Revista Brasileira de Direito e Gestão Pública
www.gvaa.com.br/revista/index.php/RDGP/
ISSN: 2358-2405

A seara penal frente a Era Digital: Existe um direito cibernético processual penal?

The penal harvest in the face of the Digital Age Is there a criminal procedural cyber law?

Igor Aurélio Vieira[1], Nalckson Vinícius Diniz Silva[2], Agílio Tomaz Marques[3] e Rosana Santos de Almeida[4]

v. 11/ n. 3 (2023)
Julho/Setembro

Aceito para publicação em 21/07/2023.

[1]Graduando em Direito pela Universidade Federal de Campina Grande;
[2]Graduanda em Direito pela Universidade Federal de Campina Grande;
[3]Doutorando pela Universidade Federal de Campina Grande, Mestre pela Universidade Federal de Campina Grande, Graduado em Direito pela Universidade Federal do Cariri; Juiz de Direito do Tribunal de Justiça da Paraíba;
[4]Graduanda em Universidade Federal de Campina Grande.

Resumo: Este artigo tem como objetivo fornecer uma visão geral concisa do desenvolvimento histórico da comunicação e suas consequências sociais. Ao estabelecer essa base, ele se aprofundará no debate abrangente em torno do crime e do procedimento criminal. Assim, o foco dessa discussão é a interseção desses dois assuntos no âmbito do ciberespaço. Além disso, para analisar criticamente o arcabouço legal nacional, é imprescindível recorrer a exemplos internacionais e abordar os desafios potenciais para combater efetivamente a cibercriminalidade. Por fim, este artigo irá explorar conflitos de competência e apresentará perspectivas otimistas em relação ao futuro do direito penal no contexto da cibercriminalidade. Para tanto, o avanço tecnológico e a sociedade digital exigem uma abordagem especializada do direito penal e processual penal para enfrentar os desafios emergentes. É necessário, sobretudo, acompanhar de perto as transformações sociais e tecnológicas, garantindo a proteção dos direitos individuais e coletivos no ambiente digital, e promovendo a segurança e a justiça na era digital, tal como bem argumentado por Aristóteles.
Palavras-chave: Crimes cibernéticos; Cibercrime; Processo penal; Territorialidade; Lei n. 12.965/2014.

Abstract: This article aims to provide a concise overview of the historical development of communication and its social consequences. By laying this foundation, it will delve into the overarching debate surrounding crime and criminal procedure. Thus, the focus of this discussion is the intersection of these two subjects within the realm of cyberspace. Furthermore, in order to critically analyze the national legal framework, it is imperative to draw on international examples and address the potential challenges to effectively combat cybercrime. Finally, this article will explore conflicts of jurisdiction and present optimistic perspectives regarding the future of criminal law in the context of cybercrime. To this end, technological advancement and the digital society require a specialized approach to criminal law and criminal procedure to address emerging challenges. It is necessary, above all, to closely monitor social and technological transformations, ensuring the protection of individual and collective rights in the digital environment, and promoting security and justice in the digital age, as well argued by Aristotle.
Keywords: Cybercrime; Criminal procedure, Territoriality, Law no 12.965/2014.

1. Introdução

Em uma sociedade altamente automatizada em que os processos cotidianos estão intrinsecamente vinculados com a atividade digital é impossível não nos questionarmos sobre os direitos e deveres que possuímos nos ambientes virtuais. Porém, sendo mais específico no que tange a este artigo, indaga-se qual é o impacto da rápida evolução tecnológica na sociedade moderna e como isso levanta a necessidade de um direito cibernético e processual penal para abordar os desafios legais emergentes relacionados à atividade criminal no ambiente digital?

O objetivo deste artigo é, portanto, explorar o desenvolvimento histórico da comunicação e suas prováveis consequências sociais, abordando as transformações causadas pela sociedade digital e discutindo a necessidade de um direito cibernético e processual penal para lidar com os desafios legais emergentes relacionados à atividade criminal no ambiente digital. Além disso, o presente artigo busca lançar sob escrutínio a relação entre o avanço tecnológico, o direito penal e o processual penal, analisando a legislação nacional e comparada de crimes informáticos, além de discutir as dificuldades no combate ao cibercrime e a questão da territorialidade do direito digital. Enfim, tentando esgotar a apresentação pode-se dizer que o objetivo final é fornecer uma visão crítica e discutir perspectivas do direito penal cibernético.

Sendo assim, para desenvolver tal assunto fez-se necessário sorver bastante da metodologia histórico bibliográfica, além de obtermos as respostas ao longo deste material por meio do método dedutivo, isto é parte-se de uma premissa maior, o que é uma generalização, para em seguida aprofundar-se na temática.

A estrutura esquelética desta obra se divide em três fragmentos primordiais, na fase inicial tecer-se-á a parte histórica do tema abordado, atribuindo vida fática e cronológica aos eventos que ensejaram este trabalho. Segundamente, discute-se direito de fato, sendo possível classificarmos uma subdivisão deste, pois inicialmente haverá uma abordagem sobre a legislação nacional, incluindo o contexto histórico que desaguou no sistema em voga, finalmente é traçado uma linha que liga comparativamente o Direito internacional e o brasileiro.

Por fim, apresentar-se-á ponderações críticas sobre tudo o que foi abordado, delineando de modo empírico as constatações adquiridas dos estudos provenientes deste tema.

