IV CONGRESSO INTERNACIONAL DE DIREITO E INTELIGÊNCIA ARTIFICIAL (IV CIDIA)

ACADEMIA CYBER - OS RISCOS DA INTELIGÊNCIA ARTIFICIAL E OS PILARES FUNDAMENTAIS DO DIREITO

A168
Academia cyber - Os riscos da inteligência artificial e os pilares fundamentais do direito [Recurso eletrônico on-line] organização IV Congresso Internacional de Direito e Inteligência Artificial (IV CIDIA): Skema Business School – Belo Horizonte;

Coordenadores: Felipe Rodrigues Bomfim, Karina da Hora Farias e Priscila Céspede Cupello – Belo Horizonte: Skema Business School, 2023.

Inclui bibliografia
ISBN: 978-65-5648-796-0
Modo de acesso: www.conpedi.org.br em publicações
Tema: Os direitos dos novos negócios e a sustentabilidade.
1. Direito. 2. Inteligência artificial. 3. Tecnologia. I. IV Congresso Internacional de Direito e Inteligência Artificial (1:2023 : Belo Horizonte, MG).

CDU: 34

IV CONGRESSO INTERNACIONAL DE DIREITO E INTELIGÊNCIA ARTIFICIAL (IV CIDIA)

ACADEMIA CYBER - OS RISCOS DA INTELIGÊNCIA ARTIFICIAL E OS PILARES FUNDAMENTAIS DO DIREITO

Apresentação

O IV Congresso Internacional de Direito e Inteligência Artificial - CIDIA da SKEMA Business School Brasil, realizado nos dias 01 e 02 de junho de 2023 em formato híbrido, consolida-se como o maior evento científico de Direito e Tecnologia do Brasil. Estabeleceram-se recordes impressionantes, com duzentas e sessenta pesquisas elaboradas por trezentos e trinta e sete pesquisadores. Dezenove Estados brasileiros, além do Distrito Federal, estiveram representados, incluindo Amazonas, Bahia, Ceará, Distrito Federal, Espírito Santo, Goiás, Maranhão, Minas Gerais, Pará, Pernambuco, Paraná, Rio de Janeiro, Rio Grande do Norte, Rondônia, Roraima, Rio Grande do Sul, Santa Catarina, Sergipe, São Paulo e Tocantins.

A condução dos trinta e três grupos de trabalho do evento, que geraram uma coletânea de vinte e cinco livros apresentados à comunidade científica nacional e internacional, contou com a valiosa colaboração de sessenta e três professoras e professores universitários de todo o país. Esses livros são compostos pelos trabalhos que passaram pelo rigoroso processo de double blind peer review (avaliação cega por pares) dentro da plataforma CONPEDI. A coletânea contém o que há de mais recente e relevante em termos de discussão acadêmica sobre a relação entre inteligência artificial, tecnologia e temas como acesso à justiça, Direitos Humanos, proteção de dados, relações de trabalho, Administração Pública, meio ambiente, sustentabilidade, democracia e responsabilidade civil, entre outros temas relevantes.

Um sucesso desse porte não seria possível sem o apoio institucional de entidades como o CONPEDI - Conselho Nacional de Pesquisa e Pós-graduação em Direito; o Programa RECAJ-UFMG - Ensino, Pesquisa e Extensão em Acesso à Justiça e Solução de Conflitos da Faculdade de Direito da Universidade Federal de Minas Gerais; o Instituto Brasileiro de Estudos de Responsabilidade Civil - IBERC; a Comissão de Inteligência Artificial no Direito da Ordem dos Advogados do Brasil - Seção Minas Gerais; a Faculdade de Direito de Franca - Grupo de Pesquisa Políticas Públicas e Internet; a Universidade Federal Rural do Semi-Árido - UFERSA - Programa de Pós-graduação em Direito - Laboratório de Métodos Quantitativos em Direito; o Centro Universitário Santa Rita - UNIFASAR; e o Programa de Pós-Graduação em Prestação Jurisdicional e Direitos Humanos (PPGPJDH) - Universidade Federal do Tocantins (UFT) em parceria com a Escola Superior da Magistratura Tocantinense (ESMAT).

