

**II CONGRESSO INTERNACIONAL DE
DIREITO E INTELIGÊNCIA
ARTIFICIAL**

DIREITO PENAL E CIBERCRIMES

D597

Direito Penal e Cibercrimes [Recurso eletrônico on-line] organização Congresso Internacional de Direito e Inteligência Artificial: Skema Business School – Belo Horizonte;

Coordenadores: Fernando Henrique da Silva Horita; Fausto Santos de Moraes; Camila Martins de Oliveira. – Belo Horizonte:Skema Business School, 2021.

Inclui bibliografia

ISBN: 978-65-5648-263-7

Modo de acesso: www.conpedi.org.br

Tema: Um olhar do Direito sobre a Tecnologia

1. Direito. 2. Inteligência Artificial. 3. Tecnologia. II. Congresso Internacional de Direito e Inteligência Artificial (1:2021 : Belo Horizonte, MG).

CDU: 34



II CONGRESSO INTERNACIONAL DE DIREITO E INTELIGÊNCIA ARTIFICIAL

DIREITO PENAL E CIBERCRIMES

Apresentação

Renovando o compromisso assumido com os pesquisadores de Direito e tecnologia do Brasil, é com grande satisfação que a SKEMA Business School e o CONPEDI – Conselho Nacional de Pesquisa e Pós-graduação em Direito apresentam à comunidade científica os 12 livros produzidos a partir dos Grupos de Trabalho do II Congresso Internacional de Direito e Inteligência Artificial (II CIDIA). As discussões ocorreram em ambiente virtual ao longo dos dias 27 e 28 de maio de 2021, dentro da programação que contou com grandes nomes nacionais e internacionais da área em cinco painéis temáticos e o SKEMA Dialogue, além de 354 inscritos no total. Continuamos a promover aquele que é, pelo segundo ano, o maior evento científico de Direito e Tecnologia do Brasil.

Trata-se de coletânea composta pelos 255 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 originais, diante da grande demanda, se transformaram em doze e contaram com a participação de pesquisadores de vinte e um Estados da federação brasileira e do Distrito Federal. São cerca de 1.700 páginas de produção científica relacionadas ao que há de mais novo e relevante em termos de discussão acadêmica sobre a relação da inteligência artificial e da tecnologia com os temas acesso à justiça, Direitos Humanos, proteção de dados, relações de trabalho, Administração Pública, meio ambiente, formas de solução de conflitos, Direito Penal e responsabilidade civil.

Os referidos Grupos de Trabalho contaram, ainda, com a contribuição de 36 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, mais uma vez, 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 creditações internacionais (AMBA, EQUIS e AACSB), que demonstram sua vocação para pesquisa de excelência no universo da economia do conhecimento. A SKEMA 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. Em breve, será lançada a pioneira pós-graduação lato sensu de Direito e Inteligência Artificial, com destacados professores da área. A SKEMA estrutura, ainda, um grupo de pesquisa em Direito e Inteligência Artificial e planeja o lançamento de um periódico científico sobre o tema.

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

Belo Horizonte-MG, 09 de junho de 2021.

Prof^a. Dr^a. 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

O ASSUSTADOR AUMENTO DE CIBERCRIMES NA PANDEMIA COVID-19
THE FRIGHTENING INCREASE IN CYBERCRIME IN THE WORLD PANDEMIC
COVID-19

Melhyna Pires Aarão

Resumo

O desenvolvimento dessa pesquisa foi baseada no aumento assustador da criminalidade nos ciberespaços na pandemia do covid-19, agravado pela vulnerabilidades de pessoas tomadas pela angústia do isolamento social e, o significativo aumento no número de usuários ligados ao crime organizado aproveitando-se de comunicações globais para mascarar suas atividades maliciosas; os desafios das autoridades no combate a crimes virtuais, e a essencial necessidade de uma cooperação universal, adotando políticas de controle de criminalidade na rede, de tal modo que nenhum país consegue combater sozinho um crime transnacional, desconhecedor de fronteiras, causando graves danos no mundo inteiro.

