

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

**DIREITO PENAL E CIBERCRIMES II**

**FERNANDO HENRIQUE DA SILVA HORITA**

**WILSON DE FREITAS MONTEIRO**

**AMANDA RODRIGUES ALVES**

---

D598

Direito penal e cibercrimes II [Recurso eletrônico on-line] organização III Congresso Internacional de Direito e Inteligência Artificial (III CIDIA): Skema Business School – Belo Horizonte;

Coordenadores: Fernando Henrique da Silva Horita, Amanda Rodrigues Alves e Wilson de Freitas Monteiro – Belo Horizonte: Skema Business School, 2022.

Inclui bibliografia

ISBN: 978-65-5648-519-5

Modo de acesso: [www.conpedi.org.br](http://www.conpedi.org.br) em publicações

Tema: A inteligência artificial e os desafios da inovação no poder judiciário.

1. Direito penal. 2. Cibercrimes. 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)

## DIREITO PENAL E CIBERCRIMES 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 César 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. Medellín - 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 Prof<sup>a</sup>. Dr<sup>a</sup>. 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-3<sup>a</sup> Região) e que foi o projeto vencedor do 18<sup>o</sup> Prêmio Innovare. O evento ainda teve um Grupo de Trabalho especial, o “Digital Sovereignty, how to depend less on Big tech?”, proposto pela Prof<sup>a</sup>. 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 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. 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.

Prof<sup>a</sup>. Dr<sup>a</sup>. 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

## **CIBERGUERRA ENTRE RÚSSIA-UCRÂNIA: OS IMPACTOS CAUSADOS E A VISÃO DO DIREITO INTERNACIONAL**

## **CYBERGUERRA TRA RUSSIA-UCRAINA: GLI IMPATTI CAUSATI E LA VISIONE DEL DIRITTO INTERNAZIONALE**

**Camila Maciel Neves Gentilini**

### **Resumo**

Esta pesquisa consiste em demonstrar os impactos da Ciberguerra e a visão do direito internacional em relação ao caso da Rússia-Ucrânia. Neste caso, utilizar-se-á a vertente metodológica jurídico-sociológica, técnica da pesquisa teórica, no tocante ao tipo de investigação, o jurídico-projetivo, e raciocínio predominantemente dialético. Então, conclui-se preliminarmente que a soberania será afetada por conta da Ciberguerra, ocorrida entre Rússia-Ucrânia, visto que houve ataques a sites governamentais. Quanto a ONU, uma organização ligada ao direito internacional, a expectativa é de repúdio aos ciberataques por esta ter como objetivo resguardar boas relações entre as nações.

**Palavras-chave:** Guerra cibernética, Rússia-ucránia

### **Abstract/Resumen/Résumé**

Questa ricerca propone la dimostrazione degli impatti di una Cyberguerra e la visione del diritto internazionale in relazione al caso di Russia-Ucraina. Nel caso, sarà utilizzata una vertente metodologica giuridica-sociologica, tecnica della ricerca teorica, nel toccante al tipo d'investigazione, il giuridico-proiettivo, e raziocinio predominante dialettico. Comunque, si conclude preliminarmente che la sovranità verrà affettata per la Cyberguerra avvenuta tra Russia-Ucraina, visto gli attacchi verificati a siti governativi. Quanto l' ONU, una organizzazione legata al diritto internazionale, la aspettativa e quella di ripudio ai ciberattachi perché ha come obiettivo il risguardo alle buone relazioni tra nazioni.

**Keywords/Palabras-claves/Mots-clés:** Cyberguerra, Russia-ucraina

## **1. CONSIDERAÇÕES INICIAIS**

A presente pesquisa tem como objetivo geral a análise do impacto da Ciberguerra no caso da Rússia-Ucrânia trazendo a visão do direito internacional em relação ao ocorrido. Com especificidade, essa reporta definições de acordo com autores do que seria uma Guerra Cibernética e Ciberespaço, documenta o ocorrido trazendo as consequências, além, de investigar a relação do tema com a questão da soberania.

