PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS

ESCOLA DE DIREITO, NEGÓCIOS E COMUNICAÇÃO

NÚCLEO DE PRÁTICA JURÍDICA

COORDENAÇÃO ADJUNTA DE TRABALHO DE CURSO

ARTIGO CIENTÍFICO

CRIMES CIBERNÉTICOS

DIREITO DIGITAL E OS NOVOS PARADIGMAS DA INVESTIGAÇÃO CRIMINAL

ORIENTANDO (A) – GEOVANA XAVIER DE OLIVEIRA

ORIENTADOR - PROF. ME. EURÍPEDES CLEMENTINO RIBEIRO JÚNIOR

GOIÂNIA

2022

GEOVANA XAVIER DE OLIVEIRA

CRIMES CIBERNÉTICOS

DIREITO DIGITAL E OS NOVOS PARADIGMAS DA INVESTIGAÇÃO CRIMINAL

Artigo Científico apresentado à disciplina de Trabalho de Curso II, da Escola de Direito, Negócios e Comunicação, Curso de Direito, da Pontifícia Universidade Católica de Goiás (PUCGOIÁS).

Prof. (a) Orientador (a) – Me. Eurípedes Clementino Ribeiro Júnior.

GOIÂNIA

2022

GEOVANA XAVIER DE OLIVEIRA

CRIMES CIBERNÉTICOS

DIREITO DIGITAL E OS NOVOS PARADIGMAS DA INVESTIGAÇÃO CRIMINAL

Data da Defesa: ____ de _____ de _____

BANCA EXAMINADORA

_____

Orientador: Prof. Me. Eurípedes Clementino Ribeiro Junior Nota

_____

Examinadora Convidada: Profa.: ESP Rosângela Magalhães de Almeida Nota

SUMÁRIO

CRIMES CIBERNÉTICOS

DIREITO DIGITAL E OS NOVOS PARADIGMAS DA INVESTIGAÇÃO CRIMINAL

Geovana Xavier de Oliveira[1]

O presente artigo busca apresentar os principais crimes cibernéticos em espécie e suas características, com ênfase na recorrência de sua prática no Brasil. Foi apresentada a legislação pátria que versa sobre o tema, os principais meios de repressão e sanções aplicadas. O principal objetivo da pesquisa voltou-se para a exposição e avaliação dos principais meios de obtenção de provas digitais colhidas para apuração de autoria e materialidade delitiva. Diante das peculiaridades inerentes à esta modalidade criminosa, elencando as imprescindíveis inovações que recaíram sobre o Direito Penal e Processual Penal brasileiro. Realizou-se a pesquisa acerca das principais influências nestes delitos, apontando a importância da prevenção dos usuários e da modernização da investigação criminal, aliada aos avanços tecnológicos.

Palavras-chave: Crimes cibernéticos. Provas. Investigação.

[1] Acadêmica de Direito.

INTRODUÇÃO

Dentre as maiores conquistas tecnológicas, temos o advento da internet, que surgiu no século passado, inicialmente como um mecanismo estranho e inacessível para a maior parte das pessoas, e que hoje é a maior e mais comum rede de conexão mundial.

Discutir sobre os avanços tecnológicos e os impactos causados na sociedade em decorrência disso é inevitável atualmente, isso porque a tecnologia está presente no dia a dia da grande maioria das pessoas durante todo o tempo. Atualmente, praticamente todas as profissões se adequaram ao uso de mecanismos tecnológicos, o que revolucionou a sociedade como um todo. Além disso, a nova geração desde a infância já possui acesso à dispositivos tecnológicos, o que contribui para que seja cada vez mais acessível e inovador.

Com essa acessibilidade, a internet tornou-se também um ambiente perigoso, suscetível a prática de infrações penais, o que vem se tornando cada vez mais recorrente no mundo todo, apresentando inclusive um cenário preocupante no Brasil atualmente, tendo em vista as dificuldades enfrentadas na investigação criminal e no âmbito do judiciário brasileiro com relação a esses delitos.

Diante disso, foi realizada uma ampla pesquisa acerca do tema crimes cibernéticos, exemplificando os crimes informáticos em espécie mais recorrentes no Brasil, além dos tipos penais que foram inaugurados em virtude da crescente prática delituosa.

Foi apresentado o aspecto investigativo dos crimes cibernéticos, com ênfase na obtenção de provas digitais para apuração de autoria e materialidade desses crimes, sendo de extrema relevância para o cenário social e jurídico brasileiro, que vem enfrentando diversas adversidades em decorrência dessa prática delituosa.

Nesse sentido, foi realizada uma abordagem histórica do surgimento da internet, a crescente acessibilidade do uso de dispositivos tecnológicos,

apresentando uma análise do momento em que se tornou mais presente na cultura da população, se transformando o principal meio de comunicação, bem como identificando a partir de quando passou a representar uma ameaça à segurança dos usuários, despertando assim o olhar do Estado para essa problemática.

Procedeu-se uma pesquisa para apresentar quais foram os principais mecanismos utilizados para atingir o objetivo de fornecer segurança ao ambiente virtual, os desafios enfrentados inicialmente e os avanços de sua utilização.

Além disso, buscou apresentar os principais métodos, aliados à informática, para investigação no âmbito da criminalidade cibernética, quais foram as principais inovações tecnológicas implementadas e os principais desafios enfrentados e como o ordenamento jurídico brasileiro tem buscado sanar as falhas neste processo.

CRIMES CIBERNÉTICOS

1.1 CONCEITO, HISTÓRICO E CLASSIFICAÇÃO

1.1.1 Conceito

Diante do avanço da internet e principalmente do uso das redes sociais, a comunicação se tornou mais fácil, rápida e acessível para todos. Apesar dos inúmeros benefícios advindos da tecnologia, surgiu um novo foco de criminalidade no espaço virtual, e bem assim, a necessidade de haver uma definição acerca dessa nova prática, bem como uma apresentação teórica desses delitos.

