UNIVERSIDADE FEDERAL DE UBERLÂNDIA
FACULDADE DE DIREITO “PROF. JACY DE ASSIS”
TRABALHO DE CONCLUSÃO DE CURSO
NÚCLEO DE PRÁTICA JURÍDICA
ARTIGO JURÍDICO CIENTÍFICO

REFLEXÕES SOBRE OS DESAFIOS ENFRENTADOS PELO DIREITO CRIMINAL DIANTE DOS CRIMES PERPETRADOS NA INTERNET

ORIENTANDO – LUCAS MATEUS AMARAL TELES

ORIENTADOR – PROF. KARLOS ALVES BARBOSA

UBERLÂNDIA
2024

LUCAS MATEUS AMARAL TELES

REFLEXÕES SOBRE OS DESAFIOS ENFRENTADOS PELO DIREITO CRIMINAL DIANTE DOS CRIMES PERPETRADOS NA INTERNET

Artigo científico apresentado perante a Faculdade de Direito “Prof. Jacy de Assis”, da Universidade Federal de Uberlândia (UFU), Estado de Minas Gerais, como parte dos requisitos exigidos para a conclusão do curso de Direito e respectiva aquisição do título de bacharel.

Prof. Orientador – Karlos Alves Barbosa

UBERLÂNDIA

2024

LUCAS MATEUS AMARAL TELES

REFLEXÕES SOBRE OS DESAFIOS ENFRENTADOS PELO DIREITO CRIMINAL DIANTE DOS CRIMES PERPETRADOS NA INTERNET

Data da Defesa: 12 de abril de 2024

BANCA EXAMINADORA

Orientador: Prof. Karlos Alves Barbosa

Examinador (a) Convidado (a): Prof. (a): Edihermes Marques Coelho

UBERLÂNDIA
2024

Resumo

Diante do avanço sem precedentes da tecnologia no Brasil, uma questão que se coloca em debate prediz sobre os desafios que a legislação penal e processual penal terá de enfrentar a partir da constatação das altas taxas anualmente em crescente expansão dos crimes cometidos no âmbito virtual. A abordagem merece atenção em virtude de que o país não é dotado de uma legislação robusta sobre o tema, mas munido apenas de artigos específicos no Código Penal e em outras leis esparsas que nem mesmo se situam no contexto penal, como o caso do Marco Civil da Internet (Lei nº 12.965, De 23 de Abril de 2014). Assim sendo, indivíduos que empregam o uso de tecnologia para o exercício criminoso se veem cada vez mais atraídos a reforçarem a prática da conduta mediante a falta de determinadas reprimendas consolidadas. Usou-se para o presente trabalho a aplicação de metodologia de pesquisa mediante revisão bibliográfica, exploratória, e de leituras noticiais publicadas na Rede Mundial de Computadores. À vista disso, atinge-se o ideal de que, o cibercrime, crime virtual, crime digital, entre outras nomenclaturas que batizam essa prática de crime, cuidando-se de um fenômeno social e econômico, intrínseco às transformações tecnológicas, por ser de fato experenciado pela comunidade, culminam na influência direta das reflexões do Direito Penal e consequentemente do Direito Processual Penal.

Palavras-Chave: Direito Penal. Processo Criminal. Cibercrime. Internet. Legislação.

Abstract

Faced with the unprecedented advancement of technology in Brazil, an issue that is being debated predicts the challenges that criminal and criminal procedural legislation will have to face based on the observation of the high rates of crimes committed in the virtual sphere every year. The approach deserves attention because the country does not have robust legislation on the subject, but only has specific articles in the Penal Code and other scattered laws that are not even in the criminal context, such as the Marco Civil of the Internet (Law nº 12,965, of April 23, 2014). Therefore, individuals who employ the use of technology for criminal activity find themselves increasingly attracted to reinforcing the practice of crime through the lack of certain established reprimands. For this work, the application of research methodology was used through bibliographical, exploratory review, and news readings published on the

World Wide Web. In view of this, the ideal is reached that cybercrime, virtual crime, digital crime, among other nomenclatures that baptize this practice of crime, taking care of a social and economic phenomenon, intrinsic to technological transformations, as it is in fact experienced by the community, culminate in the direct influence of reflections on Criminal Law and consequently on Criminal Procedural Law.

Keywords: Criminal Law. Criminal proceedings. Cybercrime. Internet. Legislation.

SUMÁRIO

INTRODUÇÃO

No estado de direito, conforme leciona os manuais de Direito Constitucional, vigora o Império da Lei. Nesse sentido, sendo a lei suprema, nenhuma figura, a não ser ela própria, haverá de ser cumprida, em observância dos princípios extraídos da dignidade da pessoa humana. O modelo vigente no Estado Democrático de Direito se contrapõe aos antigos modelos autocráticos, oligárquicos e ditatoriais de Estado. Numa ótica em que as normas jurídicas não são positivadas, seja por meio de legislação, seja pelos costumes, sempre haverá o rechaço da democracia. Dado isso, é imperioso notar que o Direito é questão fundamental para a existência da democracia, haja vista a sua força na consolidação da justiça, igualdade, legalidade, responsabilidade, obrigação e a autonomia da vontade.

No Estado Democrático de Direito, os indivíduos têm seus direitos e deveres estabelecidos nas normas que compõe o Ordenamento Jurídico, ou, caso o país seja signatário de tratado internacional, no conjunto de normas deste (tratado). Nesse modelo, todos se submetem às normas, de modo que, o artigo 3° da LINDB (Lei de Introdução às Normas do Direito Brasileiro), pontua que "ninguém se escusa de cumprir a lei, alegando que não a conhece". Na mesma linha segue o artigo 21 do Código Penal, expondo que "o desconhecimento da lei é inescusável".

A dicotomia Direito Público e Privado, numa ordem bem estabelecida, há de ser criteriosa e bem definida, de modo que o Direito Público cuida de questões de ordem também pública, representando uma relação vertical entre o Estado e o indivíduo. Outrora, o Direito Privado estabelece uma ordem horizontal de relacionamento, por cuidar de matérias de ordem privada. Através do Direito Público e Privado, diversos outros sub-ramos regram determinadas matérias fático-sociais.

No que se refere às questões de natureza penal, a legislação criminal (formada principalmente pelo Código Penal e Processual Penal) preveem a resposta jurídica-estatal adequada a cada delito cometido dentro de sua jurisdição (*jus puniendi*). Nesse sentido, o Código Penal tem matéria específica, bem como o Código de Processo Penal, que reúne as normas do dinamismo da atividade jurisdicional. Não há dúvidas de que as normas criminais estão em constante adaptação às inovações do progresso tecnológico humano. O Direito pátrio tende a avançar ao "colocar seus olhos na rede" (SOARES, 2019). Com o advento do avanço das trocas de informação na Internet, está em evolução o que se chama de "Meio Ambiente Digital", que nas palavras de Soares (2019), "ficam sob a guarida de interpretação dos artigos

220 a 224 (Capítulo V - DA COMUNICAÇÃO SOCIAL) da Constituição Federal de 1988, conjuntamente com os artigos 215 e 216...da mesma Carta" (SOARES, 2019, *s/p*). Com isso, vem surgindo um tema que reflete discussões, que se concentra na análise do uso da Internet para prática de condutas ilícitas. Assim, criminosos têm cada vez mais empregado o uso da Internet para cometimento de crimes previstos no ordenamento jurídico penal, conforme as facilidades e vantagens apresentadas por essa prática relativamente nova.

O desenvolvimento da tecnologia trouxe para a humanidade muitos benefícios e diversas facilidades, tais como comodidade, entretenimento, engajamento social, integração, criação de novas profissões, comunicação entre usuários da rede global, encurtamento de distâncias, entre outras benfeitorias. Todavia, caminhando de mãos dadas a esses aspectos positivos, vêm surgindo novas práticas criminais, que alinham o potencial humano para o delito ao uso da tecnologia, acarretando com isso parcial ou completo descumprimento das normas de natureza criminal, no caso destas não estarem investidas de devida adequação. Nos últimos anos, popularizou-se o termo de que a "internet é terra sem lei". Esse sentimento faz com que o cibercriminoso (o agente que comete crimes na Internet, seja ele próprio, impróprio ou misto, definições feitas adiante) se veja cada vez mais atraído a reiterar a conduta, dados os diversos fatores benéficos, tais como o anonimato, sensação de ineficácia das leis atuais e, sobretudo, a sensação de impunidade. A cultura brasileira de combate ao cibercrime (ato ilícito via Internet) não é das mais efetivas, tendo em vista o ineditismo do célere desenvolvimento tecnológico no país, acarretando diversos desafios sobre esse novo tema.