No mundo atual em que vivemos, a cada dia mais a tecnologia acaba por adentrar em nossa sociedade em diferentes aspectos, seja na área militar, política, economia, dentre outras. Chegamos a um ponto em que nos encontramos todos - pessoas, empresas, países - interconectados por conta da tecnologia. Entretanto, a mesma pode acabar por trazer consequências negativas, que não havíamos pensado quando decidimos criá-las. Um exemplo a ser considerado é aquilo que mais se tem ouvido falar neste ano de 2022: a Ciberguerra ou Guerra Cibernética entre a Rússia e Ucrânia.

Este novo tipo de guerra, assim como qualquer outra guerra, acaba por trazer impactos na economia, na sociedade e na política, como se tem visto no atual conflito. Além, de que esta nova forma de guerra, não só poderá produzir impactos localizados, como se tem a possibilidade de impactar outros países, demonstrando a importância de se debater sobre o tema.

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. CIBERGUERRA ENTRE RÚSSIA E UCRÂNIA**

O tema abordado acaba por trazer diversas discussões na atualidade, assim, como a definição de Guerra Cibernética, Segundo Mehan:

A Ciberguerra, portanto, infere tanto o conflito relacionado à informação a nível nacional, militar, bem como atividades de conflito de baixa intensidade pretendidas para infligir níveis limitados de dano (MEHAN,2014).

Já para Clarke e Knake, as “ações de um Estado Nação para penetrar nos computadores ou redes de outra nação para o propósito de causar danos ou perturbações”. (CLARKE; KNAKE, 2010). As duas definições acabam por apresentar ponto em comum, em que a Ciberguerra seria algo realizado para não causar algum dano físico, porém isso não significa que esta não cause danos econômicos, políticos ou sociais. (VITORINO, 2021).

Jorge apresentou uma assertiva qual seria a sua concepção de ciberguerra, essa se vem presente no artigo “Das ‘Guerras Cibernéticas’”. Segundo o autor:

A “guerra cibernética” é um novo, mas não inteiramente separado, componente de um ambiente de conflito multifacetado. Ela desafia a visão tradicional do Estado como o principal ator no sistema internacional e a sua influência decisiva na guerra. O espaço cibernético dá um poder desproporcional a atores pequenos e relativamente insignificantes. Neste sentido, a “guerra cibernética” presta-se especialmente bem a organizações mais extremistas, que podem atacar o coração ou a infra-estrutura de uma sociedade a partir de uma posição remota e de um endereço não identificável (JORGE, 2012).

Através dessa fala proposta pelo autor pode-se dizer que a guerra cibernética é algo novo e deve ser considerado como parte de um ambiente de conflito. Este novo ambiente irá desafiar a visão tradicional de Estado, pois esta pode acabar por fornecer poder a atores pequenos e insignificantes. Ele sustenta que a guerra cibernética é algo que se pode acabar por ajudar organizações mais extremistas, onde podem atacar a infraestrutura de uma sociedade sem mesmo se encontrar perto desta. Além disso, é possível não haver nenhuma ligação ou rastro a esses ataques realizados. Logo podemos perceber com este raciocínio foi exatamente a situação ocorrida entre a Rússia e Ucrânia.

Compreendida a definição, há de levantar quais seriam as motivações e razões para que esse tipo de guerra aconteça. Existem diversas motivações para essa acontecer, mas a maioria acaba por visar a obtenção de uma vantagem em conflitos físicos. Entretanto, essa pode instaurar o medo na nação fazendo com que haja uma pressão no governo para que se concluir o conflito. Por fim, há a possibilidade dessa ocorrer visando atrapalhar ou até mesmo tornar inviável algum projeto em processo de desenvolvimento.(BRANCO, 2022).