Painéis temáticos do congresso contaram com a presença de renomados especialistas do Direito nacional e internacional. A abertura foi realizada pelo Professor Dierle Nunes, que discorreu sobre o tema "Virada tecnológica no Direito: alguns impactos da inteligência artificial na compreensão e mudança no sistema jurídico". Os Professores Caio Lara e José Faleiros Júnior conduziram o debate. No encerramento do primeiro dia, o painel "Direito e tecnologias da sustentabilidade e da prevenção de desastres" teve como expositor o Deputado Federal Pedro Doshikazu Pianchão Aihara e como debatedora a Professora Maraluce Maria Custódio. Para encerrar o evento, o painel "Perspectivas jurídicas da Inteligência Artificial" contou com a participação dos Professores Mafalda Miranda Barbosa (Responsabilidade pela IA: modelos de solução) e José Luiz de Moura Faleiros Júnior ("Accountability" e sistemas de inteligência artificial).

Assim, a coletânea que agora é tornada pública possui um inegável valor científico. Seu objetivo é contribuir para a ciência jurídica e promover o aprofundamento da relação entre graduação e pós-graduação, seguindo as diretrizes oficiais da CAPES. Além disso, busca-se formar novos pesquisadores na área interdisciplinar entre o Direito e os diversos campos da tecnologia, especialmente o da ciência da informação, considerando a participação expressiva de estudantes de graduação nas atividades, com papel protagonista.

A SKEMA Business School é uma entidade francesa sem fins lucrativos, com uma estrutura multicampi em cinco países de diferentes continentes (França, EUA, China, Brasil e África do Sul) e três importantes acreditações internacionais (AMBA, EQUIS e AACSB), que demonstram sua dedicação à pesquisa de excelência no campo da economia do conhecimento. A SKEMA acredita, mais do que nunca, que um mundo digital requer uma abordagem transdisciplinar.

Expressamos nossos agradecimentos a todas as pesquisadoras e pesquisadores por sua inestimável contribuição e desejamos a todos uma leitura excelente e proveitosa!

Belo Horizonte-MG, 14 de julho de 2023.

Profª. Drª. Geneviève Daniele Lucienne Dutrait Poulingue

Reitora – SKEMA Business School - Campus Belo Horizonte

Prof. Dr. Caio Augusto Souza Lara

Coordenador de Pesquisa – SKEMA Law School for Business

O DIREITO INTERNACIONAL É (IN)EFICAZ QUANDO A CIBERCRIMINALISTICA É APLICADA NA PROTEÇÃO DOS DIREITOS FUNDAMENTAIS

INTERNATIONAL LAW IS (IN)EFFECTIVE WHEN CYBERCRIMINALISTIC IS APPLIED IN THE PROTECTION OF FUNDAMENTAL RIGHTS

Xenofontes Curvelo Piló [1]
Filipe Augusto Silva [2]
Deilton Ribeiro Brasil [3]

Resumo

O objetivo da investigação é analisar os crimes cibernéticos em relação aos Direitos Fundamentais, e o combate aos crimes por meio da cibercriminalistica. Adota-se o método descritivo e analítico e como procedimentos metodológicos a pesquisa bibliográfica. Como resultados alcançados verifica-se que há a necessidade da elaboração de leis e tratados para o combate de crimes cibernéticos, para o resguardo dos Direitos Fundamentais e das liberdades dos cidadãos contra atos ilícitos que têm a finalidade de prejudicar terceiros de boa-fé, o que se busca é a aplicação de uma justiça equitativa.

Palavras-chave: Direitos fundamentais, Cibercrimes, Cibercriminalística, Direito internacional, Novas tecnologias

Abstract/Resumen/Résumé

The objective of the paper is to analyze cyber crimes in relation to Fundamental Rights, and the fight against crimes through cybercriminalistics. The descriptive and analytical method is adopted and the bibliographical research as methodological procedures. As results achieved, it appears that there is a need to draft laws and treaties to combat cyber crimes, to safeguard the Fundamental Rights and freedoms of citizens against unlawful acts that have the purpose of harming third parties in good faith, the What is sought is the application of fair justice.