Por conseguinte, as normas criminais já estabelecidas, o direito fundamental ao procedimento justo e efetivo, bem como a criminologia, ficam diante de uma provocação oriunda da necessidade de nova técnica de abordagem, tratamento e recepção para as questões pós anos 2000 (com a democratização da Internet), o qual aponta para o surgimento de novas questões éticas e jurídicas derivadas da inédita forma de relação social via Internet. Em outras palavras, são questões cruciais em que o Ordenamento Jurídico brasileiro precisa se adaptar para a manutenção da boa convivência social. A internet potencializou consideravelmente as clássicas práticas delituosas (tais como o Racismo – art. 20 da Lei 9.459/97; Calúnia – art. 138 do Código Penal; Difamação – art. 139 do Código Penal; Injúria – art. 140 do Código Penal; Ameaça – art. 147 do Código Penal; Furto – art. 155 do Código Penal; Dano – art. 163 do Código Penal; Apropriação indébita – art. 168 do Código Penal; Estelionato – art. 171 do Código Penal; Violação ao direito autoral – art. 184 do Código Penal; Pedofilia – art. 247 da Lei nº 8.069/90 – Estatuto da Criança e do Adolescente; Crime contra a propriedade industrial

– art. 183 e ss. da Lei nº 9.279/96; Crimes de Pirataria – art. 12 da Lei nº 9.609/98, dentre outros).

Citando caso análogo, como o caso do artigo 240 do Estatuto da Criança e do Adolescente (ECA), que define o crime de "produzir, reproduzir, dirigir, fotografar, filmar ou registrar, por qualquer meio, cenas de sexo explícito ou pornográfico, envolvendo criança ou adolescente", percebe-se que, dado que o contexto social em que a norma elaborada não se vislumbrava o impacto da Internet, ela acaba por ser aplicada apenas em situações em que há uma vítima humana envolvida diretamente. Contudo, dado o uso das artimanhas de Inteligência Artificial, como a criação de imagens absurdamente realistas, discussão que se levanta debate sobre a percepção do tipo penal em comento (artigo 240 do ECA), porém, sem uma vítima humana conforme preceitua a legislação, ou seja, a presença de uma lacuna legal.

Ademais, com o advento da nova era da informação, houve uma adaptação de toda a conduta típica que vise a consumação do delito, ou seja, o *iter criminis*, ou caminho do crime, representado pela preparação, execução e consumação dos crimes tradicionais, agora pode ser diligenciado remotamente no ciberespaço (espaço das comunicações por redes de computação). Novos entendimentos irão versar sobre questões cruciais, podendo envolver a noção de inefetividade da legislação, questões de combate direto ao cibercrime, como a identificação do autor; as noções de competência no âmbito interno e internacional (questão processual); competência para processo e julgamento na jurisdição pátria; desatualização legislativa; falta de legislação robusta; despreparo na investigação e coleção de provas digitais; entre outros.

1. PANORAMA GERAL ACERCA DOS CIBERCRIMES

No mundo contemporâneo, com o vasto avanço tecnológico (dado o advento de equipamentos de hardware e software ligados na Rede Mundial de Computadores – Internet), deu-se origem a novas atividades empregadas pelo quociente humano no ambiente virtual. Dentre essas novas atividades, se insere a conduta delituosa na Rede. Por ser ato malicioso perpetrado via Internet, popularizou-se várias nomenclaturas, tais como cibercrime, crime virtual, crime com emprego de internet, dentre outros. É certo que o uso da Internet é meio crucial no levantamento da conduta. Com isso, a Internet tem se tornado palco para a configuração de condutas rechaçadas pelo Direito Criminal, onde o agente criminoso tem lesado, direta ou indiretamente, usuários que se conectam a ela.

No *modus operandi* empregado pelo cibercriminoso, objetiva-se a obtenção de diversos resultados (por exemplo: racismo em todas as formas; crimes de ódio; roubo de dados; ataques a sistemas; estelionato; fraude digital; chantagem; roubo de informações corporativas ou pessoais; pirataria; divulgação de dados mediante chantagem; phishing – tipo de ciberataque; indução a suicídios; *et. alia*.). Para o sucesso na consumação do delito, emprega-se o uso de equipamentos eletrônicos, tais como computadores pessoais, celulares, tablets e afins.

1.1. Tentativa conceitual dos cibercrimes

O crime cibernético, sinonimamente conhecido também por crime digital, crime informático ou virtual, pode ser conceituado de maneira ampla como uma atividade maliciosa pela internet, através do uso de dispositivos de informática, como computadores, celulares, entre outros. Para Damásio e Milagre (2016, p. 49), trata-se "do fato típico e antijurídico cometido por meio da ou contra a tecnologia da informação". Segundo Damásio (2016, p. 48), o cibercrime se encontra intimamente relacionado com as transformações tecnológicas, dado que a desenvoltura tecnológica, dispensado seus inúmeros benefícios, protagonizou a origem dessa nova modalidade de crime, sem a qual não existiria.

Pode-se relacionar o cibercrime também ao incremento das práticas criminosas já estabelecidas e tipificadas na legislação criminal (dentre os quais: calúnia; difamação; injúria; ameaça; furto; dano; apropriação indébita; estelionato; violação ao direito autoral; pedofilia; crime contra a propriedade industrial; pirataria; crimes de ódio; crimes contra a honra; induzimento ao suicídio; instigações a condutas palpáveis). Ressalta-se que, os crimes virtuais podem ser de ordem própria, imprópria ou mista (definição doutrinária).

1.1.1. Cibercrime impróprio

O cibercrime impróprio ou comum é aquele em que o agente se utiliza meramente da Internet para a prática de crimes já existentes, p. ex., estelionato, chantagem, etc. Assim, o manuseio da Internet se constitui apenas como outra via para configuração da conduta.

1.1.2. Cibercrime próprio

O cibercrime próprio ou legítimo é aquele em que a conduta do agente visa, de maneira exclusiva e intrínseca, o dano a sistemas informáticos, por meio de atentados, utilização em massa de *vírus* de computador, etc.

1.1.3. Cibercrime misto

Nas palavras de Soares (2019), o cibercrime misto é aquele em que a utilização da Internet é "...condição indispensável (*sine qua non*) para que a ação criminosa se efetive, mesmo que se vise atingir outro bem jurídico. Ou seja, a lei protege, além do bem informático, outro bem diferente deste, existindo dois tipos penais em vista." (SOARES, 2019, *s/p*).

1.2. Da noção de consumação do cibercrime

Em síntese, a conduta caracterizadamente ilegal, cometida na Internet e mediante o seu uso, propende a ser entendida como cibercrime, vez que se trata de conduta típica operada com o manuseio da Internet. Buscando apoio na doutrina criminalística, aprecia-se a definição de Prado (2019), que, para os crimes em comento, quando da consumação e tentativa, *in verbis*:

> Consuma-se o delito com a mera invasão do dispositivo informático ou instalação de vulnerabilidades, sendo desnecessário que haja efetivamente obtenção, adulteração, destruição de dados ou informações, ou obtenção de vantagem ilícita (delito de mera atividade). A tentativa é admissível, e se verifica quando a invasão ou instalação não ocorrem por circunstâncias alheias à vontade do agente. (LUIZ REGIS PRADO, 2019, p. 1073-1074).

1.3. Esboço sobre o impacto dos cibercrimes no âmbito interno e externo

O número de crimes na internet aumentou cerca de 5% de 2021 (dois mil e vinte e um) para 2022 (dois mil e vinte e dois). No ano de 2022 foram descobertos mais de 120.000.000 (cento e vinte milhões) de arquivos com vírus espalhados pela rede global, sendo o Brasil um dos líderes mundiais neste tipo de crime.

Assim como no mundo, no Brasil os crimes cibernéticos vêm se tornando algo corriqueiro, já que as estatísticas apontam médias assustadoras de cometimento desse crime. O cibercrime tem um grande potencial, e isso faz com que seu impacto seja assustador,

podendo afetar grande camada da sociedade. A complexidade do cribercrime é extensa. As vítimas são passíveis de ataques em diversas áreas, como na moral, na privacidade, no escopo patrimonial, e assim por diante. O impacto do cibercrime na sociedade implica a necessidade de colaboração entre as autoridades nacionais e entre instituições estrangeiras, visando adaptar-se às novas maneiras utilizadas pelos cibercriminosos. Uma das maiores justificativas de se tomar iniciativas dessa natureza está no fato de que a impunidade dos crimes virtuais tem tomado proporções preocupantes. Junto da impunidade dessa conduta, a comunidade se sente cada vez mais insegura em decorrência da falta de resposta do Estado para, ao menos, estancar a ferida.

