V CONGRESSO INTERNACIONAL DE DIREITO DO VETOR NORTE

DIREITO PENAL, CRIMINOLOGIA E PROCESSO PENAL

A532
Anais do V Congresso Internacional de Direito do Vetor Norte [Recurso eletrônico on-line] organização Faculdade de Minas – Belo Horizonte;

Coordenadores: Raphael Moreira Maia, Sílvio Teixeira da Costa Filho e Camila Ramos Celestino Silva – Belo Horizonte: FAMINAS, 2021.

Inclui bibliografia
ISBN: 978-65-5648-367-2
Modo de acesso: www.conpedi.org.br em publicações
Tema: Direito e Resistência Democrática no Brasil pós pandemia.

1. Direito. 2. Pandemia. 3. Democracia. I. V Congresso Internacional de Direito do Vetor Norte (1:2021 : Belo Horizonte, MG).

CDU: 34

V CONGRESSO INTERNACIONAL DE DIREITO DO VETOR NORTE

DIREITO PENAL, CRIMINOLOGIA E PROCESSO PENAL

Apresentação

As mudanças tecnológicas, políticas, culturais dos últimos anos trouxeram impactos em todas as esferas da vida. E, sem dúvida, a pandemia do COVID-19 acrescentou ainda mais mudanças, abalos e dúvidas. E isso repercute na esfera pública, na esfera política e na esfera do Direito.

Por isso, o Congresso Internacional do Vetor Norte, em 2021, chegou a sua quinta edição sob o tema central "O Direito e a resistência democrática no Brasil pós pandemia".

A proposta do V Congresso Internacional do Vetor Norte foi proporcionar discussões e debates para pensar a democracia e cidadania de forma ampla, de modo a contemplar as noções macro e públicas como constitucionalismo e questões micro e privadas: como direito sucessórios, testamentos emergenciais e etc.

Isso, pois entende-se que a cidadania e autonomia do cidadão está em conhecer seus direitos no espaço público e espaço privado, bem como partiu-se da ideia que defender o conhecimento emancipador é defender o Estado Democrático.

Nesse sentido, propôs-se grupos de trabalho e painéis que debatessem as repercussões desse novo normal nos nossos Direitos públicos e privados, repercussões essas que antecedem a COVID-19, se afloraram na pandemia e certamente continuarão no pós-pandemia.

Dessa forma, buscou-se levar aos congressistas a experiência de imersão reflexiva sobre direitos políticos, direitos sociais e direitos privados para esse momento em que se começa ver a luz no fim do túnel da pandemia, de modo que possamos avançar e não retroceder como sociedade democrática.

E dessa experiência de fomento de reflexão e pesquisa acadêmica, mas, sobretudo, de compartilhamento de conhecimento, alcança-se o presente fruto: os presente anais são a reunião desses debates, ideias, críticas, reflexões presentes na V Congresso Internacional do Vetor Norte.

Organizadores

Raphael Moreira Maia

Sílvio Teixeira da Costa Filho

Camila Ramos Celestino Silva

O COMBATE AOS CRIMES CIBERNÉTICOS E A LEI 14.155 DE 2021: MUDANÇAS SIGNIFICATIVAS NA PENALIZAÇÃO DOS CRIMES VIRTUAIS

FIGHTING CYBER CRIMES AND LAW 14.155 OF 2021: SIGNIFICANT CHANGES IN THE PENALIZATION OF VIRTUAL CRIMES

Gelciara Lorena Lopes Ramos
Davi Campos de Melo Rocha

Resumo

Atualmente, passamos grande parte de nossas vidas em ambientes virtuais, cercados de tecnologia. É natural que muitas atividades cotidianas mudem de maneira significativa, aderindo a esse formato digital. Entretanto, essa "vida virtual" acarreta uma consequência mais perigosa, pois, a exemplo das demais situações cotidianas, práticas delituosas passaram a ocupar o ambiente virtual, criando os chamados crimes cibernéticos que, não raras vezes, são encorajados pela falsa percepção do anonimato gerada pelas telas. Por isso, propomos neste trabalho refletirmos sobre a história da internet, o conceito de cybercrimes e como as alterações legais são importantes para responsabilização dos agentes nesses crimes.