Keywords/Palabras-claves/Mots-clés: Fundamental rights, Cybercrimes, Cybercriminalistics, International law, New technologies

[1] Mestre e Doutorando do PPGD - Mestrado e Doutorado em Proteção dos Direitos Fundamentais da Universidade de Itaúna-MG.

[2] Mestre e Doutorando do PPGD - Mestrado e Doutorado em Proteção dos Direitos Fundamentais da Universidade de Itaúna-MG.

[3] Pós-Doutor em Direito pela UNIME, Itália. Doutor em Direito pela UGF-RJ. Professor da Graduação e PPGD da Universidade de Itaúna-UIT e Faculdades Santo Agostinho-FASASETE-AFYA. Orientador.

INTRODUÇÃO

Com a aproximação dos seres humanos por meio da globalização da economia, das comunicações e dos indivíduos como consequência acompanhada pelo aumento da criminalidade. Com a popularização da *internet* que impactou o mundo, nos anos de 1990, revolucionando conceitos, invadindo lares, empresas, industrias por fim uma invasão global em todos os lugares do mundo.

Os perigos advindos da conectividade surpreendentemente são desprezados. Um dos precedentes para o aumento da incidência do cibercrime foi a popularização da tecnologia e *internet* em todo o globo terrestre, também resultante da revolução tecnológica, facilitando ações criminosas dessa espécie, na medida em que se aumenta a quantidade de terminais conectados à rede de *internet*.

A imaterialidade fez com que novos negócios surgissem desde serviços exclusivamente virtuais, estratégias de atividade, produtos de uso em dispositivos como programas e jogos, além da dificuldade conceitual de determinação do local. Nasce então os crimes cibernéticos, como uma nova modalidade de crime que pode abalar a própria essência e concepção de personalidade dos indivíduos que são vítimas, notadamente, casos de vingança digital, também conhecidos como *revenge* ou cyberbullying, intimidação moral ou humilhação pública praticada via internet.

A *internet* possibilita que a criminalidade cibernética não possua quaisquer limites territoriais, como os demais crimes transnacionais, com a agravante da desnecessidade de deslocamento do criminoso para prática as condutas. Em síntese, uma pessoa pode praticar inúmeras condutas lesivas sem sair de sua residência, prejudicando, contudo, pessoas residentes do outro lado do planeta.

Marjie Britz, afirma que em 1997, um subgrupo do G8 voltado ao combate dos crimes de alta tecnologia, chamado *G8 subgroup on High-tech Crime*, criou uma rede denominada *24/7 High-tech Crime Point-of-Contact Network*, que visa a interligar policiais de diversos países, inclusive não membros do G8, com a finalidade de facilitar a interlocução e a assistência mútua para repressão ao cibercrime.

Por outro lado, havendo diversas violações aos direitos fundamentais pelos criminosos através do chamado cibercrime, a pergunta que não cala a comunidade internacional e nacional está preparada juridicamente para lidar com os mesmos através da utilização da cibercriminalistica nesta revolução tecnológica do século XXI?

Com a finalidade de responder à pergunta, o objetivo deste é verificar se há a necessidade de novos e efetivos mecanismos jurídicos e de cooperação jurídica mútua para fazer frente a esse novo formato de criminalidade. Com objetivos específicos, tem- se de identificar os mecanismos específicos para proteção contra violações praticadas no ciberespaço, considerando o sistema global de proteção aos direitos humanos. Para a pesquisa foi utilizado o método descritivo e analítico. O levantamento bibliográfico forneceu as bases teóricas necessárias para a elaboração adequada do trabalho, além dos conceitos de ordem dogmática que foram utilizados.

CRIMES CIBERNÉTICOS E OS DIREITOS FUNDAMENTAIS

Com a globalização e a divulgação da *Internet*, a ausência de limites nas fronteiras dos ciberespaços acomoda não apenas criações em prol da cidadania e da participação universal, mas facilitam que ocorram infrações comuns como os crimes contra o patrimônio e a honra, e os mesmo se moldem ao ciberespaço.