Inicialmente, convém trazer à discussão o conceito de infração penal que paira na doutrina jurídica brasileira. Segundo Gonçalves e Estefam (2020, p. 261), *"Infração penal é um gênero que, em nosso ordenamento jurídico, subdivide-se em duas espécies: crime e contravenção penal."*

A primeira espécie, possui uma ampla conceituação doutrinária, mas de modo brevemente apresentado por Nucci (2019, p. 219), os conceitos de crime em sentido material e formal corresponde a:

> "Material: é a concepção da sociedade sobre o que pode e deve ser proibido, mediante a aplicação de sanção penal. É, pois, a conduta que ofende um bem juridicamente tutelado, merecedora de pena. Esse conceito é aberto e informa o legislador sobre as condutas que merecem ser transformadas em tipos penais incriminadores. Como ensina Roxin, "o conceito material de crime é prévio ao Código Penal e fornece ao legislador um critério político-criminal sobre o que o Direito Penal deve punir e o que deve deixar impune".
>
> Formal: é a concepção do direito acerca do delito, constituindo a conduta proibida por lei, sob ameaça de aplicação de pena, numa visão legislativa do fenômeno. Cuida-se, na realidade, de fruto do conceito material, devidamente formalizado."

A segunda espécie, denominada contravenção penal, se distingue somente no campo da pena a ser aplicada à conduta tipificada, sendo que esta espécie abrange tão somente os delitos chamados de "crimes de menor potencial ofensivo" em razão da pena cominada em seu preceito secundário.

De maneira sucinta, não sendo o objeto deste artigo adentrar debate acerca de entendimentos doutrinários da conceituação de crime e contravenção penal, nota-se que o conceito de infração penal, em uma interpretação ampla,

representa a resposta estatal ao clamor social pela busca do sentimento de justiça, sendo que, havendo uma regulamentação positivada acerca da reprovabilidade de uma conduta, traz maior sensação de confiança à sociedade de modo geral, de que existem consequências para atos praticados em desconformidade com a lei, de maneira que haverá prejuízo concreto ao agente, tentando fazer com que de certa forma “o crime não compense”.

Partindo desse pressuposto, adequando ao ambiente virtual, chega ao ordenamento jurídico e à doutrina os denominados crimes virtuais. Em uma rasa análise primordial, apresenta-se como infrações penais perpetradas por intermédio da rede mundial de computadores.

Por se tratar de uma modalidade relativamente nova, não há um único conceito e nomenclatura definidos, sendo muito abrangente. Nesse sentido, Maia *apud* Silva (2017, p. 31):

> “Existem, por exemplo, muitos nomes para denominação dos crimes cibernéticos, de tal forma que não existe uma nomenclatura sedimentada acerca do seu conceito. De uma maneira ou de outra o que importa não é o nome atribuído a esses crimes, uma vez que o que deve ser observado é o uso de dispositivos informáticos e a rede de transmissão de dados com o intuito de delinquir, lesando um bem jurídico. Além disso a conduta deve ser típica, antijurídica e culpável.”

Algo essencial para o conceito desse tipo de crime é que os crimes de informática são condutas descritas em tipos penais realizadas por computadores ou contra computadores, sistemas de informação, ou dados nele armazenados (CASTRO, 2003, p. 01).

Em outras palavras, o indivíduo poderá utilizar-se do dispositivo tecnológico como **meio** para praticar um ilícito penal diretamente contra alguém ou algo, como por exemplo lesar o seu patrimônio; por outro lado, poderá atacar diretamente o dispositivo eletrônico, buscando atingir sistema informático ou dados nele contidos.

Em virtude do alcance global das conexões virtuais, é inevitável a exposição de todos os usuários, tanto que mesmo em caso de o indivíduo optar por não se sujeitar ao uso das redes informáticas, os mais simples exercícios de cidadania submetem toda a população à integração de uma rede de dados, como

por exemplo os sistemas informáticos da Secretaria de Segurança Pública, onde constam os dados de identificação de toda a população, sob controle estatal.

Embora haja um reforçado sistema de segurança implementado para garantir que não ocorrerá um ataque criminoso, tudo que consta no mundo digital pode ser acessado e, inclusive, simplesmente desaparecer do plano virtual a qualquer momento, a depender do grau de gravidade da invasão sofrida.

Dentro do aparato do direito digital, diversos são os bens jurídicos tutelados, desde o direito à privacidade à proteção da vida. Desse modo, todo bem jurídico lesado através da internet e por dispositivo informático, está englobado no sentido de crime cibernético, partindo do pressuposto da utilização da tecnologia como meio para prática criminosa, bem como em casos em que sistemas de informação são lesados pela incidência de delitos.

Acerca da diferenciação entre os crimes com relação ao meio utilizado e quanto ao objeto atingido, será realizada posterior análise quanto à classificação.

1.1.2 Histórico

A humanidade passa por uma constante evolução tecnológica há séculos, sendo que desde a criação dos primeiros dispositivos informáticos, ocorrem avanços que caminham cada vez mais para a modernização destes dispositivos, bem como para promover acessibilidade a todos.

Dentre as modernizações tecnológicas, a internet foi um dos marcos mais importantes da evolução social. O advento dessa tecnologia na sociedade subsidiou a criação de diversos mecanismos, principalmente de comunicação, que transformaram de forma permanente as relações sociais. Nesse sentido:

> “Assim decolou a internet, no auge do processo de barateamento das comunicações, hoje vista como um meio de comunicação que interliga dezenas de milhões de computadores no mundo inteiro e permite o acesso a uma quantidade de informações praticamente inesgotáveis, anulando toda distância de tempo e lugar.” (FURLANETO NETO; GUIMARÃES, 2002, p.2).

