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

OS DIREITOS HUMANOS NA ERA TECNOLÓGICA II

JOÃO BATISTA MOREIRA PINTO

LUCAS GONÇALVES DA SILVA

LUCAS AUGUSTO TOMÉ KANNOA VIEIRA

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

Coordenadores: Lucas Gonçalves da Silva, Lucas Augusto Tomé Kannoa Vieira e João Batista Moreira Pinto – Belo Horizonte: Skema Business School, 2022.

Inclui bibliografia
ISBN: 978-65-5648-513-3
Modo de acesso: www.conpedi.org.br em publicações
Tema: A inteligência artificial e os desafios da inovação no poder judiciário.
1. Direitos humanos. 2. Inteligência artificial. 3. Tecnologia. I. III Congresso Internacional de Direito e Inteligência Artificial (1:2022 : Belo Horizonte, MG).

CDU: 34

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

OS DIREITOS HUMANOS NA ERA TECNOLÓGICA II

Apresentação

O Congresso Internacional de Direito e Inteligência Artificial (CIDIA) da SKEMA Business School Brasil, que ocorreu em formato híbrido do dia 08 ao dia 10 de junho de 2022, atingiu a maturidade em sua terceira edição. Os dezesseis livros científicos que ora são apresentados à comunidade científica nacional e internacional, que contêm os 206 relatórios de pesquisa aprovados, são fruto das discussões realizadas nos Grupos de Trabalho do evento. São cerca de 1.200 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, dentre outros temas.

Neste ano, de maneira inédita, professores, grupos de pesquisa e instituições de nível superior puderam propor novos grupos de trabalho. Foram recebidas as excelentes propostas do Professor Doutor Marco Antônio Sousa Alves, da Universidade Federal de Minas Gerais (SIGA-UFMG – Algoritmos, vigilância e desinformação), dos Professores Doutores Bruno Feigelson e Fernanda Telha Ferreira Maymone, da Universidade do Estado do Rio de Janeiro (Metalaw – A Web 3.0 e a transformação do Direito), e do Professor Doutor Valmir Cézar Pozzetti, ligado à Universidade Federal do Amazonas e Universidade do Estado do Amazonas (Biodireito e tutela da vida digna frente às novas tecnologias).

O CIDIA da SKEMA Business School Brasil é, pelo terceiro ano consecutivo, o maior congresso científico de Direito e Tecnologia do Brasil, tendo recebido trabalhos do Amazonas, Bahia, Ceará, Distrito Federal, Espírito Santo, Goiás, Maranhão, Minas Gerais, Mato Grosso do Sul, Mato Grosso, Pará, Pernambuco, Piauí, Paraná, Rio de Janeiro, Rio Grande do Norte, Rio Grande do Sul, Santa Catarina, Sergipe e São Paulo. Tamanho sucesso não seria possível sem os apoiadores institucionais do evento: o CONPEDI – Conselho Nacional de Pesquisa e Pós-graduação em Direito, o Instituto Brasileiro de Estudos de Responsabilidade Civil – IBERC e 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. Destaca-se, mais uma vez, a presença maciça de pesquisadores do Estado do Amazonas, especialmente os orientandos do Professor Doutor Valmir César Pozzetti.

Grandes nomes do Direito nacional e internacional estiveram presentes nos painéis temáticos do congresso. A abertura ficou a cargo do Prof. Dr. Felipe Calderón-Valencia (Univ. Medelín - Colômbia), com a palestra intitulada “Sistemas de Inteligência Artificial no Poder Judiciário - análise da experiência brasileira e colombiana”. Os Professores Valter Moura do Carmo e Rômulo Soares Valentini promoveram o debate. Um dos maiores civilistas do país, o Prof. Dr. Nelson Rosenvald, conduziu o segundo painel, sobre questões contemporâneas de Responsabilidade Civil e tecnologia. Tivemos as instigantes contribuições dos painelistas José Luiz de Moura Faleiros Júnior, Caitlin Mulholland e Manuel Ortiz Fernández (Espanha).

Momento marcante do congresso foi a participação do Ministro do Tribunal Superior do Trabalho – TST Maurício Godinho Delgado, escritor do mais prestigiado manual de Direito do Trabalho do país. Com a mediação da Profª. Drª. Adriana Goulart de Sena Orsini e participação do Prof. Dr. José Eduardo de Resende Chaves Júnior, parceiros habituais da SKEMA Brasil, foi debatido o tema “Desafios contemporâneos do gerenciamento algorítmico do trabalho”.