Sendo a internet utilizada, por pessoas inescrupulosas, como pratica de infrações penais vem levado desentendimentos pelo mundo, onde há questionamentos quanto a dificuldade de definir o tempo e o lugar de determinada conduta criminosa, principalmente pelo fato de tais infrações podem partir de lugares diversos do mundo, e a inexistência de fronteiras típica da web e podem envolver vários ordenamentos jurídicos de países distintos tornando complexa e dificultosa um efetivo combate das atividades criminosas no ciberespaço, bem como estabelecer qual o pais competente para processar, julgar e penalizar os infratores.

Atualmente, o Estado Democrático de Direito é adstrito pelos direitos fundamentais, que são "todas aquelas posições jurídicas concernentes às pessoas, que, do ponto de vista do direito constitucional positivo, foram, por seu conteúdo e importância, integradas ao texto da Constituição (SARLET, 2007)

Continua o autor, na seara dos direitos fundamentais existem quatro dimensões, na atual doutrina constitucional. A primeira geração refere-se às garantias e direitos fundamentais, assumindo "particular relevo no rol desses direitos, especialmente pela sua inspiração jusnaturalista, os direitos à vida, à liberdade, à propriedade e à igualdade perante a lei."

O que não se deve e não se pode violar, principalmente através de crimes virtuais,

são os direitos que correspondem a direitos garantidos à sociedade de forma individual ou coletiva, fundamentais à existência do indivíduo com pleno gozo do princípio da dignidade da pessoa humana.

O DIREITO INTERNACIONAL E O CIBERCRIME

Considera-se que a *internet* é utilizada como ferramenta de comunicação geral, servindo tanto para contatos pessoais privados como para negócios, sejam eles lícitos ou ilícitos, por mais que venhamos a preservar a privacidade dos usuários não se pode negar também o direito de segurança coletiva e a obediência as leis do pais onde se desenvolvesua atividade, desta feita os obstáculos gerados com o mau uso da internet poderiam ser evitados através de acordos de cooperação de permuta de dados entre países.

Spencer Sydow advoga que colisão de legislações de países diferentes, envolvidos, contudo, em uma rede comum mostrou a dificuldade para a investigação, apuração e punição de condutas ali perpetradas. Realidades sociais e jurídicas diversas, caminhando num mesmo trilho. Investigações policiais passaram cada vez mais misturar competências (SYDOW, 2022)

O autor ainda professa que ano após ano os meios de mídia especializada apresentam crescimento dos delitos praticados através da rede mundial de computadorese da tecnologia. A verdade é que a criação de um novo segmento da vida em sociedade exige dedicação de um novo ramo de estudo comportamental. A cibercriminologia estudao crime, o comportamento do cibercriminoso, as cibervitimas, as ciberleis e a ciber investigação. (SYDOW, 2022)

Fato é que a existência de um imenso universo a ser estudadop, explorado, debatido e redesenhado. Há uma infinidade de crimes cometidos utilizando-se da rede e que merecem a devida atenção. A rede, como a vida real, tem tendencias e momentos que, permitem a verificação de picos de criminalidade. Com toda essa incorporação social ao meio digital, os crimes praticados do mundo real não estariam apartados do mundo paralelo virtual, assim, a cada dia existe a ameaça ao indivíduo por meio do cibercrime. Seja através de furto de informações, seja de vendas de produtos ilegais, ou até mesmo de publicações com informações falsas prejudiciais.

Para Alesandro Barreto é importante ressaltar que os cibercrimes, tal qual os outros delitos graves, como tráfico internacional de drogas, de pessoas e o terrorismo, não são

alcançados pela competência do Tribunal Penal Internacional. Os crimes internacionais sob a égide do direito penal internacional, são limitados a genocídio, agressão, crimes de guerra e contra humanidade. Este diminuto escopo se dá pela fragilidade pela fragilidade do direito internacional em relação ao direito interno dospaíses. A independência das nações, conferida perla soberania, tona sinuosa a criminalização de condutas delitivas diante de diversos obstáculos decorrentes de interesses políticos, religiosos e econômicos (BARRETO, 2020).