Palavras-chave: Cybercrimes, Crimes cibernéticos, Lei 14.155/21, História da internet

Abstract/Resumen/Résumé

Currently, we spend most of our lives in virtual environments, surrounded by technology. It's natural that many everyday activities change significantly, adhering to this digital format. However, "virtual life" entails a more dangerous consequence, because in everyday situations, criminal practices have come to occupy the virtual environment, creating the so-called cyber crimes that, not infrequently are encouraged by the false perception of anonymity generated through the screens. Therefore, in this work, we propose to reflect on the history of the internet, the concept of cybercrimes and how the legal changes are important for the accountability of agents for these crimes.

Keywords/Palabras-claves/Mots-clés: Cybercrimes, Cyber crimes, Law 14.155/21, Internet history

INTRODUÇÃO

O presente estudo tem por objetivo a análise do fenômeno da revolução da internet e como essa afeta de maneira muito direta a consumação dos crimes cibernéticos - *cybercrimes*. Com o avanço tecnológico e o surgimento das redes sociais e internet, é importante pensarmos também sobre as inovações e contextualizações da ciência jurídica, uma vez que essa, deve acompanhar as evoluções sociais. Diante desse contexto, a lei passa por transformações a fim de que seja contemporânea e capaz de sanar, ainda que em parte, os desafios sociais, respondendo às demandas diretivas em relação aos crimes que, por sua vez, ultrapassam a realidade presencial e alcançam as telas.

OBJETIVOS

Essa pesquisa busca entender historicamente a origem da internet e o conceito dos crimes cibernéticos (*cybercrimes*) e suas transformações ao longo do tempo, e apresentar os dados quantitativos com relação aos crimes virtuais. Além disso, apresentar as mudanças ocorridas em virtude da lei 14.155/21 e como essas afetam diretamente a responsabilização e penalização do agente que pratica crimes virtuais e suas implicações na norma penal.

METODOLOGIA

O presente estudo teve como metodologia a pesquisa bibliográfica que contribuiu para definições de conceitos sobre a origem da internet e os crimes cibernéticos, além das análises da lei 14.155/21 e suas devidas alterações.

Foram realizadas pesquisas por meio de consultas a artigos científicos, livros e legislação penal, bem como busca e análise de dados na plataforma da SafNet Brasil a fim de mensurar quantitativamente as informações sobre denúncias e possíveis crimes virtuais no país.

ORIGEM DA INTERNET

De acordo com Castells (2003), a origem da internet vem do Arpanet, rede de computadores montada pela ARPA, Advanced Research Projects Agency, em setembro de 1969. O termo internet, por sua vez, como explica o TechTudo (2013), surge em meados da década de 70:

> O uso do termo “Internet” para uma rede TCP/IP global se deu em dezembro de 1974, com a publicação da primeira especificação completa do TCP, assinada por Vinton Cerf, Yogen Dalal e Carl Sunshine, na Universidade de Stanford. A partir de então, bastou só dar mais qualidade aos protocolos e tentar implementar novas tecnologias para fazer com que estas novas redes pudessem suportar a quantidade de acessos que era crescente a partir daquele momento.

De acordo com Capobianco (2010), a www (*Wolrd Wide Web*), conhecida como *Web* é uma parte relevante da internet e um dos seus recursos mais importantes, sendo um dos fatores que potencializou o alcance mundial da internet a partir dos anos 90.

Com a rápida expansão da internet, bem como sua abrangência mundial, foi perceptível também os inúmeros impactos na sociedade, na economia, nas relações políticas e na cultura (CAPOBIANCO, 2010). Além disso, um meio para o incidente da criminalidade, sendo esse um ambiente que propicia a sensação de um lugar sem lei e, portanto, sem impunidade.