2. A formação das sociedades digitais e sua relação com o direito.

É conveniente retornarmos ao período pré-histórico, em que o homem ainda não era sedentário. Os grupos humanos consistiam em pequenas tribos que se locomoviam de um ponto a

outro em busca não somente buscando recursos, mas também para facilitar a sua sobrevivência, pois vasculhavam a procura de ambientes mais propícios para a sua perpetuação. Não há tantos registros que solidifiquem as nossas acepções a despeito dos costumes e da estrutura desses agrupamentos.

Não obstante, porém adentrando em concepções um pouco mais abstratas, pode-se dizer de cunho filosófico, sobre um período já civilizado da sociedade, refere-se a concepções que seguem os ditames delimitados pelas teorias dos contratualistas Hobbes, Locke e Rousseau. Para os pensadores citados, os homens desenvolveram o Estado a fim de solidificar uma estrutura que garanta a sobrevivência e bem-estar da espécie humana.

Outrossim, em um mundo interconectado parece impossível conceber que num passado não tão distante havia barreiras comunicacionais tamanhas que praticamente pouco se sabia acerca daqueles que vivem longe da comunidade à qual pertencemos. Além disso, é de entendimento notório que as revoluções relacionadas à comunicação geraram uma metamorfose sem precedentes em como as sociedades interagem entre si. Tomemos por base a Reforma Luterana, que só adquiriu proporções suficientes para ir de embate direto às pregações da igreja católica com a invenção da imprensa de Gutenberg.

Ao longo do século XIX, tanto o exército prúsio quanto o exército francês e britânico superaram as armas do antigo regime, além de simultaneamente adquirirem tecnologia suficiente para produzir meios de transporte mais baratos e acelerar as comunicações, o que possibilitou à Europa unificar a superfície do globo. Neste sentido:

> Simultaneamente, o transporte mais barato e a aceleração das comunicações permitiram que os europeus unificassem a superfície do globo, trazendo os países asiáticos e africanos mais fracos para um sistema de mercado gerenciado e centrado na Europa (MCNEILL, 1982, p. 223).[1]

Aliás, o ponto que se tenta traçar é que o desenvolvimento industrial acarreta revoluções tecnológicas e, estas, por sua vez, desencadeiam novas relações comunicacionais. Se o *mens legis* já não é capaz de prever todas as possibilidades advindas das interações sociais de uma dada sociedade com o passar do tempo, como prever o fruto das interações comunicacionais constantes e instantâneas em todo o mundo?

Dessarte, infere-se que o surgimento do Estado se deu naturalmente na sociedade diante da necessidade do estabelecimento da ordem, verifica-se que a sua existência se refere a um ente ontológico ao ser social. Em outras palavras, concordamos com a perspectiva que o Estado, bem

[1] No original: Simultaneously, cheaper transport and accelerated communications allowed Europeans to unify the surface of the globe, bringing weaker Asian and African polities into a European-centered and managed market system

como a ordem social e os costumes, antecedem a condição do homem, e, portanto, estão presentes em qualquer convívio que remeta a seres sociais.

Entre uma das funções precípuas do Estado Moderno, há as dimensões dos direitos fundamentais, que possuem entre suas características a historicidade. Isto é, surgem com o decurso do tempo, não tem origem em um específico ponto no tempo. Ademais, as dimensões mais recentes são denominadas de quarta e quinta, aquela, por seu turno, refere-se a termos como a democracia, a bioética, a informação e o pluralismo, sendo que geralmente são atribuídos às obras de Norberto Bobbio. Por outro lado, esta, em contraposição àquela, possui em seu ventre a ideia de paz mundial.

Como uma espécie de contraface àquelas sociedades primitivas, que por muitas vezes tratavam a diferença com sanha, não por mero furor para com as próprias dissimilitudes, mas como um modo de auto preservação. Pode-se vislumbrar que caminhamos rumo a uma grande aldeia coletiva em que todos os indivíduos são detentores dos mesmos direitos, logo não haveria distinções, em consequência da globalização e o estupendo desenvolvimento comunicacional.

É importante abordar criticamente como a criação de uma sociedade digital impacta na sua evolução. Assim, convém citar que conforme Debord (1967, p. 5) o espetáculo é apto para sujeitar os seres humanos a si mesmos, inclusive a economia já os subjugou [...] O que é de uma vez por todas um reflexo fiel da produção das coisas e distorção da objetificação dos produtores.

Dadas as conjunturas supracitadas, cabe-nos discutir a marginalização de determinados grupos, fatores políticos e sociais que se vinculam a sociedades que cada vez menos conseguem distinguir os limites entre o mundo concreto e o digital. O mundo digital é um reflexo distorcido da sociedade do espetáculo que vivemos, todavia, tal distorção é devido a condição humana, que possui a capacidade não só de alterar o comportamento das pessoas dentro desse micro realidade, mas também tem a capacidade de moldar a sociedade além dessas barreiras virtuais.

3. Obstáculos iniciais do direito penal e processo penal frente os crimes virtuais: classificação e sujeitos.

Por conseguinte, com o surgimento do “mundo virtual” acarretou também no crescimento em crimes cometidos neste ambiente de forma assustadora. Além disso, a preocupação também se voltou para o modo de punir o agente, pois alterava assim a noção de fronteira e espaço físico.

Ademais, é de suma importância ressaltar que a norma jurídica não se modernizou da mesma maneira que os crimes virtuais, deixando o Estado com dificuldades para punir o réu por falta de lei específica, gerando uma série de analogias para estes tipos penais novos, ao qual abrem grande margem para recursos em instâncias superiores.