Encerrando a programação nacional dos painéis, o Prof. Dr. Caio Augusto Souza Lara, da SKEMA Brasil, dirigiu o de encerramento sobre inovação e Poder Judiciário. No primeiro momento, o juiz Rodrigo Martins Faria e a equipe da Unidade Avançada de Inovação do Tribunal de Justiça do Estado de Minas Gerais contaram sobre o processo de transformação em curso do Judiciário Estadual mineiro. Em seguida, o Prof. Dr. Fabrício Veiga Costa fez brilhante exposição sobre o projeto denominado “Processo Coletivo Eletrônico”, que teve a liderança do Desembargador Federal do Trabalho Vicente de Paula Maciel Júnior (TRT-3ª Região) e que foi o projeto vencedor do 18º Prêmio Innovare. O evento ainda teve um Grupo de Trabalho especial, o “Digital Sovereignty, how to depend less on Big tech?”, proposto pela Profª. Isabelle Bufflier (França) e o momento “Diálogo Brasil-França” com Prof. Frédéric Marty.

Os dezesseis Grupos de Trabalho contaram com a contribuição de 46 proeminentes 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, os quais eram compostos por pesquisadores que submeteram os seus resumos expandidos pelo processo denominado double blind peer review (dupla avaliação cega por pares) dentro da plataforma PublicaDireito, que é mantida pelo CONPEDI.

Desta forma, a coletânea que ora torna-se pública é de inegável valor científico. Pretende-se, com ela, contribuir com a ciência jurídica e fomentar o aprofundamento da relação entre a graduação e a pós-graduação, seguindo as diretrizes oficiais da CAPES. Promoveu-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 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. Foi lançada a nossa pós-graduação lato sensu em Direito e Tecnologia, com destacados professores e profissionais da área. No segundo semestre, teremos também o nosso primeiro processo seletivo para a graduação em Direito, que recebeu conceito 5 (nota máxima) na avaliação do Ministério da Educação - MEC. Nosso grupo de pesquisa, o Normative Experimentalism and Technology Law Lab – NEXT LAW LAB, também iniciará as suas atividades em breve.

Externamos os nossos agradecimentos a todas as pesquisadoras e a todos os pesquisadores pela inestimável contribuição e desejamos a todos uma ótima e proveitosa leitura!

Belo Horizonte-MG, 20 de junho de 2022.

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

A GUERRA CIBERNÉTICA DA UCRÂNIA: ABORDAGEM JURÍDICA CONTEMPORÂNEA DO DIREITO

THE CYBER WARFARE IN UKRAINE: A CONTEMPORARY LEGAL APPROACH TO LAW

Maria Eduarda Schuffner Barbosa [1]

Resumo

Esta pesquisa visa trabalhar o conceito de guerra cibernética e a sua aplicação no conflito internacional que acontece entre a Rússia e a Ucrânia no ano de 2022. A abordagem do texto tem como principal objetivo a exposição das formas de ataque do que pode vir a ser a mais nova modalidade de guerra, visto que o espaço cibernético está em ampla disseminação entre as culturas, tendo como um dos fins compreender como a situação apresentada afeta as populações no âmbito jurídico e social e estabelecer a interdependência do Direito Virtual e do Direito Internacional.

Palavras-chave: Direitos humanos, Direito internacional, Guerra cibernética, Rússia- ucrânia

Abstract/Resumen/Résumé

This research aims to work on the concept of cyber warfare and its application in the international conflict that takes place between Russia and Ukraine in the year 2022. The approach of the text has as the main objective the exposition of the forms of attack of what can become the newest modality of war, since the cybernetic space is in wide dissemination between cultures, having as the goals to understand how the presented situation affects the populations in the legal and social scope and establishing the interdependence of Virtual Law and International Law.

Keywords/Palabras-claves/Mots-clés: Human rights, International law, Cyber warfare, Russia-ukraine

[1] Graduanda em Direito, na modalidade Integral, na Escola Superior Dom Helder Câmara e graduanda em Relações Econômicas Internacionais na Universidade Federal de Minas Gerais.