2. POSSÍVEIS VÍTIMAS DO CIBERCRIME

O cibercrime não deixa de ser um crime como qualquer outro, ressalvado o uso indispensável da Internet, ou seja, a mais clara característica dos crimes virtuais se dá pelo fato da conduta ser praticada no âmbito de dispositivos e ferramentas tecnológicas vinculadas à Internet, ou mesmo através de ferramentas de mídia social. De modo geral, é comum o fato de que o cibercrime ofenda os indivíduos (e seus patrimônios) ou as organizações, por serem realidades tuteladas pela legislação criminal.

2.1. Cibercrime contra indivíduos

Diversos tipos penais são aptos de configuração quando se diz em Internet. Os crimes praticados na Internet em desfavor de indivíduos podem se desdobrar de várias formas, o que equivale dizer que, trata-se de um rol extenso. Dentro desse rol, facilmente se constata a prática dos crimes de transferência de pornografia de menores, assédio moral e psicológico (crimes de racismo de raça e/ou gênero combinados com crime de ódio), difamação, extorsão, roubo de identidade (visando cometimento de fraudes financeiras e falsidade ideológica) chantagem, exposição de informações intimas da vítima, fraude de cartões bancários, prática de *hacking* (uso de softwares maliciosos contra dispositivos eletrônicos da vítima, tais como Ransomware; Phishing; Whale-Phishing; Cavalo de Tróia; Engenharia Social; Falsificação de DNS; entre outros), dano, ameaça, et al. Desse modo, a conduta pode afetar tanto o campo material, quanto o campo imaterial (KUNRATH, 2017).

Com o intuito de ofensa à esfera patrimonial ou de saúde da vítima, os criminosos as exploram psicologicamente, visando a obtenção de informações privilegiadas, íntimas ou até

mesmo guiando-as à realização de práticas bem determinadas, as quais aferem vantagens pecuniárias ao malfeitor ou que violam a integridade física da vítima, ao ponto de que, em alguns casos, ocorra o óbito desta.

The New York Times

Epilepsy Foundation Was Targeted in Mass Strobe Cyberattack

Hackers sent images of flashing strobe lights to the foundation's thousands of Twitter followers in several attacks.

Attacker Causes Epileptic Seizure over the Internet

This isn't a first, but I think it will be the first conviction:

> The GIF set off a highly unusual court battle that is expected to equip those in similar circumstances with a new tool for battling threatening trolls and cyberbullies. On Monday, the man who sent Eichenwald the moving image, John Rayne Rivello, was set to appear in a Dallas County district court. A last-minute rescheduling delayed the proceeding until Jan. 31, but Rivello is still expected to plead guilty to aggravated assault. And he may be the first of many.
>
> The Epilepsy Foundation announced on Monday it lodged a sweeping slate of criminal complaints against a legion of copycats who targeted people with epilepsy and sent them an onslaught of strobe GIFs — a frightening phenomenon that unfolded in a short period of time during the organization's marking of National Epilepsy Awareness Month in November.
>
> [...]
>
> Rivello's supporters — among them, neo-Nazis and white nationalists, including Richard Spencer — have also argued that the issue is about freedom of speech. But in an amicus brief to the criminal case, the First Amendment Clinic at Duke University School of Law argued Rivello's actions were not constitutionally protected.
>
> "A brawler who tattoos a message onto his knuckles does not throw every punch with the weight of First Amendment protection behind him," the brief stated. "Conduct like this does not constitute speech, nor should it. A deliberate attempt to cause physical injury to someone does not come close to the expression which the First Amendment is designed to protect."

Disponível em: https://www.nytimes.com/2019/12/16/us/strobe-attack-epilepsy.html. Acesso em 17 de março de 2023.

2.2. Cibercrime contra organizações

Se o cibercrime contra indivíduos atinge pessoas humanas consideradas individualmente, na outra linha, tem-se o cibercrime voltado contra um conjunto de pessoas humanas, consideradas numa posição de coletividade. Quando o cibercrime se volta contra organizações, fica geralmente caraterizado o ataque contra governos e empresas. Ao se voltar contra os governos, este pode ser lido como prática de terrorismo (KUNRATH, 2017).

Nessa linha de pensamento, há a percepção das vulnerabilidades com que os governos acabam por ficarem reféns, tendo em vista a aderência cada vez mais comum de sua estrutura própria e da prestação de seus serviços (sociais; organizacionais; etc.) mediante o uso de programas de software, p. ex., o portal GOV.BR (plataforma digital de relacionamento do cidadão com o governo federal), aliados, indispensavelmente, à Internet. No ramo empresarial, segundo Tilia (2024), o Brasil se tornou, nos últimos anos, um dos maiores alvos de ataques cibernéticos nas américas, onde, só no ano de 2023, os setores de varejo e energia foram responsáveis cada qual por 41% (quarenta e um por cento) dos casos (CAROLINE DE TILIA, 2024, s/p).

3. CIBERCRIMES PREFERENTEMENTE PRATICADOS NO BRASIL

Em tempos pandêmicos, percebeu-se uma quantidade crescente de crimes cibernéticos devido ao isolamento social, onde as pessoas, não por opção, tiveram que se adaptar à necessidade de utilização cada vez maior das ferramentas digitais e, ao passo que o uso dessas ferramentas aumentara em tempos de covid-19, onde a maioria das pessoas passaram a trabalhar em home office, um quantitativo maior de indivíduos tornara-se vítimas do cibercrime.

Desde sua democratização, a Internet vem sendo taxada de “terra de ninguém” ou “terra sem lei”, em virtude da facilidade com que se comete delitos mediante seu uso. A grande maioria dos crimes já tipificados podem ser praticados pela Internet, isto é, a Internet tem se tornado um espaço muito atrativo para a prática de crimes, levantando questões preocupantes na luta do Estado pela prevenção de tais delitos.

Os criminosos virtuais estão por toda parte, podem acessar contas pessoais ou até um sistema inteiro, podendo-se chegar até mesmo à escala global (caso dos “hackers” profissionais). Em sua conduta, o autor pode atacar ou invadir com apenas o clique de um usuário distraído, os dados e informações cruciais deste.

Dentre os direitos e garantias fundamentais assegurados pelo sistema normativo, destaca-se a liberdade. Cada indivíduo é livre para praticar tudo o que as normas não lhe vedem. Segundo leciona Meirelles (2004), isso se compreende pela máxima de que, os indivíduos, agindo no campo privado, estão autorizados a fazer tudo o que não é proibido em lei (HELY LOPES MEIRELLES, 2004, p. 83). Além de garantia constitucional, jurídica e metafísica, a liberdade é um direito sagrado, merecedora da mais refinada proteção. Ocorre que, no uso indiscriminado da liberdade, certos agentes a usam com intenções maliciosas na Internet, acabando por ferir (principalmente mediante opiniões desrespeitosas) consideravelmente a dignidade de seus iguais. O resultado disso é o impulso das estatísticas criminais, consequentemente apoiada pelas novas modalidades de delitos praticados na Internet.

Ademais disso, pelo país ser aberto ao mundo, se torna então consumidor dos mais variados produtos produzidos em diversas partes do mundo. O Brasil é um dos maiores mercados consumeristas do mundo quando se trata de Internet. Segundo Abdala (2023):

> “O uso da internet chegou a 87,2% da população brasileira em 2022, um aumento de 21,1 pontos percentuais em relação a 2016, usada por 66,1% da população. Os dados são da Pesquisa Nacional por Amostra de Domicílios Contínua – Tecnologia da Informação e Comunicação 2022 (Pnad), divulgada nesta quinta-feira (9) pelo Instituto Brasileiro de Geografia e Estatística (IBGE).” (ABDALA, 2023. s/p)

Dentre os bens de consumo comumente adquiridos pelos brasileiros, grande parte se utiliza de Internet. Enquanto mais pessoas se inserem no mundo digital, concomitantemente maior se torna o número de possíveis vítimas do cibercrime.

