CONGRESSO INTERNACIONAL DE DIREITO, POLÍTICAS PÚBLICAS, TECNOLOGIA E INTERNET

DIREITO PENAL E CIBERCRIMES

D598
Direito penal e cibercrimes [Recurso eletrônico on-line] organização Congresso Internacional de Direito, Políticas Públicas, Tecnologia e Internet: Faculdade de Direito de Franca – Franca;

Coordenadores Ana Carolina Juzo, Clóvis Volpe Filho e Stephani Dettmer Di Martin Viena – Franca: Faculdade de Direito de Franca, 2023.

Inclui bibliografia
ISBN: 978-65-5648-917-9
Modo de acesso: www.conpedi.org.br em publicações
Tema: Desafios da Regulação do Ciberespaço.
1. Direito. 2. Políticas Públicas. 3. Tecnologia. 4. Internet. I. Congresso Internacional de Direito, Políticas Públicas, Tecnologia e Internet (1:2023 : Franca, SP).

CDU: 34

CONGRESSO INTERNACIONAL DE DIREITO, POLÍTICAS PÚBLICAS, TECNOLOGIA E INTERNET

DIREITO PENAL E CIBERCRIMES

Apresentação

É com grande satisfação que apresentamos os Anais do Primeiro Congresso Internacional de Direito, Políticas Públicas, Tecnologia e Internet, realizado entre os dias 12 e 15 de setembro de 2023, na Faculdade de Direito de Franca, composta por trabalhos apresentados nos Grupos de Trabalhos que ocorreram durante o evento, após rigorosa e disputada seleção.

Ditos trabalhos, que envolvem pesquisas realizadas nas mais diversas áreas do direito, mas primordialmente relacionados a temas centrados na relação entre o direito e o impacto das tecnologias, apresentam notável rigor técnico, sensibilidade e originalidade, buscando uma leitura atual e inovadora dos institutos próprios da área.

As temáticas abordadas decorrem de intensas e numerosas discussões que acontecem pelo Brasil, com temas que reforçam a diversidade cultural brasileira e as preocupações que abrangem problemas relevantes e interessantes.

Espera-se, então, que o leitor possa vivenciar parcela destas discussões que ocorreram no evento por meio da leitura dos textos. Agradecemos a todos os pesquisadores, colaboradores e pessoas envolvidas nos debates e organização do evento pela sua inestimável contribuição e desejamos uma proveitosa leitura!

Coordenação do Evento:

Alexandre Veronese (UnB)

Felipe Chiarello de Souza Pinto (Mackenzie)

José Sérgio Saraiva (FDF)

Lislene Ledier Aylon (FDF)

Orides Mezzaroba (CONPEDI/UFSC)

Samyra Naspolini (FMU)

Sílzia Alves (UFG)

Yuri Nathan da Costa Lannes (FDF)

Zulmar Fachin (Faculdades Londrina)

Realização:

Faculdade de Direito de Franca (FDF)

Grupo de Pesquisa d Políticas Públicas e Internet (GPPI)

Correalização:

Conselho Nacional de Pesquisa e Pós-Graduação em Direito (CONPEDI)

Faculdades Londrina

Universidade Federal de Goiás (UFG)

Universidade Presbiteriana Mackenzie (UPM)

Mestrado Profissional em Direito da UFSC

A TRANSFORMAÇÃO DOS CRIMES NA ERA DIGITAL PÓS-PANDEMIA

THE TRANSFORMATION OF CRIMES IN THE POST-PANDEMIC DIGITAL AGE

Francisco Céu Pereira [1]
Valter Moura do Carmo

Resumo

Após a pandemia da COVID-19, houve um aumento significativo nos crimes digitais em todo o mundo, atribuído às mudanças nas atividades cotidianas e à maior dependência da tecnologia durante o período de quarentena e do distanciamento social. O objetivo deste estudo é analisar, diante dessas transformações, como as reações humanas têm afetado esse comportamento criminoso e levado ao surgimento ou readaptação de crimes já existentes. A metodologia adotada foi a de revisão bibliográfica, com a análise de dados estatísticos divulgados pela imprensa. A luta contra os crimes cibernéticos requer a participação de governos, empresas, organizações e indivíduos.