No cenário internacional, a questão econômica é priorizada em relação o social e é atribuído uma posição de destaque às empresas e entes financeiros internacionais, com identidade de destaque nas relações de governo e de importância no processo globalizante. A internet não foi criada inicialmente com o objetivo a que se serve hoje. Inicialmente, conforme Diniz (2015), a rede mundial foi concebida com intuito acadêmico e militar, sendo que as forças armadas oficiais objetivavam comandar uma força nova de tecnologia com o fim de observação e captação de informações dos inimigos.

A seguridade nos meios eletrônicos, infelizmente, ainda é uma questão a ser avançada tecnologicamente, vez que, muitos são os avanços e também há muito a ser desenvolvido. Várias empresas da área de tecnologia da informação expandem e atualizam sistemas de segurança diuturnamente, pois os ataques contrários também são constantes e rápidos. Um dos enormes problemas da forma de consumo por meio da internet é precisamente a segurança nas transações, pois depreende-se do uso de dados pessoais, bancários, de cartões de crédito, etc.

O medo de utilização está na possibilidade de desvio de finalidade desses dados (MARQUES, 2013). De acordo com Marques (2013), a segurança sempre é motivo de preocupação do ser humano; afinal a proteção à vida é fundamental. No mundo digital a proteção é para os dados pessoais, já que ninguém quer ver seus dados usados de forma indevida ou ilícita. Na medida em que o mercado digital cresce, aumentam também as tentativas de burlar esse sistema. Assim, as empresas que estão em destaque no mundo digital são sempre alvos constantes de pessoas mal-intencionadas (hackers).

As tecnologias de segurança existentes são diariamente testadas e põem à prova a privacidade dos dados de usuários e empresas, mesmo que utilizados corretamente, dentro das indicações técnicas. A privacidade sobre as informações, como cartões de credito, contas bancárias e senhas devem ser protegidas com o uso correto da segurança e frequentemente modernizadas a fim de acompanhar o processo criminoso que circunda o mundo virtual, e disso depende o sucesso e expansão do comércio eletrônico. Tal vulnerabilidade existente na

rede faz com que as empresas do ramo tenham que investir cada vez mais nos sistemas de segurança, tornando-os mais eficazes em se tratando de proteção, com novos softwares.

Conforme dados da Interpol, há muitas organizações internacionais regionais, com finalidade de cobertura restrita ou ampla de estados e regiões, fazendo esforços paramanter a segurança cibernética e harmonizar o meio social virtual e seus deslindes com tais medidas internacionais para combater o cibercrime. Na região Ásia-Pacífico, a APECcontrola suas 21 economias membros para fim de promover a segurança cibernética com enfrentamento dos riscos trazidos pelo cibercrime. A APEC tem conduzido um projeto de capacitação sobre cibercrimes para os entes membros em relação a estruturas legais e investigativas, onde as economias mais avançadas da APEC apoiam outras economias- membros no treinamento de pessoal legislativo e investigativo (INTERPOL, 2012).

Destaca-se que a Convenção de Budapeste reconheceu em seus termos a conveniência de estender as salvaguardas para todos os direitos e liberdades fundamentais, pois que universais, e, especificamente o direito ao respeito pela privacidade, tendo em conta o crescente fluxo através das fronteiras dos dados pessoais sujeitos a tratamento informático, e a necessidade conciliar os valores fundamentais do respeito à privacidade e ao livre fluxo de informação entre os povos. A União Europeia tomou uma série de medidas para combater a cibercriminalidade, impulsionando política coordenada de aplicação da lei e de harmonização jurídica. A liberdade civil também temsido um foco no campo anti-cibercrime.

A Organização dos Estados Americanos (OEA), como outras organizações regionais, com 35 Estados membros, também está muito preocupada com a questão do cibercrime. Por meio de seu fórum para os Ministros da Justiça ou Procuradores-Gerais das Américas, a OEA reconhece há muito tempo o papel central que uma estrutura legal sólida desempenha no combate ao cibercrime e na proteção da internet.