1. CONSIDERAÇÕES INICIAIS

Essa pesquisa consiste na pretensão de entender o desenvolvimento da guerra que acontece entre a Rússia e a Ucrânia no contexto cibernético e a forma que ela infringe os direitos humanos. O desdobramento da problemática envolve o entendimento de que a globalização implica no maior acesso às redes sociais e às mídias, as quais facilitam que os hackers tenham como aumentar a disseminação de notícias falsas, espionagem e roubo de propriedades intelectuais como formas de ataque.

Da mesma forma, faz-se necessário aplicar esses fatos na área do direito, destacando que o direito digital passou por várias mudanças nos últimos tempos, já que a tecnologia evoluiu de uma forma que diversos tipos de infrações pudessem ser cometidas sem ter seus autores responsabilizados, já que esses podem estar em outros países, sendo necessária, na opinião de Pinheiro (2012, p. 125-126), a adoção de vários aspectos do direito internacional no direito virtual, na medida que a falta de limitações geográficas implica na forma de solucionar conflitos, sendo necessárias normas atemporais e interespaciais para que haja maior abrangência na aplicação das sanções.

Ademais, é necessário destacar que, para Liedekerke e Laudrain (2022), o pilar do próximo passo da Rússia no conflito cibernético consiste nos esforços da desinformação por meio da internet, sendo uma das poucos maneiras possíveis para infligir danos à Ucrânia sem o confronto direto, e, de acordo com ele, se o governo russo ficar sem opções, Putin recorrerá à espionagem, à interrupção de planos ocidentais, ao roubo de tecnologia e propriedades intelectuais como meio para contornar o isolamento econômico e social. Ademais, seriam feitos ataques como os que ocorreram à Ukrtelecom, uma grande empresa de telecomunicações ucraniana, atentados esses que aumentariam o temor dos ataques cibernéticos russos como meio para Putin alcançar seus objetivos, ferindo a segurança do Estado ucraniano e a soberania nacional.

A pesquisa que se propõe, na classificação de Gustin, Dias e Nicácio (2020), pertence à vertente metodológica jurídico-social. No tocante ao tipo genérico de pesquisa, foi escolhido o tipo jurídico-projetivo. O raciocínio desenvolvido na pesquisa foi predominantemente dialético e quanto ao gênero de pesquisa, foi adotada a pesquisa teórica.

2. COMO A GUERRA CIBERNÉTICA ACONTECE

Inicialmente, no intuito de entender como a guerra cibernética se desenvolve, é importante ressaltar Richard Alan Clarke, mestre em administração pelo Massachusetts Institute of Technology e especialista em segurança nacional, o qual, em sua obra ‘'Guerra Cibernética: A próxima ameaça à segurança e o que fazer respeito’’, trata sobre a forma de guerrear pela Internet, sendo tomado como referencial de abordagem a partir da sua afirmação que ressalta os prejuízos que podem ser causados:

> Em termos mais amplos, guerreiros cibernéticos podem invadir, controlar ou destruir essas redes. Se invadirem uma rede, os guerreiros cibernéticos podem roubar todas as suas informações ou mandar instruções para movimentar dinheiro, derramar petróleo, espalhar gás, explodir geradores, descarrilar trens, colidir aviões, enviar um pelotão para uma emboscada, ou fazer com que um míssil exploda no lugar errado. Caso os guerreiros cibernéticos destruam as redes, limpem os dados e transformem os computadores em suportes de porta, isso poderia fazer com que o sistema financeiro entrasse em colapso, ou uma cadeia de suprimentos parasse, ou um satélite pudesse ser colocado fora de órbita no espaço ou uma via aérea parasse. Isso não são hipóteses. Coisas assim já aconteceram, às vezes experimentalmente, às vezes por engano e às vezes como resultado de um crime cibernético ou de uma guerra cibernética. (CLARKE, 2015)

Dessa forma, as forças internacionais e países em guerra se deparam com um novo campo de batalha, que permite a criação de novas táticas, mais eficientes e difíceis de terem seus “soldados” rastreados: as mídias sociais e o espaço cibernético no geral. Ademais, fica explícita a competição para entender todas as ferramentas disponíveis na Internet, já que essas podem ser usadas nas estratégias dos ataques e das defesas nas guerras cibernéticas, sendo necessário destacar que, para Murakiev (2019), é explícito como o espaço cibernético tem sido visto como uma competição de disputa de poder, tendo como vencedor aquele que possui as melhores táticas, meios e ferramentas para conseguir acabar com o seu oponente com o máximo de danos possíveis. Outrossim, é possível introduzir o medo no ciberespaço, podendo chegar ao nível de temor que pode paralisar uma nação, podendo destruir ou fazer dano a coisas físicas, já que não tem regras quando se trata das condutas de combate da ciberguerra.

