CONGRESSO INTERNACIONAL DE DIREITO E INTELIGÊNCIA ARTIFICIAL

OS DIREITOS HUMANOS NA ERA TECNOLÓGICA II

CAMILA MARTINS DE OLIVEIRA

FABRÍCIO GERMANO ALVES

O81
Os direitos humanos na era tecnológica II [Recurso eletrônico on-line] organização Congresso Internacional de Direito e Inteligência Artificial: Skema Business School – Belo Horizonte;

Coordenadores: Fabrício Germano Alves, José Luiz de Moura Faleiros Júnior e Camila Martins de Oliveira – Belo Horizonte: Skema Business School, 2020.

Inclui bibliografia
ISBN: 978-65-5648-104-3
Modo de acesso: www.conpedi.org.br em publicações
Tema: Desafios da adoção da inteligência artificial no campo jurídico.
1. Direito. 2. Inteligência Artificial. 3. Tecnologia. I. Congresso Internacional de Direito e Inteligência Artificial (1:2020 : Belo Horizonte, MG).

CDU: 34

CONGRESSO INTERNACIONAL DE DIREITO E INTELIGÊNCIA ARTIFICIAL

OS DIREITOS HUMANOS NA ERA TECNOLÓGICA II

Apresentação

É com enorme alegria que a SKEMA Business School e o CONPEDI – Conselho Nacional de Pesquisa e Pós-graduação em Direito apresentam à comunidade científica os 14 livros produzidos a partir dos Grupos de Trabalho do I Congresso Internacional de Direito e Inteligência Artificial. As discussões ocorreram em ambiente virtual ao longo dos dias 02 e 03 de julho de 2020, dentro da programação que contou com grandes nomes nacionais e internacionais da área, além de 480 pesquisadoras e pesquisadores inscritos no total. Estes livros compõem o produto final deste que já nasce como o maior evento científico de Direito e da Tecnologia do Brasil.

Trata-se de coletânea composta pelos 236 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 quatro Grupos de Trabalho originais, diante da grande demanda, se transformaram em 14 e contaram com a participação de pesquisadores de 17 Estados da federação brasileira. São cerca de 1.500 páginas de produção científica relacionadas ao que há de mais novo e relevante em termos de discussão acadêmica sobre os temas Direitos Humanos na era tecnológica, inteligência artificial e tecnologias aplicadas ao Direito, governança sustentável e formas tecnológicas de solução de conflitos.

Os referidos Grupos de Trabalho contaram, ainda, com a contribuição de 41 proeminentes professoras e professores ligados a renomadas instituições de ensino superior do país, os quais indicaram os caminhos para o aperfeiçoamento dos trabalhos dos autores. Cada livro desta coletânea foi organizado, preparado e assinado pelos professores que coordenaram cada grupo. Sem dúvida, houve uma troca intensa de saberes e a produção de conhecimento de alto nível foi, certamente, o grande legado do evento.

Neste norte, a coletânea que ora torna-se pública é de inegável valor científico. Pretende-se, com esta publicação, contribuir com a ciência jurídica e fomentar o aprofundamento da relação entre a graduação e a pós-graduação, seguindo as diretrizes oficiais. Fomentou-se, ainda, a formação de novos pesquisadores na seara interdisciplinar entre o Direito e os vários

campos da tecnologia, notadamente o da ciência da informação, haja vista o expressivo número de graduandos que participaram efetivamente, com o devido protagonismo, das atividades.

A SKEMA Business School é entidade francesa sem fins lucrativos, com estrutura multicampi em cinco países de continentes diferentes (França, EUA, China, Brasil e África do Sul) e com três importantes acreditações internacionais (AMBA, EQUIS e AACSB), que demonstram sua vocação para ensino e pesquisa de excelência no universo da economia do conhecimento. A SKEMA, cujo nome é um acrônimo significa School of Knowledge Economy and Management, acredita, mais do que nunca, que um mundo digital necessita de uma abordagem transdisciplinar.

Agradecemos a participação de todos neste grandioso evento e convidamos a comunidade científica a conhecer nossos projetos no campo do Direito e da tecnologia. Já está em funcionamento o projeto Nanodegrees, um conjunto de cursos práticos e avançados, de curta duração, acessíveis aos estudantes tanto de graduação, quanto de pós-graduação. Até 2021, será lançada a pioneira pós-graduação lato sensu de Direito e Inteligência Artificial, com destacados professores da área.

Agradecemos ainda a todas as pesquisadoras e pesquisadores pela inestimável contribuição e desejamos a todos uma ótima e proveitosa leitura!

