XII CONGRESSO RECAJ-UFMG

CRIMINOLOGIA E CYBERCRIMES

SÉRGIO HENRIQUES ZANDONA FREITAS

YURI NATHAN DA COSTA LANNES

LUCAS JERONIMO RIBEIRO DA SILVA

C929
Criminologia e cybercrimes [Recurso eletrônico on-line] organização XII Congresso RECAJ-UFMG: UFMG – Belo Horizonte;

Coordenadores: Sérgio Henriques Zandona Freitas, Yuri Nathan da Costa Lannes e Lucas Jerônimo Ribeiro da Silva – Belo Horizonte: UFMG, 2021.

Inclui bibliografia
ISBN: 978-65-5648-374-0
Modo de acesso: www.conpedi.org.br em publicações
Tema: As novas fronteiras tecnológicas do acesso à justiça e os direitos fundamentais digitais em perspectiva crítica.
1. Direito e Tecnologia. 2. Acesso à justiça. 3. Direitos fundamentais digitais. I. XII Congresso RECAJ-UFMG (1:2021: Belo Horizonte, MG).

CDU: 34

XII CONGRESSO RECAJ-UFMG

CRIMINOLOGIA E CYBERCRIMES

Apresentação

É com muita alegria que o Programa RECAJ-UFMG – Acesso à Justiça pela Via dos Direitos e Solução de Conflitos da Faculdade de Direito da Universidade Federal de Minas Gerais, a SKEMA Business School Brasil e o Conselho Nacional de Pesquisa e Pós-graduação em Direito – CONPEDI tornam público à comunidade científica o conjunto dos oito livros produzidos a partir das discussões dos Grupos de Trabalho do XII Congresso RECAJ-UFMG, que teve por tema central "As novas fronteiras tecnológicas do acesso à justiça e os direitos fundamentais digitais em perspectiva crítica".

As discussões nos Grupos de Trabalho ocorreram em ambiente virtual ao longo dos dias 25 e 26 de novembro de 2021, dentro da programação que contou com grandes nomes nacionais e internacionais da área, além de cento e quarenta e dois pesquisadoras e pesquisadores inscritos no total, provenientes de treze Estados da federação (Alagoas, Amazonas, Bahia, Distrito Federal, Espírito Santo, Minas Gerais, Piauí, Paraná, Rio Grande do Norte, Rio Grande do Sul, Santa Catarina, Sergipe e São Paulo). Marcando um momento em que a terrível pandemia da COVID-19 finalmente dá sinais de apaziguamento, o que somente foi possível por conta da ciência, da vacinação em massa e do trabalho valoroso de todos os profissionais do Sistema Único de Saúde, o evento trouxe, após hiato de quase dois anos, painéis científicos presenciais na nova (e bela) sede da SKEMA Business School Brasil no bairro Savassi em Belo Horizonte-MG.

Os oito livros compõem o produto principal deste congresso, que há mais de uma década tem lugar cativo no calendário científico nacional. Trata-se de coletânea composta pelos cento e seis trabalhos aprovados e que atingiram nota mínima de aprovação, sendo que também foram submetidos ao processo denominado double blind peer review (dupla avaliação cega por pares) dentro da plataforma PublicaDireito, que é mantida pelo CONPEDI. Os oito grupos de trabalho geraram cerca de seiscentas páginas de produção científica relacionadas ao que há de mais novo e relevante em termos de discussão acadêmica sobre diversos temas jurídicos e sua relação com a tecnologia: Acesso à Justiça e Tecnologias do Processo Judicial; O Direito do Trabalho no século XXI; Estado, Governança, Democracia e Virtualidades; e Tecnologias do Direito Ambiental e da Sustentabilidade. No dia 26, serão abordados os seguintes temas: Formas de Solução de Conflitos e Tecnologia; Direitos Humanos, Gênero e Tecnologias do Conhecimento; Inteligência Artificial, Startups, Lawtechs e Legaltechs; e Criminologia e cybercrimes.

Os referidos Grupos de Trabalho contaram, ainda, com a contribuição de vinte e quatro proeminentes pesquisadores ligados a renomadas instituições de ensino superior do país, dentre eles alguns mestrandos e doutorandos do próprio Programa de Pós-graduação em Direito da UFMG, que indicaram os caminhos para o aperfeiçoamento dos trabalhos dos autores. Cada livro desta coletânea foi organizado, preparado e assinado pelos professores e pós-graduandos que coordenaram os trabalhos.