Em certo momento, se podia dizer que a tensão entre a Ucrânia e Rússia era uma Guerra Cibernética, já que não havia algum dano físico, mas se havia ‘hackers’ sobrecarregando a capacidade da página de ‘websites’ ligados a funções militares e bancarias de modo que estas permaneçam indisponíveis ao usuário. Um dos ataques foi ligado a ‘hackers’ armadores que se identificam como “patriotas russos”. (SUZUKI, 2022).

Essa vem sendo apontada como um novo tipo de guerra que há como palco o ciberespaço, que segundo Levy, seria um “espaço de comunicação aberto pela interconexão mundial dos computadores e das memórias dos computadores”. (LÉVY,1999). Com o início dessas questões de Ciberguerra e ataques cibernéticos, estes acabaram por trazer uma nova percepção de que as guerras podem ocorrer a partir de um ciberespaço e não mais só em arenas tradicionais como o mar, à terra, o ar ou espaços cósmicos, isto é algo perceptível na tensão entre a Rússia e Ucrânia. (JORGE, 2012).



Contudo, vale ressaltar que contrariamente ao mar, terra, ar e o espaço cósmico não é possível falar sobre de domínio no espaço cibernético. Os sistemas cibernéticos complexos são dependentes para o apoio de atividades militares e econômicas o que acaba por trazer vulnerabilidades novas a grandes Estados, que podem ser explorados por atores não estatais e/ou pequenos Estados. (JORGE, 2012).

### **3. A VISÃO E O IMPACTO DO DIREITO INTERNACIONAL**

No artigo “Wired warfare: Computer network attack and jus in bello” escrito por Schmitt, vem defendido que os princípios estabelecidos pelo Direito Internacional Humanitário (DIH) são aplicáveis quando há um ataque cibernético realizado por um Estado, de forma consciente e haja o propósito de causar morte, ferimento, destruição, mesmo que não haja uma força armada. A visão se mostra coerente já que qualquer aplicação de força realizada por um Estado, em seu uso legal, deverá seguir os princípios do Direito Internacional Humanitário (DIH).

Como relatado anteriormente, uma guerra cibernética pode ter como objetivo uma preparação para se realizar a guerra em ambiente físico. Levantado esse ponto pode-se dizer que as guerras cibernéticas também devem respeitar o Direito Internacional Humanitário (DIH) e participarem do tratado do jus ad bellum, pois essa poderá transgredir à proibição do uso da força.

Jus ad Bellum são dois conceitos apresentados na Carta das Nações Unidas e acabam por não abordar a questão da Ciberguerra. Neles se vem abordado a questão do uso da força e ataques armados. (NUNES,2015). O primeiro conceito vem abordado no inciso 4 do artigo 2 da Carta das Nações Unidas:

Todos os Membros deverão evitar em suas relações internacionais a ameaça ou o uso da força contra a integridade territorial ou a independência política de qualquer Estado, ou qualquer outra ação incompatível com os Propósitos das Nações Unidas (NAÇÕES UNIDAS, 1945).

Já o segundo conceito vem abordado no artigo 51:

Nada na presente Carta prejudicará o direito inerente de legítima defesa individual ou coletiva no caso de ocorrer um ataque armado contra um Membro das Nações Unidas, até que o Conselho de Segurança tenha tomado as medidas necessárias para a manutenção da paz e da segurança internacionais. As medidas tomadas pelos Membros no exercício desse direito de legítima defesa serão comunicadas imediatamente ao Conselho de Segurança e não deverão, de modo algum, atingir a autoridade e a responsabilidade que a presente Carta atribui ao Conselho para levar a efeito, em qualquer tempo, a ação que julgar necessária à manutenção ou ao

restabelecimento da paz e da segurança internacionais (NAÇÕES UNIDAS, 1945).