Belo Horizonte-MG, 07 de agosto de 2020.

Profª. Drª. Geneviève Daniele Lucienne Dutrait Poulingue

Reitora – SKEMA Business School - Campus Belo Horizonte

Prof. Dr. Edgar Gastón Jacobs

Coordenador Acadêmico da Pós-graudação de Direito e Inteligência Artificial da SKEMA Business School

ASPECTOS CONTROVERSOS SOBRE SEQUESTRO DIGITAL

CONTROVERSAL ASPECTS ABOUT DIGITAL HACKING

Rafael Miranda Amazonas [1]

Resumo

O presente resumo expandido trata da intenção de análise jurisprudencial dos casos de sequestro digital em âmbito nacional e internacional. Busca evidenciar que a constituição não abarca especificamente os casos de sequestro digital. A pesquisa que se propõe pertence à vertente metodológica jurídico-sociológica. No tocante ao tipo de investigação, foi escolhido, o tipo jurídico-projetivo. Faz o uso de fontes primárias e secundárias para se fundamentar a hipótese. Detalha o vírus mostrando sua história e seu funcionamento.Aborda o impacto em ambito nacional e internacional Com isso, demonstra o grande impacto dos cybers ataques de ransomware na sociedade atual.

Palavras-chave: Sequestro digital, Ransomware, Jurisprudência, Cyber ataque, Vazamento de dados

Abstract/Resumen/Résumé

This expanded summary deals with the intention of jurisprudential analysis of cases of digital hijacking at national and international levels. It seeks to show that the constitution does not specifically cover cases of digital hijacking. The proposed research belongs to the juridical-sociological methodological aspect. Regarding the type of investigation, the legal-projective type was chosen. It uses primary and secondary sources to support the hypothesis. It details the virus showing its history and its operation. It addresses the impact in national and international scope. With this, it demonstrates the great impact of cyber ransomware attacks in the current society.

Keywords/Palabras-claves/Mots-clés: Digital hijacking, Ransomware, Jurisprudence, Cyber-attack, Data leak

[1] Aluno de direito, modalidade integral, pela Escola Superior Dom Hélder Câmara

1.CONSIDERAÇÕES INICIAIS

A presente pesquisa apresenta seu nascedouro no tema que aborda a concessão de justiça nos casos de sequestro digital, em âmbito nacional e internacional. Atualmente não existe uma legislação específica que abarca esse tipo de crime, e devido a crescente no aumento nos números de casos, principalmente no Brasil, se faz necessária a análise jurisprudencial dos casos. Assim, esse crime tem influenciado diretamente a sociedade e causa impactos em diversas áreas do coletivo.

Nesse sentido, os crimes virtuais estão cada vez mais comuns no dia a dia. No entanto, por se tratar de um efeito relativamente novo, ainda são desconhecidos por grande parte da população e pouco aprofundados no campo jurídico. Sendo assim, os hackers se aproveitam dessa condição de desconhecimento da população para aplicarem golpes e lucrar com isso. Complementarmente, a Associação do Ministério Público de Minas Gerais (2012) aponta que a cada minuto 54 pessoas são vítimas de crimes digitais.

Sendo assim, crimes cibernéticos tem crescido cada vez mais. Porém, o que seria sequestro digital e qual a relevância de sua análise? Sequestro digital é o crime onde hackers encriptam dados de vítimas, desde contas de redes sociais a senhas bancárias, por meio de ferramentas como o ransomware e exigem um pagamento, geralmente na forma de criptomoedas como o bitcoin, para poder decodificar as informações e devolver ao indivíduo. Com isso, essa prática vem se tornando cada vez mais comum e faz milhares de vítimas todos os anos, contudo é pouco estudada no âmbito jurídico.

A pesquisa que se propõem pertence à vertente metodológica jurídico-sociológica. No tocante ao tipo de investigação, foi escolhido, na classificação de Witker (1985) e Gustin (2010), o tipo jurídico-projetivo. O raciocínio desenvolvido na pesquisa será predominantemente dialético. Dessa maneira, a pesquisa se propõe a analisar a jurisprudência dos casos de sequestro digital, avaliando a atual tipificação a qual os casos são encaixados e julgados.