A tecnologia surge de forma tímida e um pouco estranha para a maior parte das pessoas, apresentando-se inicialmente como algo muito abstrato e inacessível. Com o passar do tempo, de repente, têm-se a internet na palma da mão, com um alcance que parecia inimaginável por meio de um simples toque de tela.

Com o passar dos anos, constatou-se a incidência de práticas criminosas em âmbito virtual, e embora não haja a definição exata de qual conduta inaugurou a prática criminosa em âmbito virtual, é fato que, conforme os usuários passaram a dominar a ciência computacional, surgiram as invasões a dispositivos, que se assemelham aos denominados *"hackers"* atualmente.

A natureza dos delitos perpetrados virtualmente foi se alterando de acordo com a adesão dos usuários às redes sociais e a modernização tecnológica.

Atualmente existe o mercado virtual, que possibilita a compra e venda por meio de sites. Além disso, através do Internet Banking, é possível acessar a conta bancária e realizar transações de forma digital através do celular ou outo dispositivo eletrônico.

Diante dessa acessibilidade, exsurge a prática de estelionato virtual, um dos crimes virtuais mais recorrentes, que se dá em virtude da confiança do indivíduo para com quem está realizando o contato de forma virtual, e não se dando conta do risco de estar se envolvendo em uma ação criminosa, acaba realizando pagamentos à terceiros de má fé.

Ademais, surgiu também como uma das primeiras práticas criminosas virtuais, a pornografia infantil, de modo que passou a ser comercializado virtualmente conteúdo que fere a dignidade sexual de crianças e adolescentes.

Contudo, embora existam registros de algumas condutas criminosas praticadas em meio eletrônico, o despertar das autoridades para a incidência dessas condutas foi a longo prazo. Segundo Jesus e Milagre (2015, p. 23), o Brasil passou a tratar e se preocupar com o tema nas últimas duas décadas. Hoje, o país é o quarto do mundo com o maior número de ameaças virtuais.

Diante disso, a partir da constatação dos altos índices de criminalidade virtual no país, surgiu para o Direito a necessidade de regulamentar essa prática,

preocupando-se em trazer inovações legislativas e, além disso, dar um novo paradigma à investigação criminal de modo geral. Essa foi e ainda é uma das maiores dificuldades, considerando que a precariedade da estrutura investigativa da polícia brasileira, que ainda vem buscando se adequar, se espelhando no formato internacional de investigação e colheita de provas digitais.

1.1.3 Classificação

A doutrina brasileira vem buscando estabelecer uma classificação entre os crimes perpetrados em âmbito tecnológico, promovendo a segregação com base principalmente na natureza do delito e qual o bem jurídico lesado.

Apesar das diferentes denominações, os “crimes cibernéticos”, “crimes eletrônicos”, “crimes virtuais”, entre outros, possuem o mesmo sentido e significado. Todos fazem referência a uma conduta ilegal praticada por alguém que se utiliza de alguma espécie de meio eletrônico para o cometimento do crime.

Nesse sentido, para Assunção (2018, p. 11), crimes cibernéticos são referentes à:

> “Crimes de ódio em geral (contra a honra, sentimento religioso, bullying), crimes de invasão de privacidade e intimidade (que pode ou não incorrer em uma nova conduta lesiva contra a honra), crimes de estelionato, crimes de pedofilia, entre outros.”

De modo geral, verifica-se que englobam condutas tipificadas em legislação, mas se diferenciam por serem perpetradas em meio eletrônico.

Para fins didáticos, foi sistematizado em doutrina algumas classificações, trazendo os conceitos de crimes cibernéticos puros, mistos e comuns. Além da corrente doutrinária que aborda essas infrações como próprios e impróprios.

Os crimes cibernéticos *puros*, se referem aos delitos que atingem diretamente o sistema computacional, ou seja, o próprio dispositivo informático em si, integrando também os seus servidores, dados e informações contidas. Enquanto nos crimes cibernéticos *mistos,* existe a necessidade de utilização do

da Internet para efetivar a prática do delito, contudo, não é o dispositivo em si que será objeto do crime, e sim outro bem jurídico tutelado, como exemplo, Matsuyama e Lima (2017, p. 03) citam a retirada ilícita de valores monetários de contas bancárias, lesando o patrimônio de terceiros.

No que se refere aos classificados como *comuns*, é quando o agente pratica uma conduta tipificada no Código Penal, valendo-se do meio tecnológico. A título de exemplo, o agente aplica um “golpe” na vítima virtualmente, caracterizando um estelionato, conduta que pode ser praticada por outros meios, não sendo exclusivamente necessária a utilização da internet para sua realização.

Em outra análise doutrinária, passando à explanação dos crimes cibernéticos *próprios*, Oliveira (2009, p. 33) explica:

> “[...] só pode ser cometido no ciberespaço, ou seja, necessariamente, deve ser realizado no ambiente do ciberespaço, para que a conduta seja concretizada, tendo um tipo penal distinto do tradicional. Ademais, tanto a ação quanto o resultado da conduta ilícita consumam-se no ciberespaço.”

Essa classificação está diretamente relacionada aos crimes cibernéticos mistos anteriormente abordados, onde é indispensável a utilização do meio virtual para a prática delitiva.

Por fim, nos crimes cibernéticos *impróprios*, a rede mundial de computadores e a internet são apenas os meios utilizados para a concretização da infração penal, de modo que não é o meio exclusivo para praticá-la.

Sendo assim, têm-se essas classificações, que ainda são objetos de debate doutrinário, mas que na prática, tratam-se, de modo geral, de crimes em que há utilização de meios tecnológicos, de modo que as ações criminosas e os seus vestígios são lastreados em âmbito virtual.