Entre diversas outras modalidades de crimes, podemos ainda mencionar os crimes de 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); Interceptação de comunicações de informática (art. 10 da Lei nº 9.296/96); Interceptação de E-mail Comercial ou Pessoal (art. 10 da Lei nº 9.296/96); Crimes contra software – "Pirataria" (art. 12 da Lei nº 9.609/98) (CARNEIRO, 2012, p. 01).

Dessa forma, se faz necessário um olhar voltado a pesquisa neste âmbito, com primazia no Direito Penal e Processual Penal, pois com o passar dos anos a demanda só tem aumentado para os juristas e técnicos de informação.

Focando assim, nas transformações advindas da globalização fomentando possível solução para tal crise mundial, tendo em vista que um crime praticado por meio da Internet se dá em todos os lugares em que haja rede disponível (NOGUEIRA, 2014).

Ademais, os crimes virtuais, são vistos similarmente aos comuns, sendo "condutas típicas e culpáveis, todavia praticadas contra ou com a utilização dos sistemas de informação" (BORTOT, 2017, p. 341). Ademais, em suma, o crime virtual objetiva ter vantagem indevida apropriando-se ou transmitindo informações de cunho sigiloso.

Sendo assim, em aspecto geral, os crimes informáticos são tidos como puros, puros sem previsão legal (e alguns com previsão legal) e os impuros (COURI, 2009).

Desse modo, nos crimes considerados puros o sujeito tem o computador como objeto e meio do crime, comprometendo a segurança do sujeito passivo e para as condutas ainda não tipificadas, há a urgente necessidade de atualização no texto penal.

> Crimes eletrônicos puros [...] são aqueles praticados por computador e se realizam ou se consumam também em meio eletrônico. Neles, a informática (segurança dos sistemas, titularidade das informações e integridade dos dados, da máquina e periféricos) é o objeto jurídico tutelado. (JESUS, 2003 apud CARNEIRO, 2012, on-line).

Além disso, nos crimes configurados impuros ou mistos, o agente utiliza do computador com finalidade ilícita em crimes tipificados de acordo com sua conduta.

> [...] Já os crimes eletrônicos impuros ou impróprios são aqueles em que o agente se vale do computador como meio para produzir resultado naturalístico, que ofenda o mundo físico ou o espaço "real", ameaçando ou lesando outros bens, não-computacionais ou diversos da informática. (JESUS, 2003 apud CARNEIRO, 2012, on-line).

O crime cibernético pode ter vários fatores em sua motivação, porém no geral o autor coincide em outra classe de crime, além da busca em descobrir as vulnerabilidades de um sistema de informacional (ARAÚJO, 2021). O sujeito passivo detém o bem jurídico assegurado pela legislação, na qual se relaciona a conduta do sujeito ativo.

4. Perspectivas jurídico-penais para o ciberespaço no direito digital penal e processual penal brasileiro.

O ciberespaço tem um impacto significativo no campo do Direito Penal e do Processo Penal, pois está intrinsecamente relacionado à ocorrência de cibercrimes. Tanto os cibercrimes impróprios, que são crimes tradicionais cometidos por meio do ciberespaço, quanto os cibercrimes próprios, que são condutas criminosas específicas do ambiente digital, exigem uma análise cuidadosa no âmbito jurídico.

No Direito Penal, é necessário identificar comportamentos lesivos no ciberespaço e estabelecer tipos penais adequados para abrangê-los. Conforme mencionado anteriormente, os cibercrimes impróprios englobam fraudes eletrônicas, ataques à honra e ameaças nas redes sociais, *cibergrooming*, *cyberbullying*, *cyberstalking*, transmissão e difusão de conteúdo proibido, entre outros. Por outro lado, os cibercrimes próprios envolvem condutas como hacking, ataques DoS ou DDoS, infecção de sistemas por malware, ransomware e interceptação ilegal de dados na rede.

Dentro do Direito Processual Penal, a prova digital se destaca como uma modalidade nova e desafiadora trazida pelo ciberespaço. Embora seja possível aplicar os princípios e institutos desenvolvidos para a produção e valoração da prova física, as evidências digitais possuem especificidades que exigem procedimentos diferenciados para sua coleta e tratamento como prova válida em processos criminais. Isso inclui desafios como a pesquisa informática para identificar dados relevantes em sistemas computacionais e a questão da aplicação territorial das leis quando os dados estão armazenados em outros países.

É importante ressaltar que a prova digital desempenha um papel fundamental no Processo Penal, pois é utilizada para comprovar a autoria e/ou materialidade de infrações penais. Com o aumento do uso de dispositivos eletrônicos, especialmente smartphones, evidências de crimes como homicídios, lesões corporais e estupros podem ser armazenadas nesses dispositivos, utilizados para

sua gravação ou transmissão. Portanto, é imprescindível estudar minuciosamente a prova digital nesse contexto.

Um tema que afeta tanto o Direito Penal quanto o Processo Penal é o lugar do crime. A cibercriminalidade é considerada uma infração internacional ou transnacional, uma vez que pode afetar simultaneamente várias ordens jurídicas de diferentes países. Isso gera desafios para determinar a jurisdição competente para investigação e ação penal. Os critérios tradicionais de ação/omissão e consumação do crime nem sempre são adequados para resolver a questão da jurisdição, especialmente quando os cibercrimes podem ser cometidos à distância e seus efeitos podem ser observados em países diferentes. A fragmentação geográfica dos cibercrimes também afeta a produção de provas, uma vez que as evidências podem estar dispersas em diferentes países, exigindo cooperação internacional para sua obtenção.