Assim, conforme a sociedade vai se tornando cada vez mais relacionada ao mundo digital, a possibilidade de captura de diversas vítimas é facilitada aos criminosos virtuais. A implicação dessa realidade caminha de mãos dadas à inércia com que o sistema legislativo brasileiro se adapta à novas realidades de convívio social, dado a falta de leis claras sobre a matéria. Nesse ponto, não se deseja uma inflação legislativa, no sentido de regulação de todo e qualquer fato banal da vida, inclusive daqueles não merecedores de regulação, mas sim uma legislação certeira e específica, que não deixe de lado tema crucial. Fala-se do acompanhamento atento e responsável da legislação diante das transformações inéditas decorrentes da Internet, junto do aperfeiçoamento de tecnologias acessórias, responsáveis pelo surgimento de novos fatos no âmbito da comunidade.

Tendo em vista a imprescindibilidade das relações sociais, precipuamente no sentido de troca de informações, que dão engajamento ao bom funcionamento do organismo social, se justifica a atenção aos possíveis problemas oriundos do uso mal-intencionado da Internet. A partir do uso mal-intencionado da Internet, a configuração de determinados delitos se impõe, causando dano legal, de modo que, caberá ao Estado o uso do procedimento legal pertinente, isto é, um processo criminal, que resultará ou não em punição ao autor (DAMÁSIO, 2016). Nesse sentido, percebe-se que, a relação entre Internet e Direito é estreita, no sentido de que os atos jurídicos da vida começaram a tomar novas características com o advento do uso da Internet, seja no âmbito civil, como a propagação de contratos, relações de consumo, etc., seja em âmbito criminal, vide a propagação de condutas tipificadas.

4. O CIBERCRIME NOS DIPLOMAS CRIMINAIS

O cibercrime, embora essa nomenclatura não seja expressa na legislação, é conduta reprovada pelo Direito, tendo contemplação penal na alçada da legislação circunspecta (Dec. Lei 2.848 de 1940), bem como em diplomas especiais. Infelizmente, o avanço da tecnologia trouxe novas formas de aplicação dos delitos já existentes (SOARES, 2019). Em seguida, o trabalho passa a aduzir alguns tipos penais específicos, visando concretude do tema.

4.1. Invasão de Dispositivo Informático/Furto de Dados; Dano e Estelionato

A configuração do delito de invasão de dispositivo informático/furto de dados, se dá mediante a obra do autor do injusto quando da invasão de dispositivo alheio, sem a devida autorização do proprietário, que se torna vítima do injusto penal, podendo ser pessoa física ou jurídica, bem como instituições privadas ou públicas. Visa-se fins ilegais, tais como furto de dados, obtenção de informações privilegiadas, etc. Este tipo está previsto no artigo 154-A do CP, o qual fora adicionado na legislação com a edição da lei 12.737 de 2012, esclarecendo que sua configuração ocorre nos casos em que se tem a invasão de aparelho eletrônico para que dados de privacidade, de informações bancárias, de sigilo profissional e, semelhantes, sejam subtraídos, furtados, adulterados, e até mesmo que o dispositivo eletrônico mantenha-se propício à invasão de Vírus (*softwares maliciosos*).

Mediante tais ações, urge destacar a exposição de dados íntimos da vítima, com o qual o autor possa dar ensejo à prática do crime de estelionato, cuja tipificação encontra-se prevista no artigo 171 do CP. Outro destaque constante aborda sobre a sutileza da conduta, que pode passar despercebida em algumas situações, dando ensejo à impunidade e consequente reiteração da conduta (KUNRATH, 2017). Uma vez munido o ofensor com dados de privacidade da vítima, o crime de estelionato, previsto no artigo 171, pode facilmente se configurar, haja vista a facilidade de contato entre vítima e autor, proporcionado pela Internet. Nesse ínterim, cita-se outra possibilidade, que pode desaguar com o crime de dano, previsto no artigo 163 do CP, ao ponto da conduta que vise, mediante a Internet, destruir patrimônio intelectual alheio, visto o alto valor de bens imateriais contidos na Rede.

4.2. Calúnia, Racismo (de todas as espécies), Difamação e Injúria (Crimes contra a honra); Ameaça e Violação de Direitos Autorais

No âmbito do ciberespaço, como enfatizado desde o início do presente trabalho, é meio que decorre relativo sucesso na consumação de diversas condutas reprovadas pela legislação criminal, de modo que, a conduta típica, antijurídica e culpável encontra potencial chance de sucesso com o emprego da tecnologia de informação. Os crimes de calúnia, racismo, injúria e difamação são crimes que se tornaram cada vez mais rotineiros na Internet.

O crime de racismo encontra assento no artigo 20 da Lei 9.459 de 1997, o qual se constitui como um dos mais comuns no espaço virtual. Com o emprego da Internet, a mancha do racismo (de raça, cor, etnia, religião ou procedência nacional) estrutural na sociedade infelizmente tende a se fortalecer, haja vista a facilidade com que o racista encontra na propagação de seu ódio na Internet (por ter longo alcance e, com isso, impactar uma

quantidade significativa de pessoas ou grupos), principalmente via perfis falsos em redes sociais.

A calúnia está prevista no artigo 138 do CP, configurando-se ao momento em que um indivíduo é acusado em público por uma infração que não cometera, isto é, imputação de um crime a uma pessoa, em se sabendo que ela é inocente. No mesmo sentido, o crime de difamação, previsto no artigo 139 do CP, se dá mediante a imputação de fatos ofensivos a alguém, visando que a pessoa da vítima seja menosprezada pela comunidade. No crime de injúria, previsto no artigo 140 do CP, ocorre a ofensa da honra e da integridade da vítima através de comentários perniciosos na Internet.

O crime de ameaça está disposto no artigo 147 do CP, que, em relação à Internet, tende a ser facilmente perpetrada, haja vista a grande propagação proporcionada pela Internet. Dá-se violação ao direito autoral, crime previsto no artigo 184 do CP, e em especial no âmbito da Internet, pela facilidade de consulta a diversos acervos guardados na Rede, aumentando-se o risco da conduta pela deflagração, na própria Internet, de conteúdos não autorizados.

4.3. Crime de Pornografia Infantil na Internet

O crime de pornografia infantil na internet é o responsável por fomentar o delito da pedofilia. Tendo sua previsão legal no Estatuto da Criança e do Adolescente (Eca, Lei Nº 8.069, de 13 de julho de 1990), é o delito que se evidencia quando da prática de se tirar fotos, fazer cenas, etc., envolvendo pornografia ou sexo explícito, com a presença de crianças. Desse modo, o artigo 241-B do ECA se tornou o dispositivo responsável por tratar dos crimes de aquisição de pornografia infantil.

5. A INTERPRETAÇÃO DA LEGISLAÇÃO CRIMINAL DIANTE DOS CIBERCRIMES

O cibercrime tem demandado do Estado uma análise acurada dos problemas perpetrados na sociedade. Diante disso, com vista às transformações sociais, políticas e tecnológicas, há diversos esforços dos mecanismos criminais, no sentido de adequação às necessidades demandadas por tais transformações. A transformação social é responsável pelo surgimento de problemas complexos, pois, tratar do ser humano nunca foi tarefa simples. Atento ao quociente humano, o Direito Criminal e seus operadores tendem a adotar medidas

que previnam o impacto do cibercrime, já que este vem se adaptando em proporção às novas formas de interação social.

Com isso, surge a clara percepção de que, atualmente, o cibercrime representa um desafio à aplicabilidade do Direito Penal e Processual Penal, não sendo satisfatório adotar apenas uma ou outra medida, mas sim um conjunto das que forem mais adequadas e estejam de acordo com o Ordenamento Jurídico, suas garantias e seus princípios. Nesse sentido, o legislador tende ao direcionamento da interpretação progressiva, haja vista seu caráter evolutivo, que nas palavras de Lima (2020), *verbis*:

> Considera-se interpretação progressiva (adaptativa ou evolutiva) como aquela que busca ajustar a lei às transformações sociais, jurídicas, científicas e até mesmo morais que se sucedem no tempo e que acabam por interferir na efetividade que buscou o legislador com a edição de determinada norma processual penal. (RENATO BRASILEIRO DE LIMA, 2020, P. 98).

Neste cenário, busca-se aplicar soluções imprescindíveis para a consolidação de um sistema de justiça realmente eficiente, razoável, justo e condizente com as reivindicações contemporâneas. Seja na ótica da legislação material, com a criação e estruturação de novos tipos incriminadores (SOUZA, NETO; 2009), seja na legislação processual, em se aperfeiçoando o rito processual, para que se torne justo e efetivo.