2 LEGISLAÇÃO BRASILEIRA E DELITOS INFORMÁTICOS

Diversas são as espécies de crimes praticadas virtualmente. No entanto, com enfoque nos crimes cibernéticos comuns, sendo estes aqueles em que o agente se utiliza da tecnologia como **meio** de praticar o fato típico, algumas especificamente são mais recorrentes, surgindo, inclusive, algumas inovações legislativas que objetivam reprimir novas práticas delitivas, diante da abrangência de condutas perpetradas em meio digital, sendo que estas passarão a ser analisadas adiante.

2.1 Estelionato e outras fraudes

Sem dúvidas, os crimes contra o patrimônio são os mais comuns no ambiente virtual. Dentre esses, o de maior destaque é o estelionato, previsto no artigo 171 do Código Penal Brasileiro, que consiste em *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.*

No que se refere ao termo “artifício” mencionado no tipo penal, explica Mirabete (2021, p. 325):

> “[...] o artifício existe quando o agente se utilizar de um aparato que modifica, ao menos aparentemente, o aspecto material da coisa, figurando entre esses meios o documento falso ou outra falsificação qualquer, o disfarce, a modificação por aparelhos mecânicos ou elétricos, filmes, efeitos de luz etc.”

Atualmente, é comum encontrar nas redes sociais alertas aos usuários acerca de novos “golpes” que estão vitimando muitas pessoas, ocasião em que os agentes sempre simulam uma situação que não aparenta ser uma fraude, e a vítima, diante da falsa concepção de realidade, fornece ao criminoso vantagem indevida.

Sempre que o *modus operandi* de uma fraude se torna muito difundido, de modo que o sucesso na empreitada criminosa se torna mais difícil de ser atingido, são inauguradas novas formas de ludibriar a vítima, e assim se mantém no mundo criminoso os famosos “estelionatários”.

Diversos são os métodos utilizados para obtenção da vantagem ilícita virtualmente, sendo que o mais comum é aquele em que o agente simula a realização de um negócio, como por exemplo a compra e venda de um objeto, sempre oferecendo uma vantagem altamente irresistível de modo que atraia o interesse de mais pessoas.

Além disso, é recorrente também a prática da técnica denominada *phishing*. A empresa de segurança informática Avast (2020) explica acerca do que se refere o mencionado termo:

> "[...] é uma maneira desonesta que cibercriminosos usam para enganar você para revelar informações pessoais, como senhas ou cartão de crédito, CPF e número de contas bancárias. Eles fazem isso enviando e-mails falsos ou direcionando para websites falsos".

Ou seja, *phishing* se refere a prática onde o criminoso age se passando por uma empresa, geralmente uma instituição bancária ou qualquer outra a qual a vítima seja vinculada de alguma forma, solicitando informações pessoais para que possam ter acesso aos dados da vítima e, a partir disso, obter alguma vantagem ilícita.

Verificada a necessidade de previsão legal para repressão dessa prática, que muito se assemelha ao delito de estelionato, foi promovida uma alteração legislativa inaugurado um novo tipo penal de fraude eletrônica, previsto nos §§2º-A e 2º-B do art. 171, qualificando o crime quando for cometido mediante a utilização de redes sociais, contatos telefônicos ou qualquer outro meio fraudulento análogo, além da utilização de servidor mantido fora do território nacional.

Dessa forma, evidente que a qualificadora que trata da fraude eletrônica se refere exatamente ao acesso que o agente possui às informações pessoais da vítima virtualmente. Nessa situação, podemos destacar o envio de mensagens para amigos e/ou familiares simulando a necessidade de depósitos bancários ou outras transações financeiras, ligações simulando se tratar de instituição bancária, a fim de obter dados pessoais bancários da vítima para extrair valores de sua conta.

Outra importante inovação legislativa promovida pela lei n. 14.155/2021, inserida no artigo 70 do Código de Processo Penal, foi a alteração da competência para julgamento do delito de estelionato quando praticado mediante depósito, mediante emissão de cheques sem suficiente provisão de fundos em poder do sacado ou com o pagamento frustrado ou mediante transferência de valores, passando a ser o juízo competente o local de domicílio da vítima.

2.2 Pornografia infantil

Para os efeitos da legislação especial brasileira, considera-se criança a pessoa com até 12 (doze) anos de idade incompletos, de acordo com o disposto no art. 2º da Lei n. 8.069/90. No entanto, conforme previsto em lei, é tipificado como estupro de vulnerável a conduta de ter conjunção carnal ou praticar outro ato libidinoso com menores de 14 (quatorze) anos, não sendo excluída a ilicitude do ato pelo consentimento do menor, equiparando, dessa forma, os adolescentes até a mencionada idade como vulneráveis para fins de proteção jurídica especial.

A pornografia infantil consiste em práticas criminosas que atingem a dignidade sexual de crianças e adolescentes, previstas no Código Penal Brasileiro e na lei n. 8.069/90, o Estatuto da Criança e do Adolescente (ECA).

A lei prevê como ilícito penal de pornografia infantil a prática de condutas relacionadas à produção, manutenção e compartilhamento de imagens que contenham conteúdo pornográfico envolvendo crianças e adolescentes.

No âmbito da criminalidade virtual, há de se reconhecer que a atual geração infanto-juvenil possui acesso à internet e todos os recursos disponíveis precocemente, sendo que desde antes da alfabetização as crianças já são familiarizadas em informática e todos os recursos inerentes ao meio digital, aderindo ao uso das redes sociais e outros meios de comunicação.

De acordo com pesquisas realizadas por veículos de informação, os índices de prática de pornografia infantil cresceram absurdamente durante o

período pandêmico, isso porque as crianças e adolescentes passaram a ficar mais tempo em casa e, consequentemente, nas redes sociais.