Palavras-chave: Inteligência artificial, Crimes digitais, Pandemia covid-19

Abstract/Resumen/Résumé

After the COVID-19 pandemic, there has been a significant increase in digital crimes around the world, it is attributed to changes in daily activities and greater reliance on technology during the period of quarantine and social distance. The purpose of this study is to analyze, given these transformations, how human reactions have affected this criminal behavior and led to the making or readaptation of existing crimes. The methodology adopted was of a bibliographical review, with the analysis of statistical data released by the press. The fight against cybercrime requires the participation of governments, companies, organizations and individuals.

Keywords/Palabras-claves/Mots-clés: Artificial intelligence, Digital crimes, Covid-19 pandemic

[1] Acadêmico de Direito

INTRODUÇÃO

Assim como em todo o mundo, os crimes digitais no Brasil têm se tornado cada vez mais frequentes. O crescimento da tecnologia e os avanços de mecanismos de Inteligência Artificial, conforme crescem, desencadeiam novas formas de praticar crimes. Entre os principais tipos de crimes cibernéticos no país estão a fraude-eletrônica, o roubo de dados, o *phishing*, o *ransomware*, a invasão de sistemas; e, entre 2018 e 2021, o crescimento de estelionatos por meio eletrônico chega a quase 500%, mediante dados informados pelo Fórum Brasileiro de Segurança Pública. Toda a estrutura que possibilita a um usuário divulgar conteúdos e informações nas redes, sejam elas quais forem, também colabora para que crimes em diversos âmbitos sejam praticados diariamente (RODRIGUES, 2022).

Segundo dados, o Brasil registrou, no primeiro semestre de 2022, 31,5 bilhões de tentativas de ataques cibernéticos a empresas. O número é 94% superior na comparação com o primeiro semestre do ano passado, quando foram 16,2 bilhões de registros (OLIVEIRA, 2022).

Durante a última década, foram feitos muitos avanços jurídicos no que diz respeito à proteção e segurança no ambiente virtual. O Marco Civil da Internet (Lei nº 12.965, de 23 de abril de 2014) tem o objetivo de regular os direitos e deveres dos usuários da rede. Já a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709, de 14 de agosto de 2018) foi criada para regulamentar as atividades de coleta e tratamento de dados pessoais, além de proteger a captação, armazenamento e compartilhamento de dados pessoais coletados por sites e empresas.

A legislação mais recente referente a crimes cibernéticos é a Lei nº 14.155, de 27 de maio de 2021, que alterou o Código Penal, para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet, e o Código de Processo Penal, para definir a competência em modalidades de estelionato.

O presente trabalho possui como objetivo investigar e compreender os aspectos relacionados aos crimes cometidos no ambiente digital, principalmente após a pandemia, buscando identificar suas características, causas, consequências e possíveis medidas de prevenção e combate.

METODOLOGIA DE PESQUISA

Para atingir os objetivos da pesquisa, optou-se por realizar pesquisa do tipo bibliográfica. A pesquisa bibliográfica envolve o conjunto de conhecimentos humanos reunidos em obras. Seu objetivo principal é guiar o leitor a um determinado assunto e facilitar a produção, coleção, armazenamento, reprodução, utilização e comunicação das informações coletadas para a realização da pesquisa (FACHIN, 2003, p. 125).