Em uma sociedade organizada, regida por um sistema de normas efetivas, um de seus focos principais precisa se direcionar ao aperfeiçoamento do sistema penal e processual penal. Em caso de não compatibilidade entre a legislação criminal e as demandas atuais, a população ficará à mercê dos riscos que ameaçam sua qualidade de vida. Entre os riscos advindos da contemporaneidade, o uso mal-intencionado de tecnologias não pode ser descartado, pelo fato de que, com o emprego desse novo meio, que facilita a vida, o trabalho, a informação, dentre tantos outros, em proporção se coloca o risco de inefetividade dos instrumentos de repressão de condutas típicas. Não há escassez de pensamentos que se orientam no sentido de que, quanto maior o avanço tecnológico, concomitantemente maiores serão as possibilidades destrutivas acessíveis ao indivíduo.

Essa situação é precária ao ponto de que pode ocorrer de um indivíduo, sem necessariamente estar apoiado em um grupo criminoso, dar efetividade a práticas criminosas das mais perigosas possíveis (por exemplo, criação de bombas nucleares; a criação de vírus geneticamente causadores de peste), apenas com o apoio da tecnologia. A sociedade global, continental, estadual e local, fica em risco diante dessas situações, tendo em vista a venerabilidade da dependência da tecnologia, ao ponto de que poucos apagões poderiam

causar literalmente uma anarquia. Bom exemplo disso está na prática do “bioterror”, que certamente poderá gerar milhares de vítimas mundo afora.

Dessa maneira, a legislação criminal (vide Código Penal e de Processo Penal, e demais) não pode permanecer estagnada, ou carente de interpretação progressiva, pois, do contrário, estaria de certa maneira com relativa inutilidade diante das atuais práticas criminosas. O rechaço ao cibercrime tende a ocorrer equanimemente, vide a urgência de abordagem compatível da legislação frente aos desafios da atualidade. Nenhuma camada da sociedade propende ao esquecimento, de modo que a inclinação das novas necessidades legislativas se direciona ao atendimento das novas formas de interação (via Internet), e a aderência das já existentes ao mundo digital. Nesse diapasão, o princípio da isonomia, que nas palavras de Junior (1999) trata-se de “dar tratamento isonômico às partes significa tratar igualmente os iguais e desigualmente os desiguais, na exata medida de suas desigualdades” (NERY JUNIOR, 1999, p. 42), sendo verdadeira base principiológica tão cara ao sistema jurídico brasileiro, restará efetivado.

6. DESAFIOS ENFRENTADOS NA PERSECUÇÃO PENAL DOS CIBERCRIMES

A facilidade encontrada pelo cibercriminoso para praticar crimes na internet vem se tornando algo comum. Embora o país detenha normas específicas que guarnecem o tema, elas ainda carecem de uma abordagem mais completa e dinâmica, que englobe toda a ação do indivíduo que pratique o ato criminoso. Nesse sentido, Soares (2019) exemplifica de modo claro uma das questões prejudiciais: “Imagine-se um cracker que reside na Argentina, invadindo uma empresa americana, se utilizando de um provedor na Inglaterra, causando prejuízos efetivos na China” (DANIEL MENAH CURY SOARES, 2019. s/p).

Em análise da legislação pertinente, o artigo 5° do Código Penal, menciona que a todo crime praticado em território nacional haverá de ser aplicada a legislação penal brasileira. Outrora, sendo o ato criminoso praticado no âmbito digital, a lei nacional será aplicada se a página da Rede utilizada para o crime for também nacional. Caso o criminoso seja brasileiro e, se utilize de meios caracterizadamente estrangeiros para praticar o delito, sem que se verifique sua identidade, levantam-se dúvidas sobre a aplicabilidade da legislação, podendo tornar o processamento embaraçoso. Isso pode caracterizar uma fragilidade, pelo qual acaba incentivando o cibercrime, tendo em conta os pontos que favorecem sua prática, como a exterritorialidade, anonimato, dificuldade de identificação do local físico onde o criminoso

esteja executando a conduta, et. al. Nas palavras de Moura (2021), ao relacionar a questão que envolve a equação custo/benefício dessa natureza de crime, ensina que:

> "a desterritorialidade, o anonimato, a mínima chance de cair nas malhas do controle formal, a falta de aparelhamento da polícia e os impedimentos tecnológicos aliados aos altíssimos lucros obtidos promove um crescimento exponencial deste tipo de criminalidade, fazendo valer o risco por parte do criminoso." (MOURA, 2021, p. 123)

O crime consumado em recinto totalmente digital reivindica a seguinte questão: Pelo princípio da territorialidade, que se baseia numa dimensão espacial física para determinar a competência do juízo (competência em razão do território), qual o raciocínio a ser tomado na incidência do cibercrime? Com este tipo de pergunta, surge diversos empecilhos, entre os quais, de quem será a competência para a investigação? Ou, jurisdição para processo e julgamento do agente?

Condutas como a invasão de sites, dados bancários, contas pessoais e até vídeos ou fotos divulgadas na internet, sem autorização, caracteriza crime cibernético, e nesse sentido, o cibercriminoso, por estar atrás de um computador, tem a enganosa impressão de total anonimato. A falta de conhecimentos técnicos em questões estritamente tecnológicas, em muitos casos, por parte das autoridades, enseja a ideia de que o agente criminoso esteja "um degrau" acima dos mecanismos de combate proporcionados pelo Estado. Por outro lado, estando em ordem os meios de comprovação do tipo penal e da materialidade do fato, a propositura da denúncia junto ao Poder Judiciário ficará ao crivo do Ministério público, que tende a analisar a licitude e pertinência das informações necessárias à propositura da daquela (denúncia), se for o caso. Dado que, não se pode imputar uma acusação a um indivíduo sem a precedência de um inquérito provido de legalidade.

Por conseguinte, há de fato um amplo caminho a se percorrer. O Direito Criminal vem encontrando variados desafios com o advento célere das transformações tecnológicas e de questões prejudiciais proporcionadas pelos cibercrimes (em constante evolução). Desafios como a cooperação Internacional aliada às questões jurisdicionais, o anonimato e a dificuldade de identificação dos criminosos, a dificuldade de autenticidade de provas digitais devido a sua grande facilidade de manipulação. A estagnação legislativa também protagoniza a inaplicabilidade aos novos casos. Em somatório, com a evolução rápida das camadas digitais, o despreparo do Estado frente às novas modalidades de delitos na Rede pode representar prejuízo na tutela de uma gama de direitos individuais relacionados à privacidade de suspeitos e de vítimas.

6.1. Questões gerais acerca de jurisdição e competência

É comum o fato de que os crimes virtuais sejam praticados em jurisdição diversa de onde a consumação tenha-se dado. A jurisdição significa o poder de ditar o direito abstrato ao caso concreto, à luz da distribuição da competência. O título V do Código de Processo Penal estabelece as regras de competência. Para Lima (2020), a jurisdição pode ser compreendida, *in verbis*:

> Como função estatal exercida precipuamente pelo Poder Judiciário, caracteriza-se a jurisdição pela aplicação do direito objetivo a um caso concreto. Como função estatal que é, a jurisdição é una (princípio da unidade da jurisdição), o que, no entanto, não significa dizer que um mesmo juiz possa processar e julgar todas as causas. Com efeito, nem todos os juízes podem julgar todas as causas, razão pela qual motivos de ordem prática obrigam o Estado a distribuir esse poder de julgar entre vários juízes e Tribunais. Dessa forma, cada órgão jurisdicional somente pode aplicar o direito objetivo dentro dos limites que lhe foram conferidos nessa distribuição. Essa distribuição, que autoriza e limita o exercício do poder de julgar no caso concreto, é a competência. (RENATO BRASILEIRO DE LIMA, 2020, p. 413).