Destaca-se, ainda, que diante do descontrolado uso das redes sociais por parte dos infantes, muitos acabam sendo levados a situações de superexposição, tendo se tornado cada vez mais comum a exibição e sexualização do próprio corpo diante de fotos e vídeos publicados na internet, muitas vezes sem o conhecimento de seus responsáveis.

Em contrapartida, estão como espectadores desse palco virtual os agentes criminosos que utilizam dessa exposição para produzir conteúdo criminoso, posteriormente publicando e compartilhando os registros em sites ou aplicativos.

As redes sociais possuem políticas próprias de segurança e privacidade de consentimento obrigatório pelos usuários, além de estarem sujeitas à legislação nacional.

Inclusive, recentemente, após investigações e apurações de denúncias, foi determinado o bloqueio do aplicativo de comunicação *Telegram*, que diante do mecanismo de criação de grupos com capacidade de integrar até 200 mil participantes, tornou-se um ambiente de ocorrência de crimes virtuais de diversas naturezas, inclusive a pornografia infantil, além de propagação de notícias falsas e ataques à democracia brasileira, disseminando ideais extremistas.

Nesse sentido, o Ministro cita em sua Decisão trecho do relatório da Polícia Federal acerca do que foi obtido em investigação do mencionado aplicativo:

> “Dentre os aplicativos de mensageria mais usados pelos abusadores sexuais de crianças, por exemplo, está o TELEGRAM. Esses criminosos se utilizam de forma individual e, principalmente, por meio de grupos (cibernéticos) para cometerem crimes gravíssimos contra crianças e adolescentes. A plataforma está sendo utilizada com a finalidade de adquirir imagens de abuso sexual infantil, bem como para realizar a difusão dessas imagens (fotos e vídeos). Muitos desses indivíduos, que têm se unido em grupos com centenas de pessoas de vários locais do Brasil e do mundo, vendem e compartilham imagens de condutas gravíssimas relacionadas a estupro de vulnerável. Ademais, há grupos destinados especificamente para produtores

> desse tipo de material delitivo, ocasião em que crianças estão em situação atual de extrema violência. (...)”

Segundo apurado, esses conteúdos estão disponíveis em grupos secretos em que o ingresso se dá através do acesso por um link compartilhado por quem já possui o acesso.

Após o cumprimento das medidas impostas, foi revogado o bloqueio da rede social, no entanto, o Poder Judiciário brasileiro segue atuando no combate à criminalidade virtual, com as exigências de que as empresas responsáveis pelas redes sociais utilizadas no território nacional cumpram a política de segurança e privacidade a fim de garantir um ambiente seguro para todos os usuários, além de evitar que novas vítimas sofram os danos causados pela prática do ilícito penal.

2.3 Crimes contra a honra e Cyberstalking

Diante da distância física e do acesso irrestrito a vida do outo, as pessoas têm a sensação de que podem falar o que quiserem, quando e da forma que quiserem, acreditando estarem blindadas pela capa de um perfil virtual e que a Internet é “terra sem lei”.

Fato é que quanto mais a pessoa se expõe, quanto mais fornece informações pessoais e dá acesso à sua vida particular, mais as pessoas acreditam que tem o direito de opinar e de interferir, principalmente quando se tratar de pessoa pública.

Assim, buscam validar seus posicionamentos pelo direito de liberdade de expressão, direito assegurado no art. 5º, inciso IV da Constituição Brasileira: *É livre a manifestação do pensamento, sendo vedado o anonimato*. No entanto, nenhum direito é absoluto, existindo um limite estabelecido para liberdade de expressão, sendo este atingido a partir do momento em que a opinião configura uma infração penal.

Além disso, o Superior Tribunal de Justiça já reconhece a natureza dos delitos contra a honra praticados virtualmente, sendo estes consumados imediatamente quando é proferida a ofensa:

> Crimes contra a honra praticados pela internet. Natureza do delito.
>
> "Crimes contra a honra praticados pela internet são formais, consumando-se no momento da disponibilização do conteúdo ofensivo no espaço virtual, por força da imediata potencialidade de visualização por terceiros' (CC 173.458/SC, Rel. Ministro João Otávio de Noronha, Terceira Seção, DJe 27/11/2020)." HC 591.218/SC, Rel. Ministro Joel Ilan Paciornik, Quinta Turma, julgado em 09/02/2021, DJe 12/02/2021.

No entanto, além dos crimes contra a honra, é previsto o delito de *stalking*, que consiste em praticar atos de perseguição contra a vítima, ameaçando os direitos de liberdade e segurança. Esse tipo penal surge da necessidade de proteção à liberdade pessoal do indivíduo, ainda não tutelada na forma dos dispositivos já previstos. Nesse sentido, é o trecho do parecer do Senado Federal ao Projeto de Lei que foi sancionado:

> “O novo tipo penal proposto supre uma lacuna em nossa legislação penal, que, embora criminalize o constrangimento ilegal e preveja como contravenção penal as condutas de perturbação do sossego alheio e perturbação da tranquilidade, não trata da perseguição reiterada que ameaça à integridade física ou psicológica da vítima, restringindo-lhe a capacidade de locomoção ou, de qualquer forma, invadindo ou perturbando sua esfera de liberdade ou privacidade.”

O mencionado tipo penal é previsto no art. 147-A, sendo possível a sua prática também no âmbito virtual, caracterizando o *Cyberstalking.* Embora nem sempre seja praticado por anônimos, este delito também está diretamente ligado à exposição virtual e às consequências causadas pela divulgação excessiva de dados e informações pessoais.