Palavras-chave: Palavras chaves: cibercrimes, Pandemia do covid-19, Aumento do fluxo criminal na rede

Abstract/Resumen/Résumé

The development of this research was based on the frightening increase in cyberspace crime in the covid-19 pandemic, aggravated by the vulnerabilities of people taken by the anguish of social isolation and the significant increase in the number of users linked to organized crime taking advantage of global communications. to mask their malicious activities; the challenges of the authorities in combating cybercrimes, and the essential need for universal cooperation, adopting crime control policies on the network, in such a way that no country can fight a transnational crime, unaware of borders, causing serious damage in the world. whole.

Keywords/Palabras-claves/Mots-clés: Keywords: cybercrime, Covid-19 pandemic, Increased criminal flow in the network

INTRODUÇÃO

Muito se tem falado sobre crimes virtuais, e discussões sobre a Web são intermináveis, não seria uma exceção, por tanto junto com o novo coronavírus, estamos enfrentando uma avassaladora onda de crimes cibernéticos, impulsionado pela instantaneidade que esses crimes tanto fazem vítimas, quanto se modernizam, camuflados pela deslocalização e a-temporalidade proporcionando rapidez na consumação e, tornando muito mais difícil a localização desses delinquentes; já que onde o agente comete o crime é diferente dos seus efeitos, sendo praticado na privacidade de suas residências, escritórios sem muita dificuldade. O anonimato é outra característica tentadora dessa modalidade criminosa, agravada pelo crescente número de usuários ligados ao crime organizado, inclusive por criminosos sem experiência anterior no Ciberespaço.

O Escritório das Nações Unidas sobre Drogas e Crime (UNODC), fez uma análise introdutória das ameaças habilitadas para Darknet contra países do sudeste Asiático, o relatório avalia a partir de perspectivas de usuários, criminosos e policiais, com um foco na criminalidade cibernética. Acredita-se que um número crescente de criminosos esteja usando a Darknet Tor para se envolver em toda gama de atividades ilícitas, tendo diariamente relatos de algo novo sendo comercializado na rede, com modalidades de crimes mais variados.

A ações criminosas visam principalmente, compra e venda de drogas, kits de ferramentas para crimes cibernéticos, passaportes falsos, moeda falsa, material de exploração infantil online, cartões de créditos, violações de identificação pessoal, tráficos de armas e pessoas, fraudes financeiras, crimes encomendados, intolerância racial e Religiosa, terrorismo, Invasão de privacidade, Assédio moral, sexual e psicológico, Homofobia, transações ilícitas de criptomoedas, Apologia e incitação a crimes contra a vida dentre outros... (UNODC, 2021).

A Darkweb atrai sites por oferecer anonimato e está livre da censura online, apresentando um crescimento considerável anual tendo seus números excepcionalmente aumentados pela pandemia do Covid-19. As ameaças cibernéticas estão em constante evolução para acompanhar as tendências da internet, os cibercriminosos disseminam vírus maliciosos causando prejuízos na velocidade da luz em todo globo terrestre.

É importante salientar o aperfeiçoamento e sofisticação das técnicas com propósito de prática delituosa, a criminalidade cibernética possui mais conhecimentos tecnológicos que um usuário de internet comum, buscam países de menor capacidade legal e tecnológica para intensificar suas práticas criminosas. Como efeito problema dessa pesquisa, embasada na explosão dos crimes cibernéticos- O principal desafio é a questão da territorialidade pelo princípio da competência territorial e redefinição de fronteiras com leis abrangentes que possam entender essa nova estrutura em campo virtual.

1

Os cibercriminosos estão atacando as redes e sistemas de computadores de indivíduos, empresas e até organizações globais em um momento em que as defesas cibernéticas podem ser reduzidas devido à mudança de foco para a crise de saúde INTERPOL, 2021)

¹ Escritório Nações Unidas sobre Drogas e Crime (UNODC). Darknet Cybercrimes Threats to Southeast Asia.