DESENVOLVIMENTO

Esse crescimento se mostrou em evidência durante a pandemia da Covid-19, a qual teve um impacto significativo nesse aumento, os casos de golpes relacionados a compras *on-line*, boletos falsos e outros tipos de fraudes, também aparecem com índices crescentes. Além disso, o Brasil também é conhecido por ter um alto número de casos de crimes cibernéticos relacionados a crimes sexuais, como a produção e distribuição de pornografia infantil. O Safernet, em fevereiro de 2023, apresentou dados de 306 denúncias por dia no Brasil com conteúdo na internet vinculados a crianças (BRASIL TEM, 2023). Esses crimes merecem uma atenção especial das autoridades, inclusive pelo fato de que tanto a Constituição Federal, o Estatuto da Criança e do Adolescente como o Código Penal garantem a proteção contra o abuso e a exploração sexual das crianças e dos adolescentes.

Alguns aspectos que podemos visualizar dessas mudanças pós-pandemia estão ligadas ao aumento do trabalho remoto, que cresceu com a adoção generalizada do trabalho durante a pandemia, em que muitas empresas e organizações se tornaram mais vulneráveis a ataques cibernéticos. Os criminosos digitais aproveitaram a falta de segurança nas redes domésticas e as vulnerabilidades nos sistemas de TI das empresas para realizar ataques de *phishing*, *ransomware* e outros tipos de invasões. Outro ponto foi o aumento das transações *on-line,* pois o aumento substancial nesse tipo de transação facilitou a diminuição da circulação de dinheiro em espécie, incluindo compras, serviços bancários e pagamentos eletrônicos. Isso proporcionou mais oportunidades para os criminosos cibernéticos visarem informações financeiras pessoais, como números de cartão de crédito e detalhes de contas bancárias, por meio de técnicas como roubo de identidade e ataques a sistemas de pagamento.

Um dos aspectos que mais preocupa a sociedade vem com o maior uso de aplicativos de videoconferência e comunicação *on-line*, esse modo de comunicação naturalmente se desenvolveu com o distanciamento social, em que o uso desses aplicativos se tornou essencial para o trabalho, a educação e a socialização. Dessa forma, surgiram preocupações com a

privacidade e a segurança dessas plataformas, com relatos de invasões de reuniões virtuais e vazamento de informações confidenciais.

A pandemia criou um ambiente propício para a propagação de desinformação e golpes *on-line*. Os criminosos digitais se aproveitaram da ansiedade e do medo das pessoas, promovendo curas falsas, testes de COVID-19 falsos, informações falsas sobre vacinas e outros golpes relacionados à saúde. Consequentemente, destacou-se a importância dos dados de saúde e pesquisa, levando ao aumento dos ataques cibernéticos direcionados a hospitais, instituições de pesquisa e empresas farmacêuticas. Os criminosos tentam roubar informações sobre tratamentos médicos, dados de pacientes e pesquisas relacionadas à COVID-19. Todas essas violações refletem no Direito, e com surgimento de tantas leis na busca de frear esses aspectos, a eficiência da segurança digital depende de vários fatores, incluindo a qualidade das medidas de segurança integradas, o nível de tolerância dos ataques e a conscientização e comportamento dos usuários.

Nesse contexto, a importância dos dados de saúde e pesquisa se tornou ainda mais evidente. Hospitais, instituições de pesquisa e empresas farmacêuticas se viram alvo de ataques cibernéticos em busca de informações valiosas sobre tratamentos médicos, dados de pacientes e pesquisas relacionadas à COVID-19. As consequências dessas violações vão muito além do âmbito digital, tendo impacto direto no campo do Direito, exigindo o desenvolvimento de novas legislações para enfrentar esses desafios emergentes.

Em resposta a essa ameaça crescente, várias leis foram criadas na tentativa de frear essas atividades criminosas. No entanto, a eficiência da segurança digital vai além das regulamentações. Um dos fatores cruciais é a qualidade das medidas de segurança implementadas por organizações e instituições. Investir em tecnologias avançadas de proteção, criptografia robusta e sistemas de detecção de intrusões é essencial para garantir a segurança dos dados.