A perseguição virtual é configurada quando a vítima sofre ameaças à sua integridade física e psicológica reiteradas vezes por meio de mensagens que são, em regra, encaminhadas através de redes sociais, muitas vezes por perfis *“fakes”*, onde o agente se vale do anonimato para proferir tais ameaças, acreditando que sua identidade não será descoberta. No caso de pessoas públicas e famosos, é extremamente comum a existência de *“haters”,* indivíduos que se dedicam diariamente a ofender e praticar atos que depreciem a imagem

e honra dessas pessoas, e quando atingem o ponto mais alto de obsessão, proferem ameaças injustas e graves, praticando o delito mencionado.

3 A INVESTIGAÇÃO CRIMINAL NOS CRIMES CIBERNÉTICOS

3.1 Investigação policial

No Brasil, existe um sistema de investigação preliminar processual, que tem por objetivo apurar indícios de autoria e materialidade dos delitos, produzindo elementos probatórios para subsidiar eventual denúncia. Em regra, essa busca preliminar é realizada através do Inquérito Policial, procedimento investigativo instaurado pela polícia judiciária.

Acerca do objeto do mencionado procedimento, leciona o doutrinador Aury Lopes Júnior (2021, p. 161):

> "O inquérito policial serve – essencialmente – para averiguar e comprovar os fatos constantes na *notitia criminis*. Nesse sentido, o poder do Estado de averiguar as condutas que revistam a aparência de delito é uma atividade que prepara o exercício da pretensão acusatória que será posteriormente exercida no processo penal. É importante recordar que, para a instauração do inquérito policial, basta a mera possibilidade de que exista um fato punível. A própria autoria não necessita ser conhecida no início da investigação."

Embora muitos doutrinadores considerem a dispensabilidade do Inquérito Policial, esse procedimento é de suma importância para o sistema processual penal brasileiro, em que pese a delegacia de polícia ser o local de primeiro acesso à justiça que as vítimas e os infratores têm logo após a ocorrência do ilícito penal. Podemos reconhecer que o trabalho desempenhado pela polícia judiciária é como um "filtro", onde busca averiguar a procedência das primeiras informações fornecidas acerca dos crimes, bem como realizar a produção das provas que irão embasar eventual denúncia perante o Poder Judiciário.

No que se refere a investigação policial nos crimes informáticos, o art. 4º da lei n. 12.735/12 dispõe que os órgãos da polícia judiciária deverão se estruturar, dispondo de equipes de pessoal e de equipamentos especializados

para combate às ações criminosas perpetradas em rede de computadores, de modo que seja mais eficaz o desempenho do trabalho investigativo.

Em observância à legislação, muitos estados já possuem atualmente ao menos uma delegacia estadual especializada para repressão a crimes cibernéticos, a exemplo do Estado de Goiás, que conta com uma equipe policial especializada e qualificada para atuar na investigação dos diversos delitos praticados por meio da rede mundial de computadores.

Dentre as atividades policiais desenvolvidas na persecução penal dos cibercrimes, um dos procedimentos existentes aliados a tecnologia é a infiltração virtual de agente policial. Esse procedimento é previsto no art. 190-A do Estatuto da Criança e do Adolescente, na lei n. 12.850 (Lei de Organizações Criminosas) e na lei n. 9.613/98 (Lei de Lavagem de Dinheiro) observado o disposto na legislação.

Esse recurso é comumente utilizado para a infiltração de agentes em ambientes virtuais restritos, sobretudo quando se trata de crimes contra a dignidade sexual de crianças e adolescentes, normalmente praticados em ambientes restritos na internet onde os agentes acessam de forma anônima, como por exemplo a Deep Web e a Dark Web, são utilizados para desenvolver a atividade criminosa.

É importante ressaltar que, embora demande a existência de uma estrutura investigativa especializada, também são utilizadas todas as formas tradicionais de investigação da polícia judiciária brasileira durante a persecução penal, tais como realização de perícias, reconhecimentos e prova testemunhal.

3.2 Procedimento probatório e as provas digitais

Quando nos referimos à identificação de autoria nos crimes virtuais, existem duas premissas divergentes que podem ser identificadas: que nos delitos informáticos, é de maior complexidade o procedimento para identificação do agente em que pese a ausência de sua presença física no local do crime,

passando o sentimento de impunibilidade, principalmente diante de casos de anonimato.

Essa é a principal impressão causada a todas as vítimas, de acordo com Burg (2017):

> "A internet facilita a impunidade, uma vez que a investigação é mais complicada e, muitas vezes, quando é identificado o autor, já ocorreu a prescrição. Isso sem contar na questão da fronteira: o crime pode ser cometido por alguém que está em outro país, com leis completamente diferentes. (...) A legislação brasileira não está adequada e, muitas vezes, o crime prescreve sem que haja um avanço significativo nas investigações. Nos crimes contra a honra, por exemplo, há uma enorme dificuldade para se identificar o autor de ofensas realizadas na internet, e sem a identificação sequer é possível oferecer queixa-crime."

Em contrapartida, existe a corrente que assevera que tudo que está no meio informático deixa rastros, sendo passível de identificação, uma vez que, a partir do momento em que uma conexão virtual é estabelecida, todos os dados acessados através dela são compartilhados por meio de uma rede de conexão.

Nesse sentido, o autor Carlos Alberto Rohrmann (2005, p. 4) aponta:

> "A comunicação de dados através da Internet não se dá pela mesma lógica da comunicação telefônica ordinária. Nesta, uma vez estabelecida a ligação entre duas pessoas, o circuito se fecha, pois a comunicação ocorre como se houvesse uma ligação dedicada, exclusiva, entre as duas pessoas. Já no caso da Internet, a comunicação não 'fecha' um circuito dedicado. As mensagens trocadas entre os usuários são transformadas em 'pacotes' que trafegam por rotas variadas ao longo da rede."