Diante dessa implicação, a questão se embasa na determinação do juízo que deterá competência dentro da distribuição de competência, tendo em vista extirpar supostas nulidades processuais na persecução do cibercrime (haja vista a nebulosidade quando da definição da competência em crimes virtuais nos casos em que não se pode definir o local de residência da vítima). Na arena internacional, em se falando de limites jurisdicionais, percebe-se que há a necessidade da cooperação jurídica Internacional entre os países que potencialmente venham ter suas jurisdições demandadas pelo fato delituoso. Nessa linha, Soares (2016) corrobora ao expor que:

> Uma das características marcantes dos crimes informáticos é a transnacionalidade, o que significa que uma pessoa de qualquer cidade, estado ou país pode cometer crimes contra qualquer pessoa conectada à rede, não importando o local onde a vítima e o agressor se conectam. Isso trás problemas quanto à questão da territorialidade do crime. Apesar dessa "quebra de fronteiras", cada país possui a sua própria soberania acerca da investigação e punição à crimes informáticos. Imagine-se um cracker que reside na Argentina, invadindo uma empresa americana, se utilizando de um provedor na Inglaterra, causando prejuízos efetivos na China. Onde ele seria julgado? E se um dos países envolvidos não prevê punição para aquela conduta criminosa, enquanto outro o faz? A consumação do crime se daria em todos os locais onde a rede é acessível? A resposta para tais questionamentos não são fáceis e as soluções seriam complexas. A maioria dos países do mundo adotam, acerca do local do crime, o "Princípio da Ubiquidade" (considera-se local do crime tanto onde houve a conduta quanto onde ocorreu o resultado). (SOARES, 2019, s/p)

Para além da indicação da jurisdição nacional competente (após a sua determinação), urge a pergunta: A qual juízo recairá a competência para seu regular processo e julgamento? Pela regra de competência do artigo 69 do CPP, ela será determinada pelo local da infração do crime, pelo local de domicílio ou residência do réu, pela natureza da infração, pela distribuição, pela conexão ou continência, pela prevenção ou pela prerrogativa de função. Porém, quanto ao cibercrime, como ficaria? Sabendo-se que, os elementos citados pelo artigo 69 do CPP não são fáceis de serem determinados na incidência daquele.

6.1.1. Competência criminal nos cibercrimes impetrados no âmbito nacional

A respeito da competência criminal perante os crimes cometidos no ciberespaço, busca-se avaliar o juízo responsável pelo processo e julgamento de uma eventual ação. A competência será deduzida após análise do caso concreto. Em acordo com o artigo 6° do Código Penal (CP), considera-se o local do crime o mesmo em que aconteceu a ação ou omissão, parcial ou totalmente, tal como onde se produziu ou deveria produzir-se o resultado. Todavia, no que tange ao cibercrime, muitas vezes a sua manifestação pode se dar em múltiplos locais, dificultando-se a identificação de qual foro teria competência para a persecução penal.

Seguindo a linha de raciocínio do artigo 6° do CP, segue-se em análogo entendimento o artigo 70 do CPP, segundo o qual a competência para a persecução penal será do local onde foi consumada a infração. À vista disso, interpreta-se que a regra da competência é a do foro do local da infração, assim dizendo, o referido artigo traz à baila regra determinadora da competência em vista do lugar em que se efetivar a infração. Noutro giro, em caso de tentativa, a competência recairá ao foro do local onde se praticou o derradeiro ato de execução.

A regra do artigo 70 do CPP externa o entendimento de que a competência se dá principalmente pelo local onde houve a consumação da infração, ou em caso de tentativa, do local onde ocorreu o ato final relacionado à execução. A redação do artigo 70 e seus parágrafos é certeira e clara ao dispor sobre as regras de competência nos crimes convencionais. Segundo leitura do §2° do art. 70 do CPP, a competência determinar-se-á pelo local em que o crime tenha sido parcialmente produzido, no caso em que o último ato de execução tenha sido praticado fora da jurisdição brasileira, ou seja, competente será o juízo do local onde intencionou-se a produção do resultado. Porém, enfatizando o fato de que crimes genuinamente digitais dispensam consumação em locais físicos, e que este pode se consumar

com a sua simples propagação via Internet, torna-se demasiadamente complexa a aplicação da regra do artigo supracitado.

6.1.2. Entendimento do STJ acerca de conflito de competência

O STJ (Superior Tribunal de Justiça) já se posicionou sobre a questão envolvendo conflito negativo de competência, quando da prática de delitos na Internet, a partir do início de advento dos aplicativos populares de comunicações, dado no início da década passada. Nesse sentido, segue-se:

> CRIME CONTRA A HONRA PRATICADO PELA INTERNET. NATUREZA FORMAL. CONSUMAÇÃO NO LOCAL DA PUBLICAÇÃO DO CONTEÚDO OFENSIVO. COMPETÊNCIA DO JUÍZO SUSCITANTE PARA O CONHECIMENTO E JULGAMENTO DO FEITO. 1. 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. 2. Conflito conhecido para declarar a competência do Juízo suscitante para o conhecimento e julgamento do feito. (STJ - CC: 173458 SC 2020/0171971-7, Relator: Ministro JOÃO OTÁVIO DE NORONHA, Data de Julgamento: 25/11/2020, S3 - TERCEIRA SEÇÃO, Data de Publicação: DJe 27/11/2020)

Concomitantemente, em caso semelhante envolvendo conflito de competência de medida protetiva (CC: 0003836.68.2016.8.16.0011), no qual a vítima do injusto penal residira em Naviraí/MS, e o autor de reiteradas ameaças em Curitiba/PR, via aplicativos de comunicação populares como o WhatsApp e o Facebook, o Relator ministro Marco Aurélio Bellizze Ribeiro Dantas, deliberou em condizente cognição.

6.2. Escorço sobre as provas digitais

Quando se trata de processo penal, um dos elementos essenciais à persecução criminal cuida-se do elemento de prova. Conforme menciona Auri Lopes Jr., “o processo tem por finalidade buscar a reconstituição de um fato histórico (o crime sempre é passado, logo, fato histórico), de modo que a gestão da prova é erigida a espinha dorsal do processo penal” (2020, p. 577). Na legislação processual penal, consta no artigo 155 que a formação da convicção do juiz se dará pela livre apreciação da prova produzida por meio do contraditório judicial.

Exceto nos casos de provas cautelares, não repetíveis e antecipadas, o juiz não poderá fundamentar sua decisão de maneira exclusiva com base nos elementos de informação

colhidos no momento da investigação. Ainda para reforçar, consta no artigo 157 que, provas ilícitas são inadmissíveis, pleiteando-se por seu desentranhamento dos autos. Prova ilícita é aquela obtida em violação às normas constitucionais ou legais. É o que se depreende, segundo Renato brasileiro de Lima, do princípio da inadmissibilidade de admissão de provas ilícitas, em acordo com o artigo 5º, inciso LVI, da Carta Magna de 1988 (2020, p. 71). Ainda segundo o autor, a busca indiscriminada da verdade material era, comumente, usada como argumento justificador de práticas violadoras de direitos, arbitrariedades e condutas antidemocráticas, o que a tornava um valor mais caro do que os valores decorrentes da proteção da Liberdade individual (2020, p. 70). A utilidade da prova se volta para o convencimento de seu destinatário, o juiz, que à luz das evidências aplicará a justiça ao caso concreto. Numa ótica objetiva, Alexandre Cebrian Araújo Reis e Victor Eduardo Rios Gonçalves dizem que "a prova é o elemento que autoriza a conclusão acerca da veracidade de um fato ou circunstância" (2016, p. 288).

De modo semelhante, Lima (2020) diz que, a prova tem diversas utilidades, e dentre elas, a utilidade no sentido probatório da causa, que se define como "a produção dos meios e atos praticados no processo visando ao convencimento do juiz sobre a veracidade (ou não) de uma alegação sobre um fato que interesse à solução da causa" (RENATO BRASILEIRO DE LIMA, 2020, p. 657). Ainda, há destaque para as questões fáticas e/ou jurídicas na fase preliminar (fase inquisitória) submetidas a um juízo valorativo pelo juiz de 1° instância, de modo que, segundo Lima (2020), "não exterioriza nenhum juízo de valor sobre os fatos ou as questões de direito, emergentes nessa fase preliminar, que o impeça de proceder com imparcialidade no curso da ação penal (RENATO BRASILEIRO DE LIMA, 2020, p. 269). Pois bem, a prova nos crimes de natureza digital pode apresentar grandes desafios ao exercício desse direito tão caro ao sistema democrático, tendo em vista a facilidade com que pode sofrer manipulações, afetando todo o processo penal, de tal modo que a prestação jurisdicional fique corrompida, externando uma verdadeira injustiça.

À autoridade exige-se dinamismo na apuração, em virtude da volatilidade das evidências probatórias havidas do âmbito digital, contra o intuito célere voltado a excluir, alterar e ocultar tais provas, por parte do cibercriminoso ou terceiro. Desafio merecedor de destaque diz respeito às possibilidades de obtenção de provas ilícitas pelas autoridades competentes, em contraposição aos direitos e liberdades individuais, o que é comum quando se há a violação da privacidade, da intimidade, e de questões pessoais sensíveis do investigado. Os desafios na investigação podem levar a dificuldades também no desenrolar do processo. É preciso que se corte na raiz a prova ilícita, haja vista o protagonismo da

persecução criminal em compatibilidade com as garantias fundamentais. Dado a importância da prova no sistema democrático, merece destaque a observação *cautelar* das provas em cibercrimes, evitando-se a impunidade da conduta do agente, e a efetividade na tutela dos direitos dos envolvidos (em represália à exposição demasiada de dados sensíveis).