Em suma, o ciberespaço impõe desafios ao Direito Penal e ao Processo Penal, demandando uma abordagem cuidadosa e adaptada para lidar com a cibercriminalidade. Os tipos penais devem ser atualizados para abranger as condutas cometidas no ambiente digital, enquanto os procedimentos e regras de produção de prova devem considerar as particularidades das evidências digitais. Além disso, é essencial a cooperação internacional para enfrentar a questão da jurisdição e garantir a eficácia do combate aos cibercrimes em um contexto globalizado.

É indubitável que o ambiente cibernético se tornou um território bastante propício para cometimento de delitos, tal excerto tem ratificação quando averiguado o levantamento dado pela Fortinet, empresa de soluções em segurança cibernética, à CNN Brasil. Segundo pesquisas apresentadas por tal empresa, “o Brasil registrou no primeiro semestre de 2022, cerca de 31,5 bilhões de tentativas de ataques cibernéticos a empresas”. O que significa que “o número é 94% superior na comparação com o primeiro semestre do ano passado, quando foram 16,2 bilhões de registros”.

Neste mesmo diapasão, é compreensível avistar que tais delitos afetam tanto bens jurídicos individuais quanto coletivos. Porque mesmo que inconscientemente podemos vislumbrar sem dificuldade um grupo de criminosos ou meramente um indivíduo solitário que em um recanto sórdido, quiçá umbrátil, através de um dispositivo eletrônico tem a possibilidade de cometer crimes em qualquer lugar do mundo.

Remontando aos primórdios da humanidade, pode-se atribuir ao início dos primeiros agrupamentos humanos distinguir o mundo em dois grupos, o caos e ordem, um perpendicularmente associado ao outro, gerando assim direitos e deveres, mas também punições para que condutas danosas a sociedades não sejam propagadas. Desse modo, surge a figura do Estado que durante a história vem servindo de ferramenta primordial das sociedades modernas, auxiliando a manter o controle da ordem pública.

Nesse liame, o Código Penal brasileiro e o Código de Processo Penal foram criados com o fim de definir as normas penais responsáveis por proteger os bens jurídicos brasileiros. Por conseguinte, com o avanço da sociedade brasileira, gerou-se, através da internet e avanço de novas práticas criminosas advindas dela, a necessidade de alterações no CP e no CPC, para acompanhar os pensamentos e evoluções no âmbito do direito nacional

Ademais, o Brasil é o segundo o relatório da Conferência das Nações Unidas sobre Comércio e Desenvolvimento, o quarto país no ranking mundial com o maior número de usuários do mundo. Nesse sentido, o crescimento tecnológico no país acarretou mudanças significativas no cotidiano dos brasileiros em suas mais diversas relações, sejam elas afetivas com a aproximação de pessoas pelo mundo digital, por meio das mídias sociais, ou até mesmo do modo de produção humana em questões trabalhistas como o teletrabalhador.

Contudo, as práticas criminosas acompanharam esse crescimento e se adentraram ao meio virtual. Em virtude disto, a lei 12.965 criada em 2014, denominada “O Marco Civil da Internet", instituiu ditames no que tange a liberdade de expressão e privacidade de brasileiros na internet, democratizando o acesso à internet com segurança.

5. Direito comparado: a legislação de crimes informáticos em outros países.

A lei n. 12.737/2012 (Lei dos Crimes Cibernéticos) sofreu infindáveis críticas em razão das suas lacunas, sem mencionar a morosidade do legislador para positivar uma norma altamente essencial no mundo moderno. Foi necessário que ocorresse um caso de repercussão nacional para que o legislador brasileiro viesse a se movimentar e articular a norma que ficou conhecida popularmente como Lei Carolina Dieckmann.

No caso supramencionado, os criminosos invadiram o e-mail de Carolina através de um

software malicioso que o contaminou tão longo que ela clicou num *spam*. Em consequência, os perpetradores adquiriram fotos íntimas da autora e requisitaram certo montante em dinheiro para não postar nas redes sociais, todavia, independentemente do pagamento, houve a postagem das fotos dela nas redes sociais. No caso em tela, os indivíduos foram indiciados por penas disciplinadas no código punitivo pátrio, sendo enquadradas nos seguintes crimes: furto, extorsão qualificada e difamação.

O que de certo modo demonstrou uma espécie de aberração jurídica, por sorte se observarmos cautelosamente o que acontecia era uma espécie de interpretação extensiva para abarcar crimes ainda não previstos na legislação pátria. Isso consistia, portanto, em uma violação clara ao art. 5º, inciso XXXIX, da CRFB, o princípio da legalidade. Porque, *in concreto*, ocorria o indiciamento de condutas delituosas diversas que sequer haviam sido tipificadas por regramentos específicos.

Tendo isso em vista, é possível verificar que foi necessário um esforço descomunal para a positivação de crimes cibernéticos no Brasil, enquanto outros países como os Estados Unidos e a Suécia, empenharam-se de maneira hercúlea para a criminalização de condutas fraudulentas e imorais relacionadas à informática ainda no final do século XX.