Embora os dados das comunicações virtuais fiquem armazenados em rede, é assegurado o direito de privacidade e de proteção dos dados de todos os usuários nas redes. No entanto, o marco civil da internet, lei n. 12.965/14, além de estabelecer os princípios que disciplinam o uso da internet em âmbito nacional, assevera que em caso de práticas criminosas, diante da necessidade de obtenção de acesso aos dados e registros de conexões, estes poderão ser obtidos mediante autorização judicial, isso porque, em regra, as provas serão obtidas através do meio utilizado para a prática da infração penal, e no caso dos crimes cometidos por meio da rede mundial de computadores, serão utilizados, de igual forma, os meios tecnológicos.

É também conforme explica Almeida (p. 9):

> “As provas geralmente são oriundas de produtos de aplicativos (mensagens escritas, áudios, imagens, vídeos etc.) e informações de âmbito eletrônico, como por exemplo uma transação bancária. Esses resultados servem para confirmar as denúncias ou para utilização a favor do investigado. Para se recuperar conversas apagadas de celulares ou aplicativos como o WhatsApp, os peritos digitais utilizam programas específicos e resgatam os conteúdos. As principais fontes de obtenção de provas digitais são: extração de informações de celulares, análise de informações fornecidas por empresas de tecnologia, redes sociais, aplicativos de comunicação e operadoras de telefonia, fontes abertas (Facebook e Instagram).”

Um fator de extrema relevância para a obtenção de êxito no processo de investigação do delito é a manutenção da prova por parte da vítima. Embora existam os registros de dados que poderão ser obtidos por ordem judicial, é necessário a existência de um ponto inicial de partida para a produção probatória. Daí a importância de sempre promover a informação dos usuários, para que em caso de ocorrência de eventual infração penal, preservem os vestígios deixados pelo delito, colaborando com posterior investigação.

3.3 Os novos paradigmas de investigação criminal

Observa-se que diante do cenário totalmente tecnológico em que se encontra a sociedade, é inevitável a busca por aliar meios tecnológicos às atividades desempenhadas em estudos, trabalho e prestação de serviços. No âmbito do trabalho policial e na prestação jurisdicional não é diferente.

Em virtude da constante utilização das inovações tecnológicas, surgem alguns questionamentos como por exemplo a respeito da confiabilidade dos métodos utilizados e, além disso, acerca da legalidade desses novos procedimentos, uma vez que o Direito Penal e Processual Penal brasileiro observa a todos os direitos e garantias fundamentais assegurados na Constituição Federal, de modo que os órgãos da justiça jamais poderão utilizar medidas que violem essas garantias.

No entanto, a implementação de um novo recurso sempre precede regulamentação legal, além da viabilidade e conveniência e do Estado em aderir

as novas formas. Exemplo de medidas tecnológicas presentes no sistema processual penal brasileiro atual são os diversos mecanismos de inteligência tecnológica e informática utilizados pela polícia brasileira, na esfera estadual e federal. Reflexo notável disso são os procedimentos de investigação tecnológica comumente utilizados pelos órgãos responsáveis.

Acerca do tema, Jorge (2018) define que:

> “Investigação Criminal Tecnológica é aquela baseada nos mais variados recursos eletrônicos. São exemplos de investigação tecnológica: interceptação telefônica e/ou telemática, pesquisa de informações disponíveis na internet e em bancos de dados físicos, pesquisa de imagens extraídas de recursos tecnológicos, incluindo câmeras de segurança, câmeras fotográficas, celulares, relatórios extraídos de softwares de análise de veículos ou utilizados para examinar dispositivos informáticos e outros meios.”

Importante frisar que esses métodos investigativos não são utilizados somente nos delitos virtuais, e sim em todas as infrações penais previstas no ordenamento jurídico brasileiro em que seja autorizada a sua implementação, observando ao previsto em seus respectivos dispositivos legais.

À luz dessas considerações, deve se ressaltar que todos os procedimentos de modernização e inovação tecnológica devem ser adotados em estrita observância às normas constitucionais vigentes, para que sejam aliados aos métodos tradicionais de investigação criminal, de modo que busque sempre pela eficiência e eficácia do trabalho investigativo na seara criminal.

CONCLUSÃO

A informatização da sociedade é uma realidade do século XXI, e o uso da internet cresceu disparadamente ao longo dos últimos anos, de modo que atualmente a regra é que todas as atividades sejam desempenhadas com o uso dos recursos virtuais e dos meios tecnológicos, se assim for possível.

No entanto, diante dessa modernização e com tantas inovações tecnológicas, surge na internet a criminalidade virtual.

O objeto da presente pesquisa foi demonstrar como se deu o início das práticas infracionais no ambiente virtual, quais foram os impactos iniciais causados e como se deu a provocação ao Estado na condição de regulamentador das relações jurídicas, momento em que foi constatada a necessidade de tutela Estatal, buscando estabelecer uma regulamentação da vida social virtual dos internautas.

Foram explanadas as diversas classificações e definições doutrinárias acerca dos delitos informáticos, o que ainda é objeto de ampla discussão entre os estudiosos da área, que buscam promover maior esclarecimento mediante a diferenciação das modalidades criminosas perpetradas na esfera da rede mundial de computadores.

Realizou-se, ainda, uma explanação objetiva acerca dos principais delitos em espécie que são praticados no âmbito virtual, com enfoque no cenário brasileiro. Dessa pesquisa, foi possível constatar que muitos dos delitos praticados na internet já são previstos no ordenamento jurídico brasileiro, no entanto, em virtude da lacuna provocada pela ausência de legislação específica com previsão para a modalidade virtual, por vezes, resulta na impunidade dos agentes criminosos.