CRIMES CIBERNÉTICOS

De acordo com Wendt e Jorge (2013), os crimes cibernéticos podem ser definidos como os delitos que são praticados contra ou por intermédios de computadores – cabe ressaltar que essa definição abrange dispositivos informáticos em geral. Para tanto, os autores, classificam como “condutas indevidas praticadas por computador” (WENDT; JORGE, 2013, p. 18) e, as subdividem em ações prejudiciais atípicas e crimes cibernéticos.

A primeira diz respeito às condutas praticadas por meio da rede, que causam algum transtorno ou prejuízo à vítima, entretanto, não há previsão legal que a criminalize, em análise do caso concreto, pode-se falar em uma responsabilização na esfera cível, mas não penal. Já em relação à segunda, os crimes cibernéticos se subdividem, segundo os autores, em “crimes cibernéticos abertos” e “crimes exclusivamente cibernéticos”. Para isso, Wendt e Jorge (2013), definem:

> Com relação aos crimes cibernéticos “abertos” são aqueles que podem ser praticados da forma tradicional ou por intermédio de computadores, ou seja, o computador é apenas um meio para a prática do crime, que também poderia ser cometido sem o uso dele. Já os crimes “exclusivamente cibernéticos” são diferentes, pois eles somente podem ser praticados com a utilização dos computadores ou de outros recursos tecnológicos que permitem o acesso à internet. Um exemplo é o crime de aliciamento de crianças praticado por intermédio de salas de bate papo na internet, previsto no art. 241-D do Estatuto da Criança e do Adolescente[1]. (WENDT; JORGE, 2013, p. 19)

[1] Lei nº 8.069, de 13 de julho de 1990

Segundo Castro e Paiva (2020), os crimes cibernéticos ou digitais, também são chamados de *cybercrimes* e, em se tratando destes, a *Deep Web* está repleta, pois, trata-se de um ambiente sem restrições e obscuro, em que, segundo os autores:

> (...) as intenções de grande parte de seus usuários são as piores possíveis, condutas tipificadas no ordenamento jurídico brasileiro como criminosas são frequentes e, grande parte destas são praticadas diretamente em lojas virtuais do BLACK MARKET (Mercado Negro), local onde de tudo se compra e se vende, dentre as quais é possível destacar: tráfico de drogas (...); tráfico de órgãos humanos (...); venda ilegal de armas de fogo e munição (...); tortura e tráfico de pessoas (...); furto mediante fraude (...); falsificação e venda de documentos (...); organização criminosa de grupos extremistas e terroristas (...); induzimento, instigação e auxílio ao suicídio (...); crimes sexuais (...); pirataria (...); canibalismo. (CASTRO; PAIVA, 2020, p. 1474)

De acordo com o SaferNet Brasil[2], em 2020, o número de denúncias anônimas recebidas em virtude de crimes cometidos pela internet, foi significativamente superior aos números de denúncias recebidas no ano anterior. Os dados recebidos pela Central Nacional de Denúncias de Crimes Cibernéticos constaram mais de 150 mil denúncias[3]. Dentre as denúncias recebidas, lideram o percentual as notificações sobre pornografia infantil e racismo.

Como apresentado, os crimes virtuais são reais e, em uma rápida avaliação, todos nós estamos suscetíveis a eles.

LEGISLAÇÃO ACERCA DOS CRIMES CIBERNÉTICOS E AS MUDANÇAS PROPOSTAS PELA LEI 14.155/21

O Código Penal Brasileiro data de 1940 e, portanto, não é capaz de abranger os crimes cibernéticos com clareza e profundidade, já que esses eram inimagináveis no tempo de sua elaboração.