De acordo com Haracemiw e Vieira (2014, p. 426), os Estados Unidos são considerados pioneiros no combate aos crimes cibernéticos. Acredita-se que as primeiras manifestações de atividades ilícitas na área da informática ocorreram neste país, no final dos anos 70, por meio de um estudante chamado Robert Tappan Morris. Morris, inclusive, começou a desenvolver um programa de computador que explorava as vulnerabilidades de segurança descobertas na internet, com o propósito de demonstrar a inadequação das medidas de segurança empregadas na rede.

A América passou a partir de então a combater veementemente crimes informáticos, mais especificamente em 1981, ocorreu o estabelecimento de mecanismos federais de proteção a sistemas computacionais. Além disso, outro marco bastante importante para o legislativo americano foi a lei de transferência de fundos eletrônicos. O *Electronic Funds Transfer act* foi responsável por incriminar fraudes informáticas que não continham relações interpessoais. Logo, tal dispositivo é a *milestone* de proteção aos consumidores que engajam em transferências eletrônicas de fundos.

Dessarte, é imprescindível ressaltar similarmente ao ato previamente citado, o grandíssimo marco brasileiro foi advindo da lei *Carolina Dieckmann*, que trouxe em seu bojo, sobretudo, o

estabelecimento de tipificações criminais, tal qual o dispositivo 154-A do Código Penal, que consiste no seguinte:

> Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita.

Além disso, faz-se mister pontuar que a publicação da lei que está sob análise desencadeou alterações em artigos penais, refere-se especificamente aos artigos 266 e 298. Dessa maneira, convém observar breves explanações de outros autores abordando tal tópico:

> A Lei 12.737/12 introduziu no ordenamento jurídico 3 tipificações penais no Código Penal: o artigo 154- A que versa sobre a invasão de dispositivo informático alheio, o artigo 266, §1º e 2º que fala sobre a interrupção ou perturbação de serviço telefônico, telegráfico, informático, telemático ou de informação de utilidade pública, artigo 298,§ único, que tipifica falsificação de cartão de crédito ou débito (MAUÉS, DUARTE, CARVALHO, 2018, p.173).

A recente legislação promoveu modificações na redação do artigo 266 do Código Penal, incluindo, de forma indireta, o parágrafo 1º. Esse parágrafo estabelece que será punido da mesma forma aquele que interromper o serviço telemático ou de informação de utilidade pública, ou dificultar o seu restabelecimento, ampliando, assim, a abrangência do crime de interrupção ou perturbação de serviço telegráfico, radiotelegráfico ou telefônico. Além disso, também foi adicionado o parágrafo único ao artigo 298, equiparando, para fins de falsificação ou alteração, o cartão de crédito a um documento particular (Harakemiv; Vieira, 2014, p. 425).

Além dessas mudanças pontuais, houve a inclusão de dois artigos ao Código Penal, referente aos arts. 154-A e 154-B, constando no título I do Código Penal, presente na ala dos crimes contra a honra. Ou seja, tais penalizações tinham como fulcro a preservação da intimidade, a vida privada, o sigilo de dados e o patrimônio, que são bens jurídicos que perpassam a singularidade dos indivíduos e se desdobram em laços sólidos com coletividade.

6. Da competência penal para crimes na internet

O Estado possui soberania para promover o seu ordenamento jurídico em seus limites territoriais, no entanto a rede virtual supera qualquer barreira física e se estende globalmente em questão de segundos. Nesse cenário é visto a importância da colaboração entre as nações no que tange

ao combate de crimes cibernéticos.

Além do mais, cada país se depara com questões de supra importância, que modificam consideravelmente a percepção sobre o direito atual, tais como local do delito e sua jurisdição regente. Ademais, é visto que a União possui competência limitada como descreve o art. 109, IV e V, da Constituição Federal de 1988:

> Art. 109. Aos juízes federais compete processar e julgar:
> IV -os crimes políticos e as infrações penais praticadas em detrimento de bens, serviços ou interesse da União ou de suas entidades autárquicas ou empresas públicas, excluídas as contravenções e ressalvada a competência da Justiça Militar e da Justiça Eleitoral;
> V os crimes previstos em tratado ou convenção internacional, quando, iniciada a execução no País, o resultado tenha ou devesse ter ocorrido no estrangeiro, ou reciprocamente (BRASIL, Constituição da República Federativa do Brasil, de 5 de outubro de 1988).

Nesse sentido, faz-se mister analisar que a competência Federal está ligada à aplicação das normas nacionais apenas a delitos cometidos em território brasileiro, ou iniciados no Brasil e tem seu resultado internacionalmente ou em casos de ações inversas, demonstrando assim a necessidade de tratados ou convenção internacional no qual versam sobre os crimes na internet.

Por conseguinte, em relação ao crime de divulgação de imagens pornográficas de crianças e adolescentes na Internet, no qual a Justiça Federal tem competência para julgar. Especificamente, através da Assembleia Geral das Nações Unidas, em sua Convenção sobre Direitos da Criança, o Brasil tomou como meta o combate da violência sexual contra crianças e adolescentes.

