escapar da detecção, passando por brechas jurisdicionais.

Por fim, a Internet e as novas tecnologias afetam e mudam tudo e todas as áreas da vida social. À medida que as redes sociais se tornam mais poderosas, a privacidade é cada vez menos valorizada. Como resultado, todo tipo de dados e informações pessoais circulam livremente no mundo virtual, expondo milhares de pessoas e tornando-as vulneráveis ao crime. Diante disso, é importante estar atento aos riscos que a Internet pode representar. Enfatizar que os usuários devem se proteger de sites questionáveis e usar a internet com sabedoria.

REFERÊNCIAS

MONTENEGRO, Bruno Picanço. **Direito e globalização: a necessidade da regulamentação do "mundo digital"** - em especial da assinatura digital e do monitoramento Conteudo Juridico, Brasilia-DF: 14 jan 2014, 07:15. Disponível em: <https://conteudojuridico.com.br/consulta/Artigos/38076/direito-e-globalizacao-a-necessidade-da-regulamentacao-do-quot-mundo-digital-quot-em-especial-da-assinatura-digital-e-do-monitoramento>. Acesso em: 4 jun 2022.

SENADO, **lei que criminaliza stalking é sancionada.** [S. l.], 5 abr. 2021. Disponível em: <https://www12.senado.leg.br/noticias/materias/2021/04/05/lei-que-criminaliza-stalking-e-sancionada>. Acesso em: 1 jun. 2022.

KAMINISKI, Omar. **A informática Jurídica, a Juscibernética e a Arte de Governar.** Revista Consultor Jurídico. 17 de julho de 2002. Disponível em: <https://www.conjur.com.br/2002-jul-17/informatica_juridica_juscibernetica_arte_governar>. Acesso em: 4 jun 2022.

CIBERCRIMINALIDADE: OS CRIMES CIBERNÉTICOS E OS LIMITES DA LIBERDADE DE EXPRESSÃO NA INTERNET. Orientador: PROF. MESTRE MARCELO DE SOUZA CARNEIRO. 2017. Monografia (Bacharelado em Direito) - Faculdade de Ensino Superior e Formação Integral de Garça, Garça-SP, 2017. Acesso em: 6 jun 2022.

NUCCI, Guilherme de Souza. **Manual de Processo Penal**. 2. ed. – Rio de Janeiro: Forense, 2021. Acesso em: 23 set 2022.

NUCCI, Guilherme de Souza. **Código penal comentado**. 21. ed. – Rio de Janeiro: Forense, 2021. Acesso em 23 set 2022.

SILVA JUNIOR, Reginald Vieira da. GENOVA, Edivaldo Waldemar. **Os desafios do direito penal frente aos crimes cibernéticos.** Revista Científica Multidisciplinar Núcleo do Conhecimento. 9 de dezembro de 2021. Disponível em:

‹https://www.nucleodoconhecimento.com.br/lei/crimes-ciberneticos›. Acesso em: 5 jun 2022.

CARDOZO, Alexandro Gianes. Competência nos Crimes Cibernéticos. **JusBrasil**, 2017. Disponível em: ‹https://agianes.jusbrasil.com.br/artigos/514359859/competencia-nos-crimes-ciberneticos›. Acesso em: 24 set 2022.

Lei Carolina Dieckmann: Saiba o que essa lei representa. **Fundação de Ensino Superior do Ministério Público**. 16 de agosto de 2021. Disponível em: ‹https://fmp.edu.br/lei-carolina-dieckmann-voce-sabe-o-que-essa-lei-representa/›. Acesso em: 24 set 2022.

VANIN, Carlos Eduardo. Propriedade Intelectual: conceito, evolução histórica e normativa, e sua importância. **Jusbrasil**. Disponível em: ‹https://duduhvanin.jusbrasil.com.br/artigos/407435408/propriedade-intelectualconceito-evolucao-historica-e-normativa-e-sua- 36 importancia#:~:text=A%20Propriedade%20Intelectual%20%C3%A9%20a,per%C3% ADodo%20de%20tempo%2C%20recompensa%20resultante›. Acesso em: 24 set 2022.