Nesta esteira, a coletânea que ora se apresenta é de inegável valor científico. Pretende-se, com esta publicação, contribuir com a ciência jurídica e com o aprofundamento da relação entre a graduação e a pós-graduação, seguindo as diretrizes oficiais da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - CAPES. Importante lembrar, ainda, da contribuição deste congresso com a formação de novos pesquisadores na seara interdisciplinar entre o Direito e a tecnologia, uma vez que o número de graduandos que apresentaram trabalhos de qualidade foi expressivo. Destaca-se a presença maciça de pesquisadores do Estado do Amazonas, especialmente os orientandos do Professor Doutor Valmir César Pozzetti vinculados à Universidade Federal do Amazonas e à Universidade Estadual do Amazonas.

O Programa RECAJ-UFMG, que desde 2007 atua em atividades de ensino, pesquisa e extensão em acesso à justiça pela via dos direitos e soluções de conflitos, nos últimos anos adota linha investigativa a respeito da conexão entre o acesso à justiça e a tecnologia, com pesquisas de mestrado e doutorado concluídas. Em 25 de junho deste ano, celebrou um termo de cooperação técnica com o Grupo de Pesquisa Normative Experimentalism and Technology Law Lab – NEXT LAW LAB da SKEMA Business School Brasil, que prevê o intercâmbio permanente das pesquisas científicas produzidas pelo NEXT LAW LAB e pelo Programa RECAJ-UFMG na área do Direito e Tecnologia, especialmente as voltadas ao estudo do acesso tecnológico à justiça e a adoção da inteligência artificial no campo do Direito. Desta parceria nascerá, seguramente, novos projetos importes para a comunidade científica deste campo.

Com o sentimento de dever cumprido, agradecemos a todas as pesquisadoras e pesquisadores pela inestimável contribuição e desejamos a todos uma ótima e proveitosa leitura!

Belo Horizonte-MG, 28 de novembro de 2021.

Prof. Drª. Adriana Goulart de Sena Orsini

Coordenadora do Programa RECAJ-UFMG

Profª. Drª. Geneviève Daniele Lucienne Dutrait Poulingue

Reitora – SKEMA Business School - Campus Belo Horizonte

Prof. Dr. Edgar Gastón Jacobs Flores Filho

Coordenador dos Projetos de Direito da SKEMA Business School Brasil

Prof. Dr. Caio Augusto Souza Lara

Professor da SKEMA Business School Brasil e Pós-doutorando vinculado ao Programa RECAJ-UFMG

CRIMES CIBERNÉTICOS: PHISHING E FAKE NEWS EM TEMPOS DE PANDEMIA

CYBERCRIMES: PHISING AND FAKE NEWS IN PANDEMIC TIMES

Cristiane Izabela de Souza Terra
Adriana Goulart de Sena Orsini [1]
Camila Cristina de Moura Abreu

Resumo

O texto é uma análise crítica acerca dos impactos causados pelos crimes cibernéticos em meio ao contexto da pandemia da COVID-19. Para isso, foi feita uma revisão bibliográfica de artigos e notícias, além da leitura da Lei 13.709 (Lei Geral da Proteção de Dados) com o intuito de se compreender a complexidade da temática. Também será discutido, no decorrer desse texto, sobre a realidade atual do Brasil em meio à pandemia, de forma a entender o verdadeiro panorama no qual o brasileiro está inserido.

Palavras-chave: Crime cibernético, Phishing, Fake news, Pandemia, Coronavírus

Abstract/Resumen/Résumé

The text is a critical analysis about the impacts caused by the cybercrimes in the COVID-19' s pandemic context. For this, a literature review on articles and news was done in addition to a reading of the Brazilian Law 13,709 (Lei Geral da Proteção de Dados) in order to understand the subject's complexity. Throughout this text, Brazil's current reality will be discussed amongst the pandemic situation too as a way to understand the real outlook where the Brazilian people are.

Keywords/Palabras-claves/Mots-clés: Cybercrime, Phishing, Fake news, Pandemic, Coronavirus

[1] Professora Doutora Associada 3 da Faculdade de Direito da UFMG. Coordenadora e Pesquisadora do Programa RECAJ-UFMG - Ensino, Pesquisa e Extensão em Acesso à Justiça e Solução de Conflitos.

1. CONSIDERAÇÕES INICIAIS

A inclusão de novas tecnologias no dia a dia dos indivíduos vem ocorrendo cada vez mais rapidamente, o que se deve, essencialmente, ao desenvolvimento expressivo da internet e dos meios de comunicação em geral, nos últimos tempos. A internet ocupa, atualmente, um espaço de extrema abrangência no cotidiano das pessoas de todo o mundo, em decorrência das grandes facilidades que proporciona. Tais facilidades foram essenciais no enfrentamento da ainda presente pandemia do novo coronavírus.