6.3. Tutela dos direitos individuais em sede de investigação

No escopo de levantamento probatório, verifica-se a constância de medidas intrusivas, tais como monitoramento indevido, interceptação de comunicações privadas, levantando questões acerca da violação de privacidade de suspeitos investigados supostamente pela prática do cibercrime. A proteção dos direitos fundamentais, como a dignidade da pessoa humana, ampla defesa e o contraditório, bem como a presunção de inocência, assegurados na Constituição de 1988 e no âmbito da legislação infraconstitucional, precisam ser observados em sede de persecução penal.

Concebe-se que, quando se trata de violação dos direitos individuais do investigado, comumente a violação se manifesta através de colhimento ilegal de prova. Nas locuções de Renato Brasileiro de Lima, “a prova será considerada ilegal sempre que sua obtenção se der por meio de violação de normas legais ou de princípios gerais do ordenamento, de natureza material ou processual” (RENATO BRASILEIRO DE LIMA, 2020, p. 685).

Com foco no artigo 155 do CPP, o juiz, por ter o encargo de formação da sua convicção com base em apreciação probatória havida em contraditório judicial, deve verificar a constância do respaldo aos direitos individuais do acusado. Desse modo, a prova produzida sem a observação das normas, além de violarem os direitos individuais, não merecem apreciação jurisdicional. Conforme se extrai da súmula 523 do STF, a qual externa que, “no processo penal, a falta de defesa constitui nulidade absoluta, mas a sua deficiência só o anulará se houver prejuízo para o réu”, seu conteúdo configura-se outro questão de ordem. No contexto dos cibercrimes, não raro pode ocorrer da autoridade investigativa colher elementos probatórios em violação a direitos individuais, precipuamente os de ordem personalíssima, v. g., a privacidade, intimidade, etc.

Caracteriza-se por prova ilícita, derivada de ilícita (CPP, art. 157, e §1°), ou semelhantes, as provas reproduzidas sem a observância da proteção dos direitos individuais do acusado. No tocante à vítima, há também o risco de se constatar violação a seus direitos individuais, caso em que o elemento probatório seja verdadeiro mecanismo de aumento de

intensidade de sofrimento desta. A questão merece atenção, dado que a falta de sua observação prejudica a aplicação do §5° do artigo 157 do CPP.

6.4. Dificuldades apresentadas pelo anonimato da conduta

A complexidade dos cibercrimes apresenta diversos empecilhos dificultadores da identificação do agente. Os cibercriminosos comumente dão vida à conduta delituosa em anonimato, ou através de camadas de tecnologia que lhes facilita a ocultação, tornando difícil para as autoridades a deflagração de sua identidade. Identificá-los, achá-los, rastreá-los, e, tarefas semelhantes, são verdadeiros desafios.

Sabe-se que para o Processo Penal é determinante o reconhecimento de pessoas. O julgamento do *Habeas Corpus* nº 598.886/SC (STJ, relator ministro Rogério Schietti Cruz, 6ª Turma, j. 27/10/2020), jogou ainda mais luz sobre o tema do reconhecimento de pessoas no âmbito do processo, fazendo com que se impulsionasse nova jurisprudência no sentido de consolidação da força cogente do procedimento prescrito no artigo 226 do CPP, que reforça o reconhecimento de pessoas. Noutro tempo, a jurisprudência ponderava a questão como simples orientação do legislador. Acontece que, na prática de delitos remotos via Internet, o reconhecimento de pessoas é algo não sustentável, ou quase completamente inaplicável, tendo em vista a dúvida sobre a autoria de pessoa humana (caso haja a presença humana na efetivação da conduta) ou apenas maquinações de tecnologias de Inteligência Artificial programadas para tal.

Essa questão representa outro desafio para o Direito Criminal, dado que, nas palavras de Jardene Braz (2023), “a preocupação que surge é na dificuldade de identificar os indivíduos que cometem crimes no âmbito da informática, tendo em vista que são vários meios utilizados para a perpetração da conduta ilícita, e podem ser facilmente apagados.” (JARDENE BRAZ, 2023, *s/p*).

Evidentemente, pela falta de mecanismos precisos no tocante à identificação do agente, a impunidade se impõe. Nesse caso, reconhecida a materialidade do delito e, não decifrado o agente, para que posteriormente seja imputada a autoria, pode resultar em impacto negativo perante a sociedade, por gerar sensação de ineficácia da legislação criminal; risco de reincidência do agente, vide a crença na impunidade; pressão demasiada às autoridades, dado o descontentamento da sociedade; e, ademais disso, a frustração suportada pela vítima.

6.5. Histórico legislativo recente sobre o tema

A sociedade está constantemente em processo de mudança. Seja no contexto de convívio privado, profissional, social e interativo, a tecnologia e seus equipamentos são atualmente indispensáveis no dia a dia das pessoas. Doravante essa nova realidade, concebe-se que normas desatualizadas e retrógradas são insuficientes no exercício da alçada regulatória. Sobre o tema, Vianna (2013) diz que, o grande desafio enfrentado pelo país, no contexto dos cibercrimes, é a falta de legislação específica (TÚLIO LIMA VIANNA, 2013, *s/p*).

Conforme os anos passam, novos meios de inserção à Internet são criados, e com eles, o desenvolvimento indesejado de novos delitos ou a inserção dos já existentes. Segundo Braz (2023), a situação se agrava quando ocorre "a omissão na edição de tipos penais de alguns ataques cibernéticos; a falta de uma legislação específica, bem como a insuficiência na organização tecnológica do Sistema de Justiça para efetivação das investigações" (JARDENE BRAZ, 2023, *s/p*). As normas penais e processuais penais devam acompanhar o ritmo de desenvolvimento da nova realidade social, amplamente influenciada pelos equipamentos tecnológicos conectados à rede (Internet).

Outrora, pelo fato de que praticamente todo e qualquer crime comum pode ser cometido na Internet, para além dos diplomas legais já existentes como o Código Penal e o Código de Processo Penal, o legislador vem seguindo noções acerca da normatização do tema, visando alcançar, pelo menos em tese, a plenitude de tratamento. Com o propósito de se resguardar de uma possível crise normativa, em razão do emergente tratamento das dificuldades técnicas existentes na persecução penal dos cibercrimes, o legislador brasileiro inclina-se cada vez mais ao embate dos delitos dessa natureza, junto do extenso rol de institutos jurídicos (por exemplo: com a edição de leis específicas, caso da lei n° 12.737 de 2012, que dispõe sobre a tipificação criminal de delitos informáticos). Com o advento da referida lei, acrescentou-se ao Código Penal os artigos 154-A e 154-B, elegendo os tipos penais por "invasão de dispositivo informático".

Dessa forma, a lei 12.737/2012 (chamada lei de crimes cibernéticos), trouxe alterações no Código Penal brasileiro e, com isso, iniciou-se, ao menos, um caminho para providências relacionadas ao problema. Urge ressaltar a alteração da redação dos artigos 266 e 298 do Código Penal, também oriunda da lei 12.737/2012. Outrossim, vale mencionar que em 2014 houve a edição do Marco Civil da Internet, regulamentado pela Lei 12.965, o qual estabelece princípios, garantias, direitos e deveres para o uso da Internet em território brasileiro. Mais recentemente, o legislador brasileiro, em atenção a essas questões, editou norma pertinente ao

tema, posto isso, entrou em vigor a lei 14.155 de 2021, com a premissa de se alterar o Código Penal brasileiro, tornando mais graves os crimes de violação de dispositivos informáticos, crimes de estelionato cometido de forma eletrônica ou pela Internet, e inclusive a alteração do Código de Processo Penal, para definir a competência nessas modalidades de crimes, que passou a ser do foro do local de domicílio da vítima (quando da incidência de cibercrimes impróprios ou mistos), outrora, determinando-se a competência pela prevenção, no caso de pluralidade de vítimas.

6.6. Excerto acerca da responsabilização criminal de menores

O estereótipo comumente deduzido do cibercriminoso é o de que ele seja um(a) adolescente com refinados conhecimentos informáticos. Se assim for, haverá uma tendência de criminalização e perpetração de medidas criminais contra pessoas menores de idade, em vista do aumento dessa modalidade de crime. Na contramão, sabe-se que a maioridade penal se inicia aos 18 anos (artigo 228 da Constituição Federal de 1988), ou seja, negativa de aplicação da persecução penal.