BRASIL. **Lei nº 14.132**, de 31 de março de 2021. Prevê o crime de perseguição; e revoga o art. 65 do Decreto-Lei nº 3.688, de 3 de outubro de 1941 (Lei das Contravenções Penais). Brasília, DF: Palácio do Planalto, 2021. Disponível em: ‹http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14132.htm. Acesso em: 22 de out de 2022›.

BRASIL. **Lei nº 12.965**, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Palácio do Planalto, 2014. Disponível em: ‹http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 22 de out de 2022›.

BRASIL. **Lei nº 12.737**, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Brasília, DF: Palácio do Planalto, 2012. Disponível em: ‹http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 22 de out de 2022›.

BRASIL. **Lei nº 2.848**, de 7 de dezembro de 1940. Código Penal. Brasília, DF: Palácio do Planalto, 1940. Disponível em: ‹http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm›. Acesso em: 22 de out de 2022.

BRASIL. **Constituição Federal**. Constituição da República Federativa do Brasil. Brasília, DF: Palácio do Planalto, 1988. Disponível em: ‹http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 22 de out de 2022›.

ASSIS, Rebeka. **Crimes Virtuais: Descubra quais são os 7 mais cometidos**. jusbrasil.com.br. Disponível em: ‹ https://rebekaassis.jusbrasil.com.br/artigos/784440112/crimes-virtuais-descubra-quais-sao-os-7-mais-cometidos›. Acesso em: 25 de out de 2022.

MORAIS, Lucas. **Ciberpedofilia: os crimes de pedofilia praticados através da internet**. conteudojuridico.com. Disponível em: ‹ https://conteudojuridico.com.br/consulta/Artigos/51597/ciberpedofilia-os-crimes-de-

pedofilia-praticados-atraves-da-internet#:~:text=Segundo%20Batista%20(2004)%2C%20fundador,caindo%20na%20rede%20dos%20ped%C3%B3filos.>. Acesso em: 24 de out de 2022.

DIREITO DIGITAL: A coleta e o tratamento de dados pelas plataformas digitais e a violação ao direito fundamental a privacidade. Orientador: PROF. ANA CAROLINA FIGUEIRÓ LONGO. 2020. Artigo Científico (Bacharelado em Direito) – Faculdade de Ciências Jurídicas, Brasília-DF. 2020. Disponível em: < https://repositorio.uniceub.br/jspui/bitstream/prefix/14919/1/Maria%20Beir%c3%b3%20-%2021602083%20OK.pdf>. Acesso em: 22 de out de 2022.

CRIMES VIRTUAIS E NOVAS MODALIDADES DE VIOLÊNCIA DE GÊNERO CONTRA A MULHER: A DIVULGAÇÃO NÃO CONSENTIDA DE IMAGENS ÍNTIMAS NA INTERNET. Orientador: PROF. DR. RAUL CARNEIRO NEPOMUCENO. 2019. Monografia (Bacharelado em Direito) – Universidade Federal do Ceará, Fortaleza-CE. 2019. Disponível em: < https://repositorio.ufc.br/bitstream/riufc/49210/1/2019_tcc_algguimar%c3%a3es.pdf>. Acesso em: 24 de out de 2022.

CRIMES VIRTUAIS: UMA ANÁLISE SOBRE A CARÊNCIA DE LEIS PARA COMBATER SUAS ESPECIFICIDADES. Orientador: PROF. THAMARA DUARTE CUNHA MEDEIROS. 2020. Artigo Científico (Bacharelado em Direito) – Universidade Presbiteriana Mackenzie, São Paulo-SP. 2020. Disponível em: < https://dspace.mackenzie.br/bitstream/handle/10899/29935/Gabriel%20Augusto%20Gon%c3%a7alves%20Lazzarini.pdf?sequence=1&isAllowed=y>. Acesso em: 25 de out de 2022.