No início de 2020, o vírus Sars-Cov-2 trouxe grandes dificuldades para o mundo inteiro com a proliferação da COVID-19, uma doença infecciosa letal e de fácil transmissão, de acordo com a *World Health Organization (WHO) Coronavirus Dashboard* (2020). Com isso, providências tiveram que ser tomadas para conter o avanço da doença, no que se destaca o incentivo às medidas de isolamento social, a exemplo do denominado *lockdown*, caracterizado pela restrição da circulação da população em locais públicos. Eficaz em conter a propagação indiscriminada do vírus, esse isolamento, contudo, trouxe à tona problemas ligados especialmente à economia.

Estabelecimentos comerciais em geral se viram prejudicados com a imposição da restrição de circulação das pessoas, quais sejam clientes e/ou funcionários, e, por consequência, precisaram se reinventar, adaptando-se às novas condições de funcionamento. A alternativa mais adotada pelo setor foi a utilização da internet, haja vista a grande possibilidade de exploração de seus recursos como a possibilidade de realização de reuniões por vídeo, compartilhamento de textos e planilhas, dentre tantos outros meios que proporcionam o chamado *home office*, trabalho realizado em domicílio via internet. Isso contribuiu significativamente para as empresas contornarem a situação atípica e, também, para que a internet fosse ainda mais utilizada por todos.

Se, por um lado, esse crescimento da internet trouxe bons resultados à economia e a outros setores da sociedade quanto ao proveito que fazem das facilidades resultantes disso, por outro, isso fez com que os crimes também se voltassem aos meios cibernéticos com maior intensidade. Ademais, criminosos tiraram proveito daquilo que a internet é capaz de oferecer, contando com o fato de que "para as TICs [Tecnologias da Informação], não há espaço nem tempo, ambos se perderam, pois não há barreiras para se conectar com o mundo tornando o usuário um disseminador e coletor de informações, sejam estas verdadeiras ou não" (MORGENSTERN, G. G.; TISSOT, T. R. G., 2015, p. 01) e, é justamente por isso que os

crimes cibernéticos se tornaram ainda mais frequentes e oportunos aos interessados no bem alheio.

Tendo em vista todo o referido cenário, este trabalho tem como premissa explorar as nuances acerca dos *cybercrimes*, especificamente o *phishing* e as *fake news* no contexto da pandemia da COVID-19, uma vez que a informatização do meio laboral tem contribuído para o crescimento dos crimes cibernéticos. Para isso, o resumo seguirá a vertente crítico-metodológica, que parte de uma teoria crítica da realidade (DIAS, GUSTIN, NICÁCIO, 2020, p. 64), utilizando para isso a revisão bibliográfica de artigos e notícias, a fim de explorar de forma objetiva a temática abordada.

2. *CYBERCRIMES, PHISHING* E *FAKE NEWS*: Definição e classificação

Para maior aprofundamento a respeito do conceito de cibercrime, *cybercrime* ou crime cibernético, é necessário que se busque, primeiramente, a sua correta. Leia-se:

> O Fórum Econômico Mundial (World Economic Forum) de 2019 definiu cibercrimes como toda atividade não-autorizada realizada através de computador para uma empresa ou para uma informação individual com fins maliciosos. Cibercriminosos, ilegalmente, acessam informações do sistema para tomar para si o que pertence a outrem, para fazer mau uso e para comprometer a integridade da informação objetivando ganhos financeiros individuais (CHIGADA; MADZINGA, 2021, tradução nossa)[1].

A título de exemplo e a partir da definição supra, os crimes cibernéticos mais comuns são aqueles voltados à invasão da privacidade alheia, quando os conhecidos hackers invadem a conta privativa de um indivíduo em uma rede social, quando da aplicação de golpes através da comunicação via e-mail ou WhatsApp. Há a congruência de tudo isso pelo fato de que há de se ter conhecimento sobre as ferramentas da internet para que se possa utilizá-las com finalidade criminosa. Sendo assim, neste estudo destacam-se dois crimes cibernéticos em voga mediante o contexto atual, quais sejam: o *phishing* e as *fake news*.