O Estatuto da Criança e do Adolescente (Lei Nº 8.069, de 13 de julho de 1990), por ter sido editado nos anos noventa, ou seja, em um contexto fora de questões atinentes à tecnologia, carece de aperfeiçoamento em relação ao problema posto, de modo a se criar meios de responsabilização e reeducação compatíveis com a Constituição, rechaçando-se interpretação desfavorável aos menores. O tema é emergente, dado que a juventude atual (menores de 17 anos) está fortemente inserida no mundo digital e, isto os faz ser uma geração constituída de “nativos digitais”.

CONSIDERAÇÕES FINAIS

De fato, o Ordenamento Jurídico brasileiro está em etapas iniciais no tocante ao tratamento dos fatos oriundos da nova realidade (entre eles, os cibercrimes). Uma das frentes tem sido a edição de normas (por exemplo, das Leis n. 12.735/2012; n. 12.737/2012; n. 12.965 e 13.260/2016; n. 13.709/2018; e, n. 14.155/2021, e outras). No entanto, ainda há a falta de medidas regulatórias concretas, que podem ser solucionadas com a tomada de pautas interdisciplinares e jurídicas sobre o tema. Ressalta-se a importância da interdisciplinaridade pelo fato de existência de ilícitos que potencialmente se configurem como penais, previstos em outros ramos jurídicos, *v. g.*, os ilícitos na celebração de contratos virtuais, onde não se

tem legislação criminal específica. Por ficar vedado ao operador do Direito incorrer em analogia incriminadora, segundo os princípios do processo criminal, é preciso que se debata a matéria, evitando injustiça, ou, falta de razoabilidade, por não ser aceitável, de um lado, a punição injusta e desumana, e por outro, demasiada impunidade. É imprescindível a sinergia entre a comunidade e as instituições democráticas (via seus representantes), para que se caminhe no sentido de aperfeiçoamento dos instrumentos normativos e dos institutos jurídicos.

Além das precauções que cabem às pessoas, quer dizer, das medidas básicas que todo usuário de Internet deve tomar, *e. g.*, estar sempre alerta, adotar hábitos cuidadosos, entre outros, é importante entender os desafios privativos das instituições, das autoridades, dentre outros, que versam sobre o aperfeiçoamento da efetividade dos mecanismos preventivos. Por conseguinte, é evidente a dedicação do legislador em se manter interessado na tutela dos direitos das pessoas (física ou jurídica), vítimas do cibercrime. Diante do dilema de combate aos cibercrimes, tendo em vista uma de suas possíveis características, a transnacionalidade, demanda-se uma resposta integral e coordenada entre os países. Assim, seja no plano interno e/ou internacional, a coibição de lacunas legislativas é questão dotada de primazia.

O Poder Legislativo tem papel crucial frente ao problema, por ser o responsável pela criação das normas. Entretanto, como o problema salta aos entornos jurídicos, como a evidência de complexidades que acarretem a dificuldade de detecção do agente que age por meio da Rede, as demais instituições do Estado tendem a exercer papel crucial nesse embate (cada qual na medida de sua responsabilidade), haja vista a possibilidade de criação de órgãos de coibição de delitos, preparação das autoridades e, quando da aplicação das normas (parte que compete ao Poder Judiciário), um raciocínio que seja razoável, efetivo e constitucional.

REFERÊNCIAS

Lima, Renato Brasileiro de. Manual de processo penal: volume único / Renato Brasileiro de Lima – 8. ed. rev., ampl. e atual. – Salvador: Ed. JusPodivm, 2020.

Badaró, Gustavo. Direito processual penal: tomo II / Gustavo Badaró. – 2. ed. atual. – Rio de Janeiro: Elsevier, 2009.

Reis, Alexandre Cebrian Araújo. Direito processual penal esquematizado® / Alexandre Cebrian Araújo Reis, Victor Eduardo Rios Gonçalves; coordenador Pedro Lenza. – 5. ed. – São Paulo: Saraiva, 2016.

Nucci, Guilherme de Souza. Curso de direito processual penal / Guilherme de Souza Nucci. – 17. ed. – Rio de Janeiro: Forense, 2020.

MOURA, Grégore Moreira de. Curso de Direito Penal Informático. Belo Horizonte: D'Plácido, 2021.

CUNHA, Rogério Sanches. Manual de Direito Penal: Parte Especial. 9ª ed. Salvador: Juspodivm, 2017.

JESUS, Damásio de. MILAGRE, Celso Antonio. Manual de crimes informáticos. São Paulo: Saraiva, 2016. Pag. 49

DAMÁSIO, José Antonio. Manual de Crimes Informáticos. São Paulo: Saraiva, 2016.

BRASIL. Constituição da República Federativa do Brasil. Disponível em https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm

BRASIL. Código Penal. Decreto Lei n. 2.848/40. Disponível em https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm

BRASIL. Código de Processo Penal. Decreto Lei n. 3.689/41. Disponível em https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm

ECA – Estatuto da Criança e do Adolescente – Lei 8069/90 Disponível em https://www.planalto.gov.br/ccivil_03/leis/l8069.htm

Direito administrativo brasileiro / Hely Lopes Meirelles. Imprenta: São Paulo, Malheiros, 2004.

Manual de direito administrativo / José dos Santos Carvalho Filho. – 34. ed. – São Paulo: Atlas, 2020.

Lopes Junior, Aury. Direito processual penal / Aury Lopes Junior. – 17. ed. – São Paulo: Saraiva Educação, 2020.

Lopes Jr., Aury Direito processual penal / Aury Lopes Jr. – 18. ed. – São Paulo: Saraiva Educação, 2021.

Bitencourt, Cezar Roberto Tratado de direito penal: parte geral, 1 / Cezar Roberto Bitencourt. – 17. ed. rev., ampl. e atual. de acordo com a Lei n. 12.550, de 2011. – São Paulo: Saraiva, 2012.

Santos, Juarez Cirino dos Direito penal: parte geral I Juarez Cirino dos Santos. - 6. ed., ampl. e atual. - Curitiba, PR: ICPC Cursos e Edições, 2014.

Curso de Direito Penal Brasileiro / Luiz Regis Prado. – 17. ed. – Rio de Janeiro: Forense, 2019.

SOUZA NETO, P. A. de. Crimes de Informática. Itajaí, 2009

KUNRATH, Josefa Cristina Tomaz Martins A expansão da criminalidade no cyberespaço. Feira de Santana : Universidade Estadual de Feira de Santana, 2017.

Crimes cibernéticos: Brasil é um dos recordistas mundiais. Diponível em https://noticias.r7.com/jr-na-tv/videos/crimes-ciberneticos-brasil-e-um-dos-recordistas

DE CADA 100 brasileiros, 87 usavam internet em 2022, aponta IBGE: Uso da rede subiu de 66,1% em 2016 para 87,2% no ano passado. [S. l.]: Fernando Fraga; Vitor Abdala, 9 nov. 2023. Disponível em: https://agenciabrasil.ebc.com.br/geral/noticia/2023-11/de-cada-100-brasileiros-87-usavam-internet-em-2022-aponta-ibge. Acesso em: 23 mar. 2024.

CRIME Cibernético: da identificação do usuário para efetividade da pena. In: BRAZ, Jardene. Disponível em: https://www.jusbrasil.com.br/artigos/crime-cibernetico-da-identificacao-do-usuario-para-efetividade-da-pena/1664917013. Acesso em: 24 mar. 2024.

VIANNA, Túlio Lima. Dos crimes pela internet. Disponível em: < http://www.academia.edu/1911162/Dos_crimes_pela_internet. Acesso em 24 de março de 2024.

Mena Cury Soares, Daniel. CRIMES informáticos: Uma Breve Resenha e Apontamentos de Complicações. [S. l.], 16 ago. 2019. Disponível em: https://www.migalhas.com.br/depeso/308978/crimes-informaticos--uma-breve-resenha-e-apontamento-de-complicacoes. Acesso em: 23 mar. 2024.

TILIA, CAROLINE DE. 5 crimes digitais que mais ameaçam empresas brasileiras. Forbes: Caroline de Tilia, 24 mar. 2024. Disponível em: https://forbes.com.br/forbes-tech/2024/03/5-ameacas-ciberneticas-que-mais-afetam-as-empresas-brasileiras/?amp. Acesso em: 30 mar. 2024.