E nesta Era Digital, um dos grandes desafios que enfrentamos mediante essa dependência da tecnologia em nossas vidas, as ameaças cibernéticas se tornaram cada vez mais sofisticadas, elaboradas e comuns. Ao abordar crimes virtuais, é importante também discutir a questão da desinformação. Segundo uma pesquisa realizada pela consultoria Oliver Wyman, mais de 60% das pessoas estão preocupadas com a possibilidade de se tornarem vítimas de notícias falsas (*fake news*) (RODRIGUES, 2022). Esses tipos de crimes incluem roubo de identidade, invasão de privacidade, fraudes, *ransomware*, *phishing* e muitos outros. Os criminosos cibernéticos são habilidosos, e muitas vezes operam em redes globais que tornam difícil sua captura e responsabilização. Esses crimes podem causar danos financeiros,

emocionais e até mesmo físicos. Os *hackers* podem acessar dados pessoais, informações financeiras e outras informações efetivas, causando prejuízos irreparáveis.

Apesar dos esforços do governo e das forças de segurança, ainda há muito a ser feito para combater os crimes digitais no Brasil e no mundo. É importante que todos nós estejamos cientes desses riscos e tomemos medidas para nos proteger, pois a segurança digital é eficiente até certo ponto, mas não pode garantir proteção total contra ameaças cibernéticas.

De acordo com informações recentes, ocorreram ataques cibernéticos no início de outubro de 2022 que resultaram em um prejuízo significativo de R$ 16 milhões para as prefeituras de São Paulo e Minas Gerais. Conforme declarado pela Polícia Civil do Estado de São Paulo, os suspeitos envolvidos utilizaram falsos sites como meio para adquirir senhas e, posteriormente, acessar as redes das vítimas (RODRIGUES, 2022).

Mas, desde 2018, o Superior Tribunal de Justiça - STJ vem divulgando jurisprudência no que se refere a crimes de fraudes digitais, tendo em vista que a internet vem abrindo portas para novos meios de cometer velhos crimes (STJ DIVULGA, 2018).

Em um levantamento publicado pelo Supremo Tribunal de Justiça em 17 de junho de 2018, os delitos pela internet atingem anualmente cerca de 62 milhões de pessoas, causando prejuízo de US$ 22 bilhões, segundo dados da empresa de Segurança Virtual Symantec (STJ DIVULGA).

CONCLUSÕES

A prevenção e a eficácia de combate a crimes cibernéticos são desafios constantes devido à natureza em constante evolução das ameaças cibernéticas. No entanto, existem várias medidas que podem ser adotadas para minimizar os riscos e aumentar a eficácia na luta contra esses crimes.

Algumas medidas que podem ajudar a lidar com o aumento dos crimes digitais após a pandemia incluem questões de investimento em tecnologia de segurança, as empresas e organizações devem investir em tecnologia de segurança para proteger suas redes e dados contra ataques. Isso pode incluir soluções antivírus, *firewalls*, autenticação de dois fatores e outras medidas de segurança. Tal como educação e conscientização precisam cada vez mais ser aplicadas desde o público mais jovem aos idosos, que são um percentual alto em crimes como golpes bancários.

Além disso, é fundamental estabelecer um nível de tolerância zero para ataques cibernéticos. Isso significa agir rapidamente para identificar, isolar e neutralizar qualquer

ameaça em potencial. A resposta rápida e eficaz diante de uma violação pode reduzir significativamente seus efeitos negativos.

Contudo, a parte mais vulnerável do sistema continua sendo o fator humano. A conscientização e o comportamento dos usuários são determinantes na proteção contra ataques cibernéticos. A educação em segurança digital é essencial para que todos os envolvidos em uma organização, desde funcionários até pacientes, todos devem estar cientes das práticas recomendadas para evitar cair em armadilhas e disseminar informações falsas. É importante educar as pessoas sobre as ameaças digitais e como se proteger contra elas. Devemos garantir que nossos dispositivos estejam sempre atualizados e protegidos por senhas fortes, evitando clicar em links suspeitos ou abrir anexos de e-mails desconhecidos.

Através disso, é preciso incentivar uma cultura de cibersegurança, na qual todos se sintam responsáveis pela proteção dos dados. Isso implica estabelecer políticas claras de segurança, treinamentos regulares e promoção de uma mentalidade vigilante em relação às ameaças virtuais.