Levando-se em conta que o Brasil ocupa o quarto na posição no tráfego de internet do mundo, ficando atrás apenas dos Estados Unidos, Rússia e China, com o número de brasileiros que usam a internet continua crescendo: subiu de 67% para 70% da população, o que equivale a 126,9 milhões de pessoas, estimando-se mais de quatrocentos milhões de aparelhos conectados entre computadores, celulares e Tablets, tornando um trabalho árduo sem uma política regional, nacional e internacional no combate eficaz dos cibercriminosos cometidos por meios eletrônicos.

A Internet cresce a cada dia. Assim, os números mais recentes, segundo um relatório produzido pelo We Are Social e Hootsuite de janeiro de 2021, apontam para que existam 4,66 bilhões de usuários na rede. Curiosamente, o mesmo relatório aponta para a existência de 5,22 bilhões de usuários com dispositivos móveis. Se no planeta existe, segundo estimativas de julho de 2020, uma população global 7,8 bilhões de pessoas, então mais de metade do mundo está ligado na rede (ISTOE, 2021).

METODOLOGIA

A metodologia empregada baseia-se em pesquisa exploratória virtual, em sites de grande credibilidade e de governos buscando contextualizar, compreender e descrever o problema desta pesquisa, focando nas principais abordagens com objetivo de oferecer contribuições com fundamentos em abordagens na internet.

CONCLUSÃO

Embora nem tudo na Deepweb seja ilícito, nota-se que está longe de ser uma prioridade nas políticas antes crimes dos países, há várias lacunas na proteção de dados no tráfego de informações em âmbito universal, tendo uma necessidade absoluta de liderança ministerial em assuntos cibernéticos em cada país para garantir que os responsáveis pela aplicação de leis possam dar suporte legal e, redefinições de fronteiras, necessitando de apoio político consistente para realizar as operações mais desafiadoras. Segundo a UNODC, operações conduzidas em Darknets são previsíveis e evitáveis e, busca-se debater a viabilidade de mecanismos e instrumentos preventivos, em uma política criminal voltada para união de nações trabalhando arduamente para criação de recursos tecnológicos de alta velocidade em abrangência mundial. Existe uma carência em estruturas legislativas que estejam interligadas com governos internacionais. É essencial uma força tarefa em combate para romper a blindagem digital imposta por esses crimes. As necessidade de adotar políticas públicas Criminais destinadas à prevenção e controle na rede, baseadas em novas tecnologias em segurança pública com redefinições de fronteiras e novos limites Territoriais nas leis do Ciberespaços, e os desafios para realizar uma política criminal baseada principalmente em mudanças de leis e instrumentos de inovações tecnológicas para criações em combate as ubiquidade imposta pela instantaneidade, dificultado a identificação desses delitos transnacionais.

Em janeiro de 2021 o Brasil aderiu a Convenção de Budapeste, o processo foi iniciado em julho último, quando o governo manifestou sua intenção de adquirir ao instrumento

internacional, para acesso mais ágil em prova eletrônica sob jurisdição estrangeiras, cooperação internacional. O Comitê de Ministros do Conselho da Europa convidou o Brasil a aderir à Convenção sobre Crimes Cibernéticos, também conhecida como Convenção de Budapeste, celebrada em 2001. O processo foi iniciado em julho último, quando o Governo brasileiro manifestou sua intenção de aderir ao instrumento internacional.

O ingresso nesse acordo de cooperação proporcionará às autoridades brasileiras acesso mais ágil a provas eletrônicas sob jurisdição estrangeira, além de mais efetiva cooperação jurídica internacional voltada à persecução penal dos crimes cibernéticos. Trata-se de iniciativa decorrente de trabalho de coordenação interinstitucional, constituído para esse fim, entre o Ministério das Relações Exteriores, a Polícia Federal (PF) e o Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional (DRCI) – ambos do Ministério da Justiça e Segurança Pública –, o Gabinete de Segurança Institucional da Presidência da República, a Agência Brasileira de Inteligência e o Ministério Público Federal. O Ministro da Justiça e Segurança Pública, Sérgio Moro, fez o pedido com base em pareceres técnicos da PF e do DRCI. O Brasil deverá tomar as providências legais internas necessárias à adesão à Convenção, podendo, contudo, desde já, participar, como observador, das reuniões sobre a Convenção e seus protocolos. Uma vez signatário, o Brasil se unirá a grupo internacional que inclui países como Argentina, Austrália, Canadá, Chile, Costa Rica, Estados Unidos, Japão, Paraguai, República Dominicana e membros da União Europeia, entre outros. A iniciativa de adesão do Brasil à Convenção de Budapeste vem somar-se à Lei nº 12.965/2014, o Marco Civil da Internet, para a persecução penal dos crimes cibernéticos (GOVERNO, 2021).