Em virtude disso, o Poder Legislativo busca atualizar a lei na tentativa de frear o crescimento da prática dos crimes em ambientes virtuais. A título de exemplos temos: a Lei nº 9.983/2000, que inseriu os novos tipos penais, 313-A e 313- B, no Código Penal, que tratam sobre o uso ou inserção de dados falsos ou modificados nos sistemas informativos; a Lei nº

[2] A SaferNet Brasil é uma associação civil de direito privado, com atuação nacional, sem fins lucrativos ou econômicos, sem vinculação político partidária, religiosa ou racial. Fundada em 20 de dezembro de 2005, com foco na promoção e defesa dos Direitos Humanos na internet no Brasil. (...) Logo que foi criada, a SaferNet Brasil se consolidou como entidade referência nacional no enfrentamento aos crimes e violações de Direitos Humanos na internet, e tem se fortalecido institucionalmente no plano nacional e internacional pela capacidade de mobilização e articulação, produção de conteúdos e tecnologias de enfrentamento aos crimes cibernéticos e pelos acordos de cooperação firmados com instituições governamentais, a exemplo do Ministério Público Federal. Disponível em: https://new.safernet.org.br/content/institucional. Acesso em 12 de out 2021.

[3] SAFERNET BRASIL. **Indicadores da Central de Nacional de Denúncias de Crimes Cibernéticos**. 2020. Disponível em: https://indicadores.safernet.org.br/. Acesso em 12 de out 2021.

11.829/2008 que alterou o Estatuto da Criança e do Adolescente (ECA), na tentativa de frear exploração sexual infanto-juvenil virtual e a pornografia; a Lei nº 12.735/12 que determinou a criação de delegacias especializadas em crimes cibernéticos; e a Lei nº 12.737/2012, que ficou popularmente conhecida como a "Lei Carolina Dieckmann" que deu origem aos tipos penais 154-A e 154-B, bem como alterou a redação dos artigos 266 e 298 do Código Penal, tratando acerca da tipificação de delitos informáticos.

Nesse contexto a mais nova Lei criada pelo Legislativo para o combate aos cybercrimes é a Lei 14.155/21, que promoveu importantes alterações no Código Penal, estabelecendo penas mais gravosas para os crimes de violação de dispositivo informático, furto e estelionato praticados pela internet, além da mudança no campo do Processo Penal que determinou a competência para os crimes de estelionato.

De início é importante ressaltarmos a mudança prevista na redação do artigo 154-A, que passou a dispor:

> Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita: Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa.
> § 2º Aumenta-se a pena de 1/3 (um terço) a 2/3 (dois terços) se da invasão resulta prejuízo econômico.
> § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido: Pena – reclusão, de 2 (dois) a 5 (cinco) anos, e multa. (BRASIL, 2021)

A principal da alteração, no que diz respeito ao caput do artigo, se encontra na pena abstratamente prevista, que anteriormente era de um ano de reclusão na pior das hipóteses, e agora pode atingir até quatro anos de reclusão. Em razão desse aumento, o crime deixa de pertencer ao rol dos crimes de menor potencial ofensivo e passa a figurar entre os de médio potencial ofensivo. Em casos concretos, essa alteração traz significativas mudanças. O tipo penal em questão deixa ser de competência do Juizado Especial Criminal, e passa a transitar nas varas criminais comuns. Outra consequência diz respeito ao autor desse delito, já que agora esse não terá mais direito ao benefício da transação penal.

O § 2º traz uma majorante, aumentando o quantum de majoração, que passou de 1/6 para 1/3, e de 1/3 para 2/3 em casos que resultem em prejuízos financeiros para a vítima.

A qualificadora prevista no § 3º também sofreu alterações nas penas previstas. A pena abstratamente prevista, que correspondia a seis meses a dois anos, passou a ser de dois a cinco

anos de reclusão, e como consequência, também deixou o rol dos crimes de menor potencial ofensivo e passou ser considerado de médio potencial ofensivo.