Phishing diz respeito à aplicação de golpes em que o criminoso utiliza de falsa prerrogativa para se obter a confiança da vítima a ponto de convencê-la a compartilhar seus dados. Geralmente, esses dados contêm informações de contas bancárias e, assim, os criminosos têm acesso ao valor que a vítima possui em dinheiro e, então, furtam-na. Mais detalhadamente,

[1] Original em inglês: "The World Economic Forum [WEF] (2019) defined cybercrimes as all unauthorised computer-mediated activities to a company or an individual's information with malicious intent. Cybercriminals illegally access information systems to steal, misuse and compromise the integrity of information for personal financial gains."

os autores Morgenstern e Tissot (2015, p. 02) esclarecem a origem do termo que dá nome a esse crime. Leia-se:

> O termo phishing é originado da palavra inglesa fishing, que significa pescar, ou seja, é a conduta daquele que pesca informações sobre o usuário de computador. É um tipo de fraude eletrônica, onde o golpista busca obter informações pessoais do usuário como senhas, dados financeiros, números de cartões de crédito e outros dados pessoais.

As *fake new*s, termo traduzido como notícias falsas em português, são outro tipo de crime cibernético que merecem especial atenção pelo impacto que podem provocar. Dizem respeito a criação de mentiras que se propagam rapidamente através das redes sociais, no caso do Brasil, especialmente pelo WhatsApp. O problema maior decorrente das *fake news* está no fato de que, devido a enorme quantidade de informações que a internet propaga sem nenhum filtro daquilo que é verdadeiro e do que é falso, muitos indivíduos acabam por acreditar nessas mentiras, contrariando aquelas notícias que são, de fato, verdadeiras.

Tamanho o impacto das *fake news* que esse termo ganhou maior relevância justamente a partir das eleições presidenciais dos EUA no ano de 2016, ano em que tomou proporções a ponto de prejudicar e influenciar o voto de toda uma nação. Pensando nisso, Estabel, Luce e Santini (2020), seguindo Zuckerman (2017), colocam as *fake news* em três categorias distintas: "1) A notícia falsa para desviar a atenção do problema real; 2) A propaganda, onde é usada a notícia falsa para promover um candidato e denegrir a imagem do outro; 3) E um número grande de notícias falsas, confundindo o leitor pelo excesso de informação."

3. A LEI GERAL DE PROTEÇÃO DE DADOS E SUA RELAÇÃO COM OS CRIMES CIBERNÉTICOS

A Lei Geral de Proteção de Dados, popularmente conhecida pela sigla LGPD, corresponde à Lei 13.709, aprovada em agosto de 2018 e que entrou em vigência em agosto de 2020. Essa lei visa preservar o direito constitucional de liberdade e privacidade, protegendo os cidadãos de futuros danos causados pela ruptura de tais direitos. Sendo assim, a LGPD é válida em todo o território nacional e sua aplicação vai muito além da mera aplicação nos meios digitais, tratando-se assim, da proteção dos dados em sentido amplo.

Uma das bases da LGPD é o consentimento, sendo que o equilíbrio entre os interesses dos titulares e as necessidades dos controladores em suas atividades, devem ser preservados. Pode-se dizer, portanto, que a LGPD foi criada com finalidade comercial, a fim de equilibrar a balança entre os dois lados. Por sua vez, é a Autoridade Nacional de Proteção de Dados (ANPD)

que gerencia as regras da LGPD, sendo o órgão responsável que garante com que a lei seja cumprida. A ANPD realiza auditorias e também pode impor sanções em caso de descumprimento da lei.

Em se tratando dos crimes cibernéticos, é notável que o crescimento do uso da internet tem contribuído massivamente para o crescimento dessa modalidade criminosa, tendo em vista que muitas pessoas utilizam a internet para diversas atividades na atualidade, tais como movimentações bancárias, pagamentos de boletos, compras online etc. Sendo assim, os *cybercrimes* tornaram-se comuns nos últimos anos, tendo crescido exponencialmente durante o período da pandemia da COVID-19, segundo o jornal O Globo.

4. *PHISHING* E *FAKE NEWS* NO CONTEXTO DA PANDEMIA

O *Phishing* nada mais é do que uma prática criminosa em que dados pessoais são extraídos de pessoas nos meios cibernéticos, a fim de aplicar golpes nesses indivíduos. Esse tipo de *cybercrime* aumentou muito durante o período da pandemia, principalmente tendo em vista que o uso dos meios digitais cresceu devido ao *home-office*.

Segundo uma pesquisa realizada pela Sophos em 2020, esse tipo de ataque vem ganhando proporções cada vez maiores, principalmente desde o início da quarentena, no qual foi constatado que muitas empresas de TI tiveram suas caixas de e-mail bombardeadas de tentativas de *phishing*. No Brasil, mais de 200 empresas participaram da pesquisa, e desse número, 73% (setenta por cento) disseram terem notado um aumento nos ataques de *phishing* (PHISHING INSIGHTS, 2020).