Nesse sentido, é importante destacar que, segundo Igreja (2022), “Antes mesmo da invasão física os ciberataques contra determinados sistemas ucranianos já estavam acontecendo. E grupos como o Anonymous já realizaram um contra-ataque tirando, inclusive, o site da agência de notícias estatal russa do ar.”. Do mesmo jeito, Suzuki (2022) ainda comenta outros ataques cibernéticos cometidos contra a Ucrânia, “Outra investida foi o envio em massa de mensagens SMS aos celulares da população ucraniana dizendo que todos os caixas eletrônicos no país estavam inoperantes para saque - uma informação falsa.”, ficando notório

que esses ataques cibernéticos podem ser usados como armas para a desinformação dos alvos, desativando sistemas de informações de locais em risco e onde se proteger, o que pode culminar na morte de civis inocentes, ferindo até mesmo a Declaração Universal dos Direitos Humanos, feita pela Organização das Nações Unidas (1948), a qual dita que "todo ser humano tem direito à vida, à liberdade e à segurança pessoal", ficando em evidência a urgência de se tratar do assunto o mais rápido possível. Concluindo em concordância com Igreja, “O ponto de partida é o reconhecimento de que essa pauta vai ficar cada vez mais importante e temos que estar preparados”.

A realidade apresentada pode servir de alerta para que seja percebido que a população está à mercê de diversos ataques no dia a dia, já que qualquer um que usa a internet está expondo seus dados para grandes empresas por meio da autorização do uso de dados pessoais e operacionais nos aplicativos, como é exposto por Fonseca (2018, apud LARA, 2019, p. 102). Dados esses que deveriam ser privados, mas podem ser usados pelos governos e instituições que tiveram à essas informações o privilégio da utilização, porém essas bases de dados também podem ser vazadas para hackers, situação que acontece globalmente, mas terá como protagonista do cenário internacional atual os ucranianos, já que até os sites oficiais do governo ucraniano foram invadidos.

3. O DIREITO VIRTUAL E A ABORDAGEM JURÍDICA CONTEMPORÂNEA

A princípio é importante que o direito virtual ainda não tem um código de normas que envolva todos os possíveis crimes cibernéticos e suas devidas punições, até por ser possível que uma pessoa cometa uma infração enquanto está em outro país, sendo necessária a estipulação de um código abrangente e internacional, para que, dessa forma, haja a condenação legal de criminosos virtuais, incluindo hackers que atentam contra governos, populações e indivíduos. Nessa direção, é primordial salientar Bobbio (2004, p. 47-48), o qual expõe no seu livro que “Kant via no direito cosmopolita não “uma representação fantástica de mentes exaltadas”, mas uma das condições necessárias para a busca da paz perpétua, numa época da história em que “a violação do direito ocorrida num ponto da terra é sentida em todos os outros”.”, citação na qual é destacado o efeito dominó que ocorre nos conflitos internacionais.

Dessa forma, fica explícito como o âmbito internacional e digital estão interligados, sendo importante citar Patrícia Peck Pinheiro, advogada especialista em Direito Digital , Propriedade Intelectual, Proteção de Dados e Cibersegurança, Graduada e Doutorada pela Universidade de São Paulo e PhD em Direito internacional discorre sobre a ligação entre o

Direito Internacional e Direito Digital em seu livro ‘’Direito Digital’’, sendo tomada como referência nesse quesito ao afirmar que

> Há uma integração entre o Direito Digital e o Direito Internacional Privado na medida em que este último é justamente constituído por regras colisionais que visam solucionar conflitos entre normas atemporais e interespaciais, pois tem como objetivo a ciência dos conflitos (Conflicts of Law). Isto porque o Direito Digital rotineiramente tem que enfrentar problemas relacionados a qual lei aplicar em um caso concreto que ocorre na Internet, qual é o Tribunal competente, como garantir a efetividade, qual o local mais relevante para a produção dos efeitos, vínculos jurídicos, onde se estabelecem os laços fáticos? Pode-se afirmar que a sociedade atual passou a exigir um Direito com características de translational law através do ciberespaço, para que ele tenha efetividade. (PINHEIRO, 2012)

Dessa maneira, fica explícita a semelhança e interdependência entre o Direito Virtual e o Direito Internacional, o qual pode ser tomado como base para a formação da jurisprudência que abordará o ciberespaço.