Além das mencionadas mudanças no artigo 154-A, a nova Lei 14.155/21 também é responsável pela criação de uma nova figura qualificada ao crime de furto, prevista no artigo 155 § 4º-B do Código Penal, que dispõe:

> A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se o furto mediante fraude é cometido por meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem a violação de mecanismo de segurança ou a utilização de programa malicioso, ou por qualquer outro meio fraudulento análogo. (BRASIL, 2021)

Essa nova qualificadora ainda pode sofrer aumento de pena em caso de resultado gravoso. Para esses casos dispõe o § 4-C a proporção desse aumento, que será de 1/3 a 2/3, se o crime é praticado mediante a utilização de servidor mantido fora do território nacional e de 1/3 ao dobro, se praticado contra idoso ou vulnerável.

A última alteração promovida pela Lei 14.155/21 no Código Penal, foi a criação da Fraude Eletrônica, disposta no §2º-A do artigo 171 do referido Código, que dispõe:

> "A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo."

Nota-se a partir da redação desse tipo penal, que se trata de um estelionato qualificado, sendo a maneira como as informações fornecidas pelas vítimas foram obtidas pelo autor a razão de sua qualificação. Nesse contexto, destacam-se os meios eletrônicos como forma de execução do delito, sendo realizados online ou não. Importante ressaltar que esse tipo penal possui o mesmo sentido de diversos golpes aplicados eletronicamente.

A partir do exposto, durante o período da Pandemia do novo Coronavírus, os crimes e ataques cibernéticos cresceram significativamente, de acordo com a Kasperskay[4] (2020), no Brasil, um a cada oito usuários da internet acessaram de abril a junho de 2020, ao menos um link que direcionasse a páginas maliciosas. Nesse sentido, o Brasil passou a ocupar a quinta posição no ranking mundial de países com maior número de usuários "atacados" e, em virtude

[4] A Kaspersky Lab é uma empresa internacional de segurança virtual fundada em 1997. A detalhada inteligência de ameaças e a experiência em segurança da Kaspersky Lab se transformam em soluções e serviços de segurança para proteger empresas, infraestruturas críticas, governos e consumidores em todo o mundo.. Disponível em: https://www.kaspersky.com.br/about Acesso em 13 de out 2021.

do benefício do auxílio emergencial, disponibilizado pelo governo aos cidadãos em situação de vulnerabilidade, os golpes tornaram-se frequentes, como apresentado abaixo pela Kasperskay[5]:

> Segundo os especialistas da Kaspersky, os ataques no Brasil se destacaram pelo uso massivo de *fakenews* relacionadas a programas de auxílio social, tirando proveito dos burburinhos causados pela irrupção da pandemia. Um exemplo citado pelo relatório mostra um e-mail com a falta informação de que o governo havia suspendido os pagamentos de contas de energia. O golpe trazia um link pelo qual o usuário era convidado a fazer um cadastro caso quisesse ter acesso ao benefício. (KASPERSKAY, 2020)

Esse crescimento espantoso em um espaço tão curto de tempo, se deve ao fato de que no contexto de pandemia, as pessoas migraram suas vidas para a internet e claro, foram acompanhadas por ações criminosas. Esses números preocupantes e, de certa forma, justificam a intenção do legislador ao criar a Lei 14.155/2021, numa clara tentativa de reprimir esse crescimento.

CONSIDERAÇÕES FINAIS

Diante da discussão exposta, é nítido que os crimes cibernéticos (*cybercrimes*), infelizmente, fazem parte do nosso cotidiano e, em razão disso, precisamos estar preparados para enfrentá-los ou ao menos nos educar para não sermos vítimas de algum deles.

Como forma de minimizar os seus impactos e acontecimentos, a Lei 14.155/21 promoveu mudanças significativas, entretanto, criar legislações aplicáveis a esses crimes é apenas parte da solução. Faz-se necessária uma maior abordagem do tema por parte das autoridades nacionais de segurança, a fim de preparar a população para enfrentar esses ataques digitais, que na maioria das vezes acontecem devido à falta de conhecimento da população em relação ao tema.