Dessa forma, em razão da informatização social, é inegável o impacto causado no Direito como ciência jurídica, surgindo assim, a necessidade de dispensar a atenção aos dispositivos legislativos nesse sentido, além da carência de considerável investimento no que tange aos métodos de

investigação, visando fornecer às autoridades policiais, órgãos investigadores e ao Poder Judiciário uma boa estrutura e capacitação tecnológica.

Nesse sentido, constata-se que os legisladores já estão atuando na efetiva criminalização de condutas que surgiram justamente em razão da prática no meio virtual, além de buscar inovar na implementação de recursos tecnológicos no quesito de investigação criminal, buscando a modernização dos métodos utilizados pela polícia, bem como pelo próprio poder legislativo e judiciário. No entanto, não é possível afirmar que as previsões legais estão sendo efetivamente aplicadas na prática.

Sendo assim, conforme previsto em lei, é necessária a instituição de órgãos de justiça especializada, promoção de campanhas de conscientização aos internautas e aplicação de uma abordagem clara e acessível acerca dos riscos, inclusive com uma atuação conjunta às redes de comunicação virtual, de modo que estas estejam sempre atuando em conformidade com a legislação pátria, na busca da repressão das atividades criminosas e na efetiva punição dos agentes.

CYBER CRIMES

DIGITAL LAW AND THE NEW PARADIGMS OF CRIMINAL INVESTIGATION

ABSTRACT

This article seeks to present the main cyber crimes in kind and their characteristics, with emphasis on the recurrence of their practice in Brazil. It was presented the national legislation that deals with the subject, the main means of repression and sanctions applied. The main objective of the research turned to the exposure and evaluation of the main means of obtaining digital evidence collected to determine authorship and criminal materiality. Given the peculiarities inherent to this criminal modality, listing the essential innovations that fell on Brazilian Criminal Law and Criminal Procedure. Research was carried out on the main influences on these crimes, pointing out the importance of user prevention and modernization of criminal investigation, combined with technological advances.

Keywords: Cyber crimes. Evidences. Investigation.

REFERÊNCIAS

ALMEIDA, Priscila Danielle Barbosa.: PROVAS DIGITAIS E SUA COLABORAÇÃO NA INVESTIGAÇÃO CRIMINAL TECNOLÓGICA. Faculdades Integradas de Santa Fé do Sul – FUNEC. 2018.

AZEVEDO, Leticia Silva; CARDOSO, Thais Mariana. CRIMES CIBERNÉTICOS: EVOLUÇÃO E DIFICULDADES NA COLHEITA DE ELEMENTOS DE AUTORIA DELITIVA. Trabalho de Conclusão de Curso (graduação) – Faculdade de Uma Bom Despacho, Curso de Direito, Bom Despacho, 2021.

Brasil. Ministério Público Federal. Câmara de Coordenação e Revisão, 2. Roteiro de atuação: crimes cibernéticos. 3.ed. rev. e ampl. Brasília: MPF, 2016.

CARVALHO, Gabriel Chiovetto. Crimes Cibernéticos Conteúdo Jurídico. Brasília. 2018. Disponível em: <https://conteudojuridico.com.br/consulta/Artigos/51878/crimes-ciberneticos. > Acesso em: 28 out 2021.

Entrevista com o advogado especialista Daniel Allan Burg. Disponível em https://www.conjur.com.br/2017-fev-05/entrevista-daniel-burg-especialista-crimes-virtuais. Acesso em 25 mar 2022

ESTEFAM, André; GONÇALVES, Victor Eduardo Rios. Direito penal esquematizado – parte geral. 9. ed. São Paulo: Saraiva Educação, 2020.

GOMIDES, Leonardo Andrade Siqueira. A TECNOLOGIA E O DIREITO PENAL: os novos paradigmas da investigação criminal. Trabalho de Conclusão de Curso (graduação) – UniEvangélica, Curso de Direito, Anápolis, 2020.

JESUS, Damásio de. MILAGRE, José Antônio. Manual de crimes informáticos. São Paulo: Saraiva, 2016.

JORGE, H. V. N. Investigação Criminal Tecnológica. Vol. 1. Rio de Janeiro: Brasport, 2018.

LOPES JR., Aury. Direito processual penal. 18. ed. São Paulo: Saraiva Educação, 2021.

MACHADO, Jonathan. O que é um keylogger? 2012. Disponível em: < https://www.tecmundo.com.br/spyware/1016-o-que-e-keylogger-.htm>. Acesso em 25 de outubro de 2021.

MAIA, Teymisso Sebastian Fernandes. Análise dos Mecanismos de Combate aos Crimes Cibernéticos no Sistema Penal Brasileiro. Trabalho de Conclusão de Curso (graduação) – Universidade Federal do Ceará, Faculdade de Direito, Curso de Direito, Fortaleza, 2017.

MARTINS, Aislan Bruno da Silva. CRIMES VIRTUAIS. Trabalho de Conclusão de Curso (graduação) – Faculdade de Sabará, Curso de Direito, Sabará, 2017.

MIRABETE, Júlio Fabbrini e FABBRINI, Renato N. Manual de direito penal: parte especial: arts. 121 a 234-B do CP – volume 2, 36° edição, São Paulo, Atlas, 2021.

NUCCI, Guilherme de Souza. Manual de direito penal. 16. ed. Rio de Janeiro: Forense, 2020.

ROCHA, Adriano Aparecido. Cibercriminalidade: os crimes cibernéticos e os limites da liberdade de expressão na internet. Garça, 2017.

ROHRMANN, Carlos Alberto. Curso de Direito Virtual. Belo Horizonte: Del Rey, 2005.

SILVA, Patrícia Santos da. Direito e crime cibernético: análise da competência em razão do lugar no julgamento de ações penais. Brasília: Vestnik, 2015