O IMPACTO GLOBAL DO RAMSOMWARE

O sequestro digital é um fenômeno relativamente recente, porém que já causou grandes impactos. Nesse sentido, o vírus ficou conhecido mundialmente após um grande ataque denominado Wanna Cry, o ataque foi relatado no portal da *British Broadcasting Corporation*- BBC que afirma:

> Um grande cyber-attack usando ferramentas que acredita-se serem roubadas da Agencia Nacional de Segurança do Estados Unidos da América atingiu

> diversas organizações ao redor do mundo. A empresa de segurança cibernética Avast disse ter visto 75.000 casos do ransomware - conhecido como WannaCry e variantes desse nome - em todo o mundo. Há relatos de infecções em 99 países, incluindo Rússia e China. (Tradução nossa)1

Nesse sentido, é evidente que o WannaCry teve grande impacto em boa parte do mundo, gerando um prejuízo de aproximadamente 1 bilhão(CHRYS, 2017). Porém, os hackers ganharam uma quantia bem menor, pois cerca de 302 pessoas acabaram se rendendo aos criminosos, sendo assim, acumularam cerca de $126.742, cento e vinte seis mil setecentos e quarenta e dois dólares.

No mesmo plano, uma das maiores fabricantes de automóveis do mundo, Honda, sofreu um ataque por um vírus denominado "Snake" que acarretou uma pausa em sua linha de operação em nível global. Assim, percebemos que o sequestro digital está presente em diversas esferas, inclusive na automobilística. Porém, infelizmente os hackers não sofrem punições devido a leis pouco abrangentes e rigorosas e ao seu anonimato.

Portanto, em âmbito global o ransomware pode atingir qualquer empresa, seja ela de pequeno ou grande porte, caso da Honda, e até mesmo órgãos governamentais, caso WannaCry. Assim, um estudo aprofundado deve ser feito para que as leis sejam abrangentes e punitivas, pois atualmente poucos hackers são presos. Logo, o sequestro digital ainda é pouco tipificado legalmente e necessita de um estudo legislativo aprofundado.

OS ASPECTOS CONTROVERSOS SOBRE SEQUESTRO DIGITAL NO BRASIL

Atualmente em âmbito nacional os crimes de sequestro digital são julgados por analogia segundo o art. 158 do código penal brasileiro. Sendo assim, são encarados sob a ótica de extorsão. Porém como não são tipificados propriamente em lei possuem muitas brechas e os criminosos na maioria das vezes saem impunes

Contextualizando-se, no Brasil, tem-se o caso da atriz Carolina Dieckmann que teve fotos intimas divulgadas na internet. Assim, detalhando o caso, o empresário de Carolina recebeu as fotos por email e um aviso pedindo a quantia de R$10 mil para que

[1] No original: "A massive cyber-attack using tools believed to have been stolen from the US National Security Agency (NSA) has struck organisations around the world. Cyber-security firm Avast said it had seen 75,000 cases of the ransomware - known as WannaCry and variants of that name - around the world.There are reports of infections in 99 countries, including Russia and China."

as mesmas não fossem divulgadas. A atriz acabou não cedendo aos hackers e teve suas fotos divulgadas. Contudo, o caso não ficou sem solução como grande parte de outras jurisprudência, a polícia encontrou quatro suspeitos que estão sendo indiciados no momento.

Outrossim, o episódio repercutiu de tal forma que na época a atual presidente, Dilma Rousseff, acabou sancionando a lei 12.737 que em seu Art. 2º de 30 de novembro de 2012 (BRASIL, 2012) prevê:

> 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.

Contudo, segundo o professor português (MASSENO, 2014): “A apontada Lei (Carolina Dieckmann) é uma das consequências de legislar apressadamente, como ocorreu "in casu"”. Pois, segundo o doutor (CRESPO, 2015) a legislação ainda não é precisa e técnica suficientemente e as penas atribuídas aos crimes deveriam ser mais adequadas à gravidade das condutas, porém essa ainda é a lei mais específica que se tem sobre crimes digitais em nosso legislativo.

No mesmo sentido, segundo (BERRETA, 2014): “o legislador apenas se preocupou em criminalizar um fato isolado, possibilitando à(s) Carolina(s) o seu direito de punir, direito este pertencente ao Estado e suas leis.”. Assim, a crítica é que a lei embora represente um marco no direito digital brasileiro foi mal elaborada pois o legislador pretendeu tomar um fato isolado e o tipo penal sem a mínima cautela (BERRETA, 2014).