4. CONSIDERAÇÕES FINAIS

A partir do exposto, verifica-se que a guerra cibernética será amplamente usada, e, provavelmente, evoluirá de uma forma que é necessário que a Organização da Nações Unidas esteja preparada para lidar com esse tipo de crime de guerra, de forma que o Estatuto do Tribunal Penal Internacional atue diretamente na prevenção e na responsabilização dos indivíduos envolvidos nos ataques cibernéticos, dos quais alguns podem ser considerados crimes de guerra. Além disso, é necessária uma medida que estimule a adesão de outros países que ainda não acolheram a legitimidade desse tipo de tratado internacional.

Em contraponto, também é notório como a sociedade, no geral, permite o acesso de vários aplicativos e sites aos seus dados por meio da aceitação dos termos de serviço, sem ao menos ler uma parte, apenas querendo ter acesso à algum tipo de conteúdo, ficando explícito a necessidade da conscientização da importância de ler o que se autoriza na internet, por ser um contrato de uso. Diante disso, é necessário destacar que ao mesmo tempo que uma pessoa pode estar dando suas informações “apenas’’ para escolha mais específica de conteúdos e anúncios, também pode estar fornecendo para uma base de dados suscetíveis aos ataques de hackers ou do uso impróprio de governos.

Portanto, entende-se que deve haver uma ação que previna maiores prejuízos à sociedade como um todo no âmbito cibernético, não só nas guerras cibernéticas, mas nos ataques que ocorrem no dia a dia, sendo necessária a criação de normas específicas para o Direito Virtual, as quais devem ter interligação com o Direito Internacional e aprovação dos países membros da ONU.

REFERÊNCIAS BIBLIOGRÁFICAS

BOBBIO, Norberto. **A Era dos Direitos.** Nova ed. Rio de Janeiro: Elsevier, 2004. p. 42-43.

CLARKE, Richard; KNAKE, Robert. **Guerra Cibernética: A próxima ameaça à segurança e o que fazer a respeito**. Tradução do livro "Cyber War: the next threat to national security and what to do about it". Rio de Janeiro: Brasport Livros, 2015.

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

IGREJA, Arthur. Rússia versus Ucrânia: O que é uma guerra cibernética e como pode afetar o Brasil?. Entrevista concedida a Bruno Pavan. **ISTOÉ Dinheiro**. Disponível em: https://www.istoedinheiro.com.br/russia-versus-ucrania-o-que-e-uma-guerra-cibernetica-e-como-pode-afetar-o-brasil/. Acesso em 17 abr. 2022.

LARA, Caio Augusto Souza. **O acesso tecnológico à justiça: por um uso contra-hegêmonico do Big Data e dos algoritmos**. 191 f. Tese de Doutorado- Programa de Pós-graduação em Direito. Universidade Federal de Minas Gerais, Belo Horizonte, 2019.

LIEDEKERKE, Arthur; LAUDRAIN, Arthur. Russia's Cyber War: What's Next and What the European Union Should Do. **Council on Foreign Relations**. Disponível em: https://www.cfr.org/blog/russias-cyber-war-whats-next-and-what-european-union-should-do. Acesso em 17 abr. 2022.

MURAKIEV, Alexey. **What is Cyber Warfare? | Ask an Expert**. Youtube, 10 dez. 2019. Disponível em: https://www.youtube.com/watch?v=5HHbU0tHVQQ. Acesso em 17 abr. 2022.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Declaração Universal dos Direitos Humanos**, 1948. Disponível em: https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos. Acesso em: 17 abr. 2022.

PINHEIRO, Patrícia. **Direito Digital**. 6 ed. São Paulo: Saraiva, 2016. p. 125-127.

SUZUKI, Shin. A guerra cibernética paralela entre Rússia e Ucrânia. **BBC NEWS**. Disponível em: https://www.bbc.com/portuguese/internacional-60551648. Acesso em 17 abr. 2022.