Além de uma cooperação internacional, pois os crimes digitais ou cibernéticos muitas vezes cruzam fronteiras internacionais, por isso é importante que os países trabalhem juntos para combater essas atividades ilegais. Isso pode incluir acordos de cooperação internacional, compartilhamento de informações e colaboração em investigações.

É importante ressaltar que a luta contra os crimes cibernéticos é um conjunto de esforços que requerem a participação de governos, empresas, organizações e indivíduos. A combinação de medidas técnicas, educacionais, legais e colaborativas pode aumentar a eficácia na prevenção e combate a esses crimes, protegendo melhor os sistemas, dados e indivíduos contra ameaças cibernéticas.

REFERÊNCIAS

BRASIL TEM 306 denúncias de pornografia infantil por dia na internet, aponta levantamento: Dados da Safernet mostram que esse é o segundo ano consecutivo com mais de 100 mil denúncias, algo que não acontecia há uma década, segundo a ONG. **G1**, 07 fev. 2023. Disponível em: https://g1.globo.com/tecnologia/noticia/2023/02/07/brasil-tem-306-denuncias-de-pornografia-infantil-por-dia-na-internet-aponta-levantamento.ghtml. Acesso em: 07 jul. 2023.

BRASIL. [Constituição (1988)]. **Constituição Federal da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, 2023. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 10 jul. 2023.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, 2021.

Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 10 jul. 2023.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 10 jul. 2023.

BRASIL. **Lei nº 14.155, de 27 de maio de 2021**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato. Brasília, DF: Presidência da República, 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14155.htm. Acesso em: 10 jul. 2023.

DINO. Crimes digitais crescem pós-pandemia e provocam corrida por ciberseguros. **Valor Econômico**, 27 jun. 2022. Disponível em: https://valor.globo.com/patrocinado/dino/noticia/2022/06/27/crimes-digitais-crescem-pos-pandemia-e-provocam-corrida-por-ciberseguros.ghtml. Acesso em: 11 maio 2023.

FACHIN, Odília. **Fundamentos de metodologia**. 4. ed. São Paulo: Saraiva, 2003.

OLIVEIRA, Ingrid. Levantamento mostra que ataques cibernéticos no Brasil cresceram 94%: País é o 2º na América Latina com mais ataques cibernéticos em 2022. **CNN Brasil**, 19 ago. 2022. 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: 12 maio 2023.

PIZARRO, Ludmila. Crimes cibernéticos atingem 62 milhões no Brasil em 2017: Prejuízo financeiro no país chegou a R$ 22 bilhões em 12 meses, segundo levantamento da Norton. **O Tempo**, 11 fev. 2018. Disponível em: https://www.otempo.com.br/economia/crimes-ciberneticos-atingem-62-milhoes-no-brasil-em-2017-1.1572879. Acesso em: 11 maio 2023.

PROFISSÃO REPÓRTER. Crimes virtuais crescem no Brasil. **G1**, 27 jul. 2022. Disponível em: https://g1.globo.com/profissao-reporter/noticia/2022/07/27/crimes-virtuais-crescem-no-brasil-veja-flagrante-e-historias-de-vitimas-com-o-profissao-reporter.ghtml. Acesso em: 11 maio 2023.

RODRIGUES, Leonardo Tulio. Especialista alerta para aumento de crimes nas redes sociais. **Central de Notícias UNINTER**, 7 nov. 2022. Disponível em: https://www.uninter.com/noticias/especialista-alerta-para-aumento-de-crimes-nas-redes-sociais. Acesso em: 16 jul. 2023

STJ DIVULGA jurisprudência sobre conceitos de crimes pela internet. **Consultor Jurídico**, 17 jun. 2018. Disponível em: https://www.conjur.com.br/2018-jun-17/stj-divulga-jurisprudencia-conceitos-crimes-internet. Acesso em: 11 maio 2023.