Outro problema conspícuo na atualidade brasileira, que se mostra de forma gritante durante a pandemia, é a realidade das *fake news*. Sabe-se que esse problema já estava presente no cenário brasileiro desde antes da eclosão da pandemia, principalmente durante o período eleitoral de 2018. Contudo, no início do processo pandêmico, começaram a surgir inúmeras notícias, que circulavam rapidamente pela internet, alcançando milhares, senão milhões de usuários, com informações errôneas e falsas, com o intuito de causar medo, pânico e desinformação.

As *fake news* acabaram por se tornar um dos maiores empecilhos no processo de vacinação no Brasil, além de corroborar exponencialmente com o negacionismo proveniente da banalização do impacto da COVID-19 por parte de parcela da população, mesmo com o Brasil batendo a marca de mais de 609 mil mortos, atualmente, segundo dados *do Our World in Data* (2021). Resta claro o modo como as *fake news* impactam negativamente na vida dos indivíduos.

5. CONSIDERAÇÕES FINAIS

Ante o exposto, a realidade factível em que se encontra o brasileiro está embargada de perigos e armadilhas quando se fala dos crimes cibernéticos. Durante a pandemia, claramente, esse tipo de prática ganhou maiores proporções, impactando negativamente a vida de milhões de indivíduos pelo país. Golpes na internet sempre foram muito presentes no Brasil, afetando desde jovens até idosos em todo o território nacional. Com a pandemia, porém, muitas empresas também passaram a ser vítimas desse tipo de atividade ilícita, além de todos os brasileiros leigos que antes já eram público-alvo desses golpistas.

Portanto, os meios cibernéticos são uma extensão do que é a sociedade e, por consequência, destaca-se a importância de dispositivos legais, como a LGPD, para que o ambiente virtual seja tão regulado quanto o meio físico. Para além dos dados, o próprio indivíduo, nessa nova realidade, posicionado como usuário digital deve ser protegido.

No entanto, é perceptível que a LGPD, embora seja uma lei efetiva em muitos aspectos, não protege integralmente os dados dos brasileiros, sendo insuficiente contra crimes como o *phishing* e os golpes por disseminação de *fake news.* Nota-se, assim, a importância de mais mecanismos de proteção jurídica do usuário digital no cenário brasileiro, tendo em vista a demanda recorrente que surgiu durante a pandemia do novo coronavírus.

REFERÊNCIAS BIBLIOGRÁFICAS

CHIGADA, Joel; MADZINGA, Rujeko. *Cyberattacks and threats during COVID-19*: A systematic literature review. SAJIM (Online). Cidade do Cabo, v. 23, n. 1, p. 1-11, 2021. Disponível em: http://www.scielo.org.za/scielo.php?script=sci_arttext&pid=S1560-683X2021000100001&lang=pt. Acesso em: 15 de out. de 2021.

CRIMES cibernéticos devem avançar mesmo com LGPD. Infocredi360, 2021. Disponível em: https://infocredi360.com.br/exclusivos/crimes-ciberneticos-devem-avancar-mesmo-com-a-lgpd. Acesso em: 06 de nov. de 2021.

CORONAVIRUS (COVID-19) Deaths. Our World in Data, 2021. Disponível em: https://ourworldindata.org/covid-deaths. Acesso em: 30 de out. de 2021.

DIAS, Maria Tereza Fonseca; GUSTIN, Miracy Barbosa de Sousa; NICÁCIO, Camila Silva. *(Re)pensando a Pesquisa Jurídica*: teoria e prática. 5. ed. São Paulo: Almedina, 2020.

ESTABEL, Lizandra Brasil; LUCE, Bruno Fortes; SANTINI, Luciene Alves. *Idosos, fake news e letramento informacional.* UFRGS: Lume Repositório Digital. Revista Brasileira de Biblioteconomia e Documentação, São Paulo, v. 16, p. 1-15, 2020.

MORGENSTERN, Grasiele Giusti; TISSOT, Tania Regina Gottardo. *Crimes Cibernéticos: Phishing - Privacidade Ameaçada.* Salão do Conhecimento, 2015.

WARBURTON, David. *2020 Phising and Fraude Report*. F5 Labs – Application Threat Intelligence, 2020. Disponível em: https://www.f5.com/labs/articles/threat-intelligence/2020-phishing-and-fraud-report. Acesso em: 20 de out. de 2021.

WHO Coronavirus (COVID-19) Dashboard. World Health Organization, 2020. Disponível em: https://covid19.who.int/. Acesso em: 04 de nov. de 2021.