Nessa mesma perspectiva, o delito possui cunho transnacional, pois tal conteúdo pode ser transmitido em qualquer computador e nacionalmente da Seção Judiciária do local onde o réu publicou. De igual forma, o artigo 7°, §2°, do Código Penal aponta que a competência extraterritorial, sendo aferido pela jurisprudência do Tribunal Federal da 4ª Região:

> DIREITO PENAL. APELAÇÃO CRIMINAL. ART. 241 DO ESTATUTO DA CRIANÇA E DO ADOLESCENTE. PUBLICAÇÃO E DISPONIBILIZAÇÃO, EM AMBIENTE VIRTUAL, DE FOTOS E VÍDEOS PORNOGRÁFICOS ENVOLVENDO CRIANÇAS E ADOLESCENTES. INTERNACIONALIDADE DEMONSTRADA. COMPETÊNCIA DA JUSTIÇA FEDERAL. MATERIALIDADE, AUTORIA E DOLO EVIDENCIADOS. CRIME DE QUADRILHA OU BANDO. ART. 288, DO CP. NÃO CONFIGURAÇÃO. DOSIMETRIA DA PENA. UTILIZAÇÃO DA INTERNET COMO INSTRUMENTO PARA A EXECUÇÃO DO CRIME. CIRCUNSTÂNCIA INERENTE À TIPIFICAÇÃO CONSOLIDADA PELA LEI 10.764/2003. CONCURSO MATERIAL. SOMA DAS PENAS PRIVATIVAS DE LIBERDADE SUPERIOR A QUATRO ANOS. SUBSTITUIÇÃO POR RESTRITIVAS DE DIREITOS. IMPOSSIBILIDADE. 1. Tratando-se da potencial prática de crime cuja previsão resulta de orientações traçadas em acordos e tratados internacionais dos

> quais o Brasil é signatário -visando combater a pedofilia via internet, deflagrada a operação policial em território pátrio a partir de investigações realizadas no exterior, tem-se por caracterizada a internacionalidade necessária a visatractiva da Justiça Federal (art. 109, inciso V, da CF/88). 2. Evidenciado, pela prova produzida, que o acusado, conscientemente, publicou e forneceu material pedófilo por meio da rede mundial de computadores, resta configurada a prática das condutas descritas no art. 241 do Estatuto da Criança e do Adolescente, tanto na redação original, quanto na anterior à Lei 11.829, de 2008. 3. O crime de quadrilha ou bando visa punir a associação de no mínimo quatro pessoas, que assim se reúnem de forma estável ou permanente com a finalidade precípua de cometer uma série de crimes. Nessa perspectiva, ainda que presentes os requisitos numérico e temporal (permanência das comunidades virtuais pedófilas por vários meses), não se tem por caracterizado o delito previsto no art. 288, do CP, quando a prova produzida evidencia que a associação dos integrantes dessas comunidades virtuais não se dava de forma estável, mas, senão, ocasionalmente. 4. A alteração legislativa promovida pela Lei 10.764, de 12.11.2003 integrou ao caput do artigo 241, do ECA, a utilização da "rede mundial de computadores ou internet" como meio de comunicação apto a apresentar, produzir, vender, fornecer, divulgar ou publicar fotografias ou imagens com pornografia ou cenas de sexoexplícito envolvendo criança ou adolescente. Portanto, sendo o uso da internet inerente ao tipo, descabe a negativação da circunstância judicial de culpabilidade sob esse fundamento. 5. Reconhecido o concurso material de crimes, as penas privativas de liberdade aplicam-se cumulativamente, consoante o disposto no artigo 69, caput, do CP. Assim, sendo a soma das penas superior a 4 anos, inviável sejam elas consideradas isoladamente para fins de substituição por restritivas de direito (art. 44, inciso I, do CP).(Santa Catarina. Tribunal Regional Federal da 4ª Região. Apelação Criminal. ACR 200572040079800, TADAAQUI HIROSE, TRF4 -SÉTIMA TURMA, D.E. 25/11/2010).

Além disso, o Código de Processo Civil em seu artigo 69 não dispõe o local de residência da vítima como competência jurisdicional, porém nos crimes virtuais o que é analisado é onde ocorreu a sua execução. Nesse cerne, nos casos de estelionato, a consumação se dá com a vantagem indevida em virtude da vítima, definindo assim a competência Estadual conforme o local que ocorreu o fato ilícito.

7. Discussões sobre legislação específica de crimes virtuais

Para Renato Opice Blum, advogado e professor de direito digital, a negligência ao criar senhas robustas é um convite aberto para a ocorrência de invasões e violações da privacidade. Para resguardar seus dados sensíveis e evitar prejuízos desnecessários, é fundamental que os usuários adotem medidas de segurança, como o uso de senhas complexas e a realização regular de alterações nas mesmas.

Desse modo, leis como a nº 12.737/12, a qual dispõe sobre a tipificação criminal de delitos informáticos, que surgiram de forma abrupta e com discussões limitadas a respeito da presente temática, devem ser alteradas à medida que se têm a necessidade frente aos novos problemas gerados pela constante evolução de tais práticas delituosas.

Sendo assim, uma legislação deficiente em seu planejamento e execução pode revelar-se tão

desprovida de eficácia quanto a inexistência de qualquer legislação. O engajamento em diálogos e a promoção de discussões aprofundadas constituem elementos basilares para assegurar que a legislação aborda devidamente as questões pertinentes.

Assim, é altamente recomendável que os usuários se esforcem para manter seu software antivírus sempre atualizado e, além disso, criem senhas para seus arquivos que não incluam informações básicas, como números de telefone ou datas de aniversário. É incontestável que os crimes mencionados só ocorrem quando o usuário colabora, seja por descuido ou falta de atenção ao que acessa ou guarda em seus dispositivos eletrônicos, como computadores e tablets. Nesse sentido, simplesmente evitando clicar em links suspeitos, contribui-se significativamente para a redução dessa forma de crime.