A Convenção de Budapeste reconheceu em seus temos a conveniência de estender as salvaguardas para todos os direitos e liberdades fundamentais, pois que universais, e, em particular, o direito ao respeito pela privacidade, tendo em conta o crescente fluxo através das fronteiras dos dados pessoais sujeitos a tratamento informático, e a necessidade conciliar os valores fundamentais do respeito à privacidade e ao livre fluxo de informação entre os povos.

O fato é que o direito penal internacional tradicional tem por objetivo harmonizar o direito substantivo e coordenar o direito processual sobre as ofensas que existem na sociedade desde o surgimento da humanidade. Em razão da complexidade estrutural e universalidade da Internet, pelas frágeis leis que regulam o ciberespaço, pela ineficácia na

prática das leis internas de um país, somada a dificuldade de identificar e processar um criminoso que atingi diversas nações, os cibercriminosos atuam livremente certos da impunidade.

CONSIDERAÇÕES FINAIS

Há um imenso universo a ser estudado, explorado, debatido e redesenhado em relação ao cibercrime. É indiscutível que a rede seja mundial, mesmo havendo mistura indiscernível de usuários por toda a supervia, mesmo que o ambiente virtual gere uma sensação de universalidade e igualdade material e formal, nessa seara pode ocorrer crimes cibernéticos. Reportando a Pablos Molina, o mesmo advoga que para o estudo criminológico há três formas de prevenção de conflitos para qualquer espécie de infração penal, sendo a prevenção primária- implementação de medidas indiretas de prevenção-, a prevenção secundária- sobre grupos sociais propensos ao crime- e a prevenção terciaria- prevenir a reincidência voltada ao delinquente.

É fundamental um esforço global, com atuação em vários segmentos sociais, onde leis sejam bem elaboradas, homogêneas e atualizadas com as demandas advindas do ciberespaço e processos céleres que se amoldem à dinâmica dos cibercrimes são imprescindíveis para uma tutela eficaz. A sistemática de informações globalizadas acomoda um número crescente de ofensas transnacionais. A circunstancia da rede do cibercrime faz com que seja uma das ofensas mais globalizadas das ameaças atuais e mais modernizadas do futuro.

O cibercrime tem efeitos devastadores no mundo físico. O cenário é ainda mais complicado pela própria natureza do espaço cibernético manifestado no anonimato no espaço e no tempo, e a não atribuição de ações e ausência de fronteiras internacionais.

Pari e passo questões envolvendo a internet quando existe colisão entre o direito brasileiro e o direito internacional é necessário para a solução desses conflitos por meio de criação de regras advindas do Direito Internacional tanto por meio de tratados, acordos de colaboração internacional ou qualquer outro meio solução de controvérsias.

REFERÊNCIAS

BARRETO, Alesandro Gonçaves; KUFA, Karina; SILVA, Marcelo Mesquita. **Cibercrimes e seus reflexos no direito brasileiro**. Salvador: Juspodium, 2020.

BRITZ, Marjie T. **Computer forensics and cibercrime:** na introduction. New Jersey: Prntice Hall, 2009.

DINIZ, E. H.; FONSECA, C. E. C.; MEIRELLES, F. S. **Tecnologia bancária no Brasil:** uma história de conquistas, uma visão do futuro. São Paulo: FGV, 2015.

INTERPOL. **A Organização Internacional de Polícia Criminal**. Disponível em: https://www. interpol.int/News-andmedia/Publications2/Fact-sheets2. Acesso em: 27 mar. 2023.

MARQUES, Érico V. **Uma análise das novas formas de participação dos bancos no ambiente de negócios na era digital.** Relatório de Pesquisa. Centro de Excelência Bancária, EAESP-FGV, 2013.

PABLOS DE MOLINA, Antonio Garcia. **Criminologia**. 5. ed. Revista dos Tribunais,São Paulo, 2006.

SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais.** 8. ed. rev. atual. Porto Alegre: Livraria do Advogado, 2007.

SYDOW, Spencer Toth. **Direito Penal Informático**. 3. ed. Salvador: Ed. Juspodium,2022.