Além disso, a lei não atingiu o seu caráter intimidatório, pois prevê: “Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa” (BRASIL, 2012). Sendo assim, os criminosos não se amedrontam com a punição, não só pela pena que é mínima, mas como também pelas brechas que ela apresenta como explicitado abaixo:

> Em primeiro lugar, nos parece que o tipo penal em questão data venia já começou mal, pois é tratado como um crime meramente formal, vez que para sua consumação exige-se apenas a invasão a um dispositivo informático alheio. A simples invasão, no entanto, (invadir por invadir) não configura o crime, vez que se exige a finalidade específica de obter, adulterar ou destruir dados e informações, de acordo com a estrita legalidade em matéria penal. Em segundo lugar, o tipo penal do artigo 154-A não fornece a definição exata de “mecanismo de segurança”, questão fulcral para cometimento ou não do crime, assim, se o dispositivo invadido não possuir qualquer tipo de proteção (senha, antivírus, firewall etc.), a conduta será atípica, uma vez inexistente a modalidade culposa. Por último, estabelece que este mecanismo deva ser indevidamente violado, invadido, devassado. (BERRETA, 2014)

Portanto, percebe-se a contradição nos casos de sequestro digital no Brasil, pois apesar de existir uma lei que tipifica crimes digitais ela ainda é pouco punitiva e abrangente, tanto que os crimes de sequestro digitais são enquadrados como extorsão. Sendo assim, o crime não é devidamente tipificado no Brasil e sua lei respectiva apresenta falhas e a sua lei analógica apresenta controversas como apontado no texto. Logo, se faz necessário o devido estudo jurídico dos casos a fim de aprimorar as leis atuais ou então criar novas.

CONSIDERAÇÕES FINAIS

A partir do exposto, verifica-se que além de o Brasil enfrentar problema com a resolução de crimes de sequestro digital, o mundo também passa pelo mesmo impasse. Pois, por ser um crime relativamente novo ainda é pouco tipificado e estudado por completo. Assim, existem muitas brechas nas legislações, no caso do Brasil tem-se as falhas da Lei Carolina Dieckmann.

Dessa forma, é necessário ressaltar que as leis ainda são pouco abrangentes e punitivas e precisam ser adaptadas. Além disso, cabe ressaltar que um estudo profundo dos casos deve ser feito, pois caso contrário só teremos legislações feitas as pressas, como no caso da lei 12.737, que acabam não contemplando os casos no geral e acarretam na perca de sentido da legislação.

Portanto, percebe-se que o sequestro digital é um problema global e pode atingir todos. Porém, ainda não existem leis suficientemente abrangentes e punitivas, não só por ser um fenômeno recente, mas como também pelo pouco estudo dos casos por juristas. Com isso, infere-se o grande impacto dos crimes digitais em toda a sociedade e ainda mais o fato dos hackers não serem punidos devidamente pelas brechas nas leis.

REFERÊNCIAS BIBLIOGRÁFICAS

BERETTA. ***Sem meios eficazes, Lei Carolina Dieckmann até atrapalha.*** Conjur- 10 de mai. 2014. Disponível em : https://www.conjur.com.br/2014-mai-10/pedro-beretta-meios-eficazes-lei-carolina-dieckmann-atrapalha. Acesso em: 07 de jun. 2020

BRASIL. ***Carolina Dieckmann fala pela 1º vez, sobre fotos e diz que espera "justiça".*** Portal G1- 14 mai. 2012. Disponível em: Acesso em: 03 de jun. 2020.

REINO UNIDO**.** ***Massive ransomware infection hits computers in 99 countries.*** Portal BBC NEWS- 13 de mai. 2017. Disponível em: https://www.bbc.com/news/technology-39901382. Acesso em: 03 de jun. 2020.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. ***Dispõe sobre a tipificação criminal de delitos informáticos***. Brasília, DF, nov. de 2012 Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 03 de jun. 2020.

CRESPO. ***As Leis nº 12.735/2012 e 12.737/2012 e os crimes digitais: acertos e equívocos legislativos***. Academia.edu- 24 de jun. 2015. Disponível em: https://www.academia.edu/14673894/As_Leis_no_12.735_2012_e_12.737_2012_e_os_crimes_digitais_acertos_e_equ%C3%ADvocos_legislativos. Acesso em: 07 de jun. 2020.

RODRIGUES. ***Catástrofe digital: ciberataque global pode superar R$ 382 bi em prejuízos***. Portal Tecmundo 19 de jul. 2017. Disponível em : https://www.tecmundo.com.br/seguranca/119464-catastrofe-digital-ciberataque-global-superar-r-382-bi-prejuizos.htm. Acesso em: 03 de jun. 2020.

CHRYS. ***Wannacry causou mais de US$ 1 bilhão em prejuízos.*** Portal BtcSoul 27 mai. Disponível em: https://www.btcsoul.com/noticias/wannacry-causou-mais-us-1-bilhao-prejuizos/. Acesso em: 03 de jun. 2020.