Por conseguinte, algumas disposições da lei podem ser consideradas vagas ou imprecisas, o que pode levar a interpretações variadas e falta de uniformidade na aplicação da lei. Com isso, o autor Coriolano Almeida Camargo Santos discorre que a eficácia do sistema de justiça está sujeita a vários elementos, incluindo a adaptação do Direito Processual às transformações tecnológicas, tanto no âmbito civil quanto no criminal, assim como o envolvimento do poder judiciário e demais instituições responsáveis por essa tarefa. No entanto, tem sido observado que essa adaptação ocorre em um ritmo consideravelmente mais lento do que o avanço das inovações tecnológicas.

8. Considerações finais

Com base nos estudos realizados sobre o impacto da rápida evolução tecnológica na sociedade moderna e a necessidade de um direito cibernético e processual penal para lidar com os desafios legais emergentes relacionados à atividade criminal no ambiente digital, é possível chegar a algumas conclusões empíricas.

Tomando por base Aristóteles, filósofo grego da antiguidade, afirmava que "a lei é a razão livre e autônoma, que se manifesta na consciência moral dos indivíduos e serve como um guia para a conduta correta". Nesse sentido, é fundamental que a legislação siga o mesmo compasso dos avanços tecnológicos para garantir a proteção dos direitos individuais e coletivos no ambiente digital.

Primeiramente, a sociedade digital trouxe consigo uma série de transformações sociais e comunicacionais sem precedentes. A revolução tecnológica e a interconectividade global abriram novas possibilidades de interação entre indivíduos, criando uma aldeia global. No entanto, essa interconexão também trouxe desafios para o direito penal e processual penal, uma vez que os crimes virtuais não reconhecem fronteiras físicas e desafiam a aplicação das leis tradicionais.

Como Aristóteles ressaltou, a lei deve ser autônoma e livre, capaz de se adaptar às demandas

e realidades da sociedade. No caso dos crimes virtuais, percebe-se que a norma jurídica não se modernizou na mesma velocidade que os avanços tecnológicos, o que levou a dificuldades na punição dos agentes e à falta de leis específicas. A ausência de legislação adequada resultou em analogias e interpretações que muitas vezes geraram recursos e controvérsias jurídicas.

Todavia, é importante destacar que alguns tipos penais já existentes podem ser aplicados aos crimes virtuais, como calúnia, difamação, furto, estelionato, entre outros. Aqui, podemos recorrer à afirmação de Aristóteles de que "a lei não pode prever todos os casos particulares, mas deve estabelecer princípios gerais que possam ser aplicados a situações específicas". Portanto, é necessário atualizar o texto penal para incluir condutas específicas relacionadas ao ambiente digital.

Platão, similarmente, também argumentava que "a justiça é a virtude fundamental da sociedade". Diante do contexto dos crimes virtuais, é essencial desenvolver perspectivas jurídico-penais para o ciberespaço no direito digital penal e processual penal. Isso inclui a atualização da legislação, a criação de leis específicas para os crimes virtuais e a adoção de medidas de combate ao cibercrime, como a proteção de dados, a investigação forense digital e a cooperação internacional.

Em suma, o avanço tecnológico e a sociedade digital exigem uma abordagem especializada do direito penal e processual penal para enfrentar os desafios emergentes. É necessário, sobretudo, acompanhar de perto as transformações sociais e tecnológicas, garantindo a proteção dos direitos individuais e coletivos no ambiente digital, e promovendo a segurança e a justiça na era digital, tal como bem argumentado por Aristóteles.

Referências

ARAÚJO, Claudio Rodrigues. **Análise da aplicação do direito penal nos crimes virtuais**. **Pensar Acadêmico**, Manhuaçu, v. 19, n. 2, p. 494-511, maio-setembro, 2021.

BOBBIO, Norberto, 1992: **A Era dos Direitos. Rede Virtual de Bibliotecas**. Rio de Janeiro, Campus, Elsevier, 2004.

BRASIL. **Constituição da República Federativa do Brasil de 1988.** Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em 22 de abril de 2023.

BRASIL. **Decreto-Lei nº 2.848, de 7 de dezembro de 1940**. Código Penal. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm Acesso em: 29 set. 2019.

BRASIL. **Decreto-Lei nº 3.689, de 3 de outubro de 1941.** Institui o Código de Processo Penal. Disponível em https://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del3689.htm Acesso em 22 de abril de 2023.

BRASIL. Lei nº 9.296, de 24 de julho de 1996. Regulamenta o inciso XII, parte final, do art. 5° da

Constituição Federal. Diário Oficial da União, de 25.7.1996. Brasília, DF, Presidência da República, 1996.

BORTOT, Jessica Fagundes. **Crimes cibernéticos: aspectos legislativos e implicações na persecução penal com base nas legislações brasileira e internacional.** VirtuaJus, Belo Horizonte, v. 2, n. 2, p.338-362, 1º sem. 2017. ISSN - 1678-3425.

CARNEIRO, Adeneele Garcia. Crimes virtuais: elementos para uma reflexão sobre o problema na tipificação. **âmbito Jurídico**, Rio Grande, XV, n.99, abr. 2012. Disponível em: http://www.ambito-juridico.com.br/site/?n_link= revista_artigos_leitura & artigo_id=11529. Acesso em: 01 maio. 2023.

CARNEIRO, A. G. Crimes Virtuais: Elementos Para uma Reflexão Sobre o Problema na Tipificação. In: **âmbito Jurídico**, Rio Grande, 15, n. 99, abr. 2012. Disponível em: https://egov.ufsc.br/portal/conteudo/crimes-virtuais-elementos-para-uma-reflex%C3%A3o-sobre-o-problema-na-tipifica%C3%A7%C3%A3o. Acesso em: 01 maio. 2023.