Como analisamos historicamente, a internet evoluiu muito rapidamente e essa evolução é contínua, o que percebemos mais claramente no atual cenário com o advento da pandemia. Pois, durante esse tempo, nos deparamos com a necessidade de migrar diversas tarefas para a modalidade remota, inclusive algumas que pareciam impossíveis de serem realizadas remotamente. Ademais, percebemos que essa realidade também alcançou a prática delituosa, que está cada vez mais presentes no mundo digital.

---

[5] KASPERSKAY. **Brasil foi o quinto país com maior proporção de vítimas de phishing após pandemia: Relatório da Kasperskay mostra que um a cada oito brasileiros sofreram tentativas de ataque entre abril e junho**. 2020. Disponível em: https://www.kaspersky.com.br/about/press-releases/2020_brasil-foi-o-quinto-pais-com-maior-proporcao-de-vitimas-de-phishing-apos-pandemia. Acesso em 13 de out 2021

Portanto, a criação de novos dispositivos legais é importante, pois trata-se de uma tentativa, ainda que de certa forma esteja ligada diretamente à repressão, mas é a possibilidade para diminuir a prática delituosa e o sentimento de que as telas são espaços absolutamente anônimos e, portanto, sem responsabilização para os delitos ali cometidos.

REFERÊNCIAS

BRASIL. **Decreto-Lei nº 2.848, de 7 de janeiro de 1940**. Código Penal. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em 12 de out 2021

BRASIL. **Lei nº 14.155, de 27 de maio de 2021**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14155.htm. Acesso em 12 de out 2021.

CAPOBIANCO, Lígia. A revolução em curso: Internet, Sociedade da Informação e Cibercultura. **Estudos em Comunicação**. v. 2, n. 7, p. 175-193, 2010. Disponível em: http://ec.ubi.pt/ec/07/vol2/capobianco.pdf. Aceso em 11 de out 2021

CASTELLS, Manuel. **A Galáxia Internet: reflexões sobre a internet, negócios e a sociedade**. 1. ed. Rio de Janeiro: Jorge Zahar Editor Ltda, 2003. p. 13-14

CASTRO, Felipe Cesar Nascimento de; PAIVA, Vilma Madelaine Martinez. Uma análise da conduta típica praticada no âmbito da internet: Crimes Cibernéticos e Digitais. **Anais do Congresso Brasileiro de Processo Coletivo e Cidadania**, n. 8, p. 1469-1488, 12 dez. 2020. Disponível em: https://revistas.unaerp.br/cbpcc/article/view/2118. Acesso em 11 de out 2021

GANEM, Pedro. O combate aos cybercrimes e a nova lei nº 14.155 de 2021. **Canal Ciências Criminais**. 2021. Disponível em: https://canalcienciascriminais.com.br/o-combate-aos-cybercrimes-e-a-nova-lei-n-o-14-155-de-2021/. Acesso em 11 de out 2021

KASPERSKAY. **Brasil foi o quinto país com maior proporção de vítimas de phishing após pandemia: Relatório da Kasperskay mostra que um a cada oito brasileiros sofreram tentativas de ataque entre abril e junho**. 2020. Disponível em: https://www.kaspersky.com.br/about/press-releases/2020_brasil-foi-o-quinto-pais-com-maior-proporcao-de-vitimas-de-phishing-apos-pandemia. Acesso em 13 de out 2021

SAFERNET BRASIL. **Indicadores da Central de Nacional de Denúncias de Crimes Cibernéticos**. 2020. Disponível em: https://indicadores.safernet.org.br/. Acesso em 12 de out 2021.

TECHTUDO. **Internet completa 44 anos; relembre a história da web**. 2013. Disponível em: https://www.techtudo.com.br/artigos/noticia/2013/04/internet-completa-44-anos-relembre-historia-da-web.html. Acesso em 12 de out 2021

WENDT, Emerson; JORGE, Higor Vinicius Nogueria. **Crimes Cibernéticos: ameaças e procedimentos de investigação**. 2. ed. Rio de Janeiro: Brasport, 2013. p. 19-21