O Pará instituiu a primeira Diretoria Estadual de combate a crimes cibernéticos (Deccc). A principal Diretoria da Polícia Civil do Pará tem como principal objetivo a prevenção e repressão de ações delituosas por meios tecnológicos (POLICIACIVIL, 2020).

Trata-se de iniciativa decorrente de trabalho de coordenação interinstitucional, constituído para esse fim, entre o Ministério das Relações Exteriores, a Polícia Federal (PF) e o Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional (DRCI){..}. O Brasil deverá tomar as providências legais internas necessárias à adesão à Convenção, podendo, contudo, desde já, participar, como observador, das reuniões sobre a Convenção e seus protocolos. A iniciativa de adesão do Brasil à Convenção de Budapeste vem somar-se à Lei nº 12.965/2014, o Marco Civil da Internet, para a persecução penal dos crimes cibernéticos (GOVERNO, 2021)

REFERÊNCIAS

BRASIL. Processo de adesão à Convenção de Budapeste - Nota Conjunta do Ministério das Relações Exteriores e do Ministério da Justiça e Segurança Pública. Disponível em <https://www.gov.br/mre/pt-br/canais_atendimento/imprensa/notas-a-imprensa/2019/processo-de-adesao-a-convencao-de-budapeste>. Acesso em: 21 de mar.2021

BRASIL. Processo de adesão à Convenção de Budapeste - Nota Conjunta do Ministério das Relações Exteriores e do Ministério da Justiça e Segurança Pública

Publicado em 11/12/2019 Atualizado em 07/01/2021. Disponível em <https://www.gov.br/mre/pt-br/canais_atendimento/imprensa/notas-a-imprensa/2019/processo-de-adesao-a-convencao-de-budapeste-nota-conjunta-do-ministerio-das-relacoes-exteriores-e-do-ministerio-da-justica-e-seguranca-publica> . Acesso em: 21 de mar.2021

Escritório Nações Unidas sobre Drogas e Crime (UNODC). Darknet Cybercrimes Threats to Southeast Asia. c2020. Disponível em <https://www.unodc.org/documents/southeastasiaandpacific//Publications/2021/Darknet_Cybercrime_Threats_to_Southeast_Asia_report.pdf>. Acesso em: 29 de mar. 2021

Escritório Nações Unidas sobre Drogas e Crime (UNODC). CYBERCRIMES. c2021. Disponível em <<https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html>>. Acesso em: 30 de mar.2021

FELIX, Diego. O Brasil é a quarta nação com maior tráfego online. Disponível em <<https://www.istoedinheiro.com.br/brasil-e-a-quarta-nacao-com-maior-trafego-online/>>. Acesso em: 08 de abr. 2021.

Organização Internacional de Polícia Criminal (INTERPOL). Covid-19 Cyberthreats. c2021. Disponível em <<https://www.interpol.int/Crimes/Cybercrime/COVID-19-cyberthreats>>. Acesso em: 23 de Mar. 2021

Organização Internacional de Polícia Criminal (INTERPOL). Cybercrimes. c2021. Disponível em <<https://www.interpol.int/Crimes/Cybercrime>>. Acesso em: 25 de mar. 2021

SOUZA. Cristian. Pará é o primeiro estado no país a instituir a Diretoria de Combate a Crimes Cibernéticos. POLÍCIA CIVIL, 2020. Disponível em: <<http://www.policiacivil.pa.gov.br/pará-é-o-primeiro-estado-no-pa%C3%ADs-instituir-diretoria-de-combate-crimes-cibernéticos>>.