CARVALHO, Marcelo Sávio Revoredo Menezes de. **A Trajetória Da Internet No Brasil: Do surgimento das redes de computadores à instituição dos mecanismos de governança.** Publicado pela UFRJ, 2006. Disponível em: http://www.nethistory.info/Resources/Internet-BR-Dissertacao-Mestrado-MSaviov1.2.pdf. Acesso em 03 de abril de 2022.

CERT.BR, Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Recomendações para Melhorar o Cenário de Ataques Distribuídos de Negação de Serviço (DDoS). Disponível em: https://www.cert.br/docs/whitepapers/ddos/ . Acesso em: 29 set. 2019.

COURI, Gustavo Fuscaldo. **Crimes pela internet.** 2009. 26 f. Artigo (Pós-Graduação em Direito) – Faculdade de Direito Candido Mendes, Escola da Magistratura do Estado do Rio de Janeiro. Rio de Janeiro, 2009.

HARAKEMIW, Rafael Antônio; VIEIRA, Tiago Vidal. Crimes Cibernéticos. Anais do 2º Simpósio Sustentabilidade e Contemporaneidade nas Ciências Sociais, 2014. Disponível em: http://www.egov.ufsc.br:8080/portal/conteudo/crimes-virtuais-an%C3%A1lise-doprocesso-investigat%C3%B3rio-e-desafios-enfrentados. Acesso em 30 de Abril de 2023.

KIST, Dario José. **Ministério Público e novas tecnologias: avanço, desafios e perspectivas**. Ministério Público do Estado do Pará por meio do Centro de Estudos e Aperfeiçoamento Funcional (CEAF). Belém - PA. 2023.

LENZA, Pedro. **Direito Constitucional Esquematizado**. 26.ed. São Paulo: Saraiva, 2022.

MAUES, G. B. Et al. (2018). CRIMES VIRTUAIS: Uma análise sobre a adequação da legislação penal brasileira. **Revista científica da FASETE.** disponível em: http://www.egov.ufsc.br/portal/sites/default/files/crimes_virtuais_2.pdf . Acesso em 30 de abril de 2023.

MCNEILL, William H. **The Pursuit of Power**: Technology, Armed Force, and Society since A.D. 1000. Chicago: The University of Chicago Press, 1982.

NOGUEIRA, Sandro D'Amato. Vitimologia: lineamentos à luz do art. 59, caput, do Código Penal

brasileiro. Jus Navigandi. Teresina, a. 8, n. 275, 8 abr. 2014. Disponível em: http://jus2.uol.com.br/doutrina/texto.asp?id=5061. Acesso em: 6 maio. 2017.

OLIVEIRA, Ingrid. **Levantamento mostra que ataques cibernéticos no Brasil cresceram 94%**. CNN Brasil, agosto de 2020. Disponível em: https://www.cnnbrasil.com.br/tecnologia/levantamento-mostra-que-ataques-ciberneticos-no-brasil-cresceram-94/#:~:text=Levantamento%20mostra%20que%20ataques%20cibern%C3%A9ticos%20no%20Brasil%20cresceram%2094%25,-Pa%C3%ADs%20%C3%A9%20o&text=O%20Brasil%20registrou%20no%20primeiro,16%2C2%20bilh%C3%B5es%20de%20registros. Acesso em: 09 maio 2023.

PADOVEZ, Rafael Silva; PRADO, Florestan Rodrigo. O direito penal brasileiro no contexto dos crimes cibernéticos. In: ETIC 2019 - Encontro de Iniciação Científica, 2018, p. 6. ISSN 12-76-8498. Disponível em: http://intertemas.toledoprudente.edu.br/index.php/ETIC/article/view/7962/67648763. Acesso em: 08 jun. 2023.

PLATÃO, **República**. Tradução Maria Helena da Rocha Pereira. 9. ed. Lisboa: Fundação Calouste Gulbbenkian, 2001.

SANTA CATARINA. Tribunal Federal da 4ª Região. Apelação Criminal. ACR 200572040079800, TADAAQUI HIROSE, TRF4-SÉTIMA TURMA, D.E. 25/11/2010.). Disponível em: http://jurisprudencia.trf4.jus.br/pesquisa/inteiro_teor.php?orgao=1&documento=2956916. Acesso em 22 abril. 2023.

SANTOS, C. A. C. **As múltiplas faces dos Crimes Eletrônicos e dos Fenômenos Tecnológicos e seus reflexos no universo Jurídico**. 2009.

VALENTE, Jonas. **Relatório aponta o Brasil como quarto país em número de usuários de internet.** 2017. Disponível em: https://agenciabrasil.ebc.com.br/geral/noticia/2017-10/relatorio-aponta-brasil-como-quarto-pais-em-numero-de-usuarios-de-internet . Acesso em: 21 abril. 2023.

VALOR ECONÔMICO. (2021, 20 de dezembro). **LGPD e demanda de mercado impulsionam a corrida da proteção de dados**. Valor Econômico. Disponível em: https://valor.globo.com/patrocinado/microsoft/ciber-seguranca/noticia/2021/12/20/lgpd-e-demanda-de-mercado-impulsionam-a-corrida-da-protecao-de-dados.ghtml. Acesso em: 08 junho. 2023.