Os ataques cibernéticos realizados por Estados, assim como está ocorrendo entre Rússia-Ucrânia, excedem as noções jurídicas tradicionais sobre o uso da força. Lembrando que esta Carta foi redigida em um período, onde os Estados infligiam danos físicos, porém, agora são novos tempos onde essas guerras estão abrangendo um novo espaço: o mundo virtual. (NUNES,2015). O Direito é algo dinâmico, que deve acompanhar a sociedade, já que nos encontramos em uma nova era aonde ocorrem ataques cibernéticos. Será que estes dois conceitos constatados na Carta das Nações Unidas não deveria ser melhorado, de modo a evitar um desenvolvimento de uma guerra cibernética como está ocorrendo entre a Rússia e Ucrânia?

Outro ponto a ser levantado é a preocupação trazida em relação à questão da soberania, é a ocorrência de ataques às infraestruturas primordiais do Estado. Os ataques realizados a estas estruturas são prejudiciais, porque afetam à segurança, economia e saúde pública, além de ser possível a obtenção de vantagens políticas e econômicas. (VITORINO, 2021).

Em 2018, o secretário-geral da ONU, Antônio Guterres alertava sobre Ciberguerras. Este defendia que deveriam ser criadas regras globais visando diminuir o impacto das Guerras Cibernéticas sobre os civis. (DEL BARRIO, 2018). Algo que vale a pena ser comentado é a existência de um documento acadêmico chamado Manual de Tallinn de 2013, que trata sobre a aplicabilidade da lei internacional na resolução de Ciberconflitos, podendo contribuir para a criação de novas leis por parte da ONU e outras organizações internacionais.

#### **4. CONSIDERAÇÕES FINAIS**

Ante o exposto, verifica-se que a análise feita do caso entre a Rússia e Ucrânia, sob o ponto de vista da Ciberguerra, pode-se concluir que eram esperadas medidas por parte do Direito para gerar novas normativas em respeito ao assunto tratado, além do acréscimo deste tipo de guerra na fonte do jus ad bellum, de modo a não evidenciar impunidades. Este fato acaba por se tornar importante e urgente não só por uma carência de leis em relação a esse tema, mas também por haver diversas interpretações sobre o assunto discutido.

As determinações da ONU (Organização das Nações Unidas) podem ser questionadas quando levada em consideração a questão da guerra cibernética, já que essa proporciona um desrespeito aos objetivos impostos pela mesma.

Logo, como o assunto é novo há pouca referencia e discussão em relação à Ciberguerra. Portanto, seria interessante que se houvesse uma ampliação dessas discussões em outras esferas.

## REFERÊNCIAS BIBLIOGRAFICAS

BRANCO, Dácio C.; **O que é uma guerra cibernética?**. Canal Tech, 01 mar. 2022. Disponível em: O que é uma guerra cibernética? - Canaltech. Acesso em: 23/05/2022.

CLARKE, Richard A.; KNAKE, Robert K.; **Cyber War: the next threat to national security and what to do about it**. HarperCollins Publishers Ltd., London, 2010.

DEL BARRIO, Javier M.; **Secretário-geral da ONU alerta que já há “ciberguerra entre Estados”**. El país, Lisboa, 20 fev. 2018. Disponível em: Secretário-geral da ONU alerta que já há “ciberguerra entre Estados” | Internacional | EL PAÍS Brasil (elpais.com). Acesso em: 30 abr. 2022.

JORGE, Bernardo W. G.De A.; **Das “Guerras Cibernéticas”**, Rio de Janeiro.24 maio.2012. Disponível em: (9) Das "Guerras Cibernéticas" | Bernardo Wahl - Academia.edu. Acesso em: 29 abr. 2022.

LÉVY, Pierre; **Cibercultura**. Editora 34, São Paulo, 1999.

MEHAN, Julie E., **Cyberwar, Cyberterror, Cybercrime and Cyberactivism: An in-depth guide to the role of security standards in the cybersecurity environment**. IT Governance Publishing, Cambridgeshire, 2014.

NAÇÕES UNIDAS. **Carta das Nações Unidas**. São Francisco, EUA, 1945. Disponível em: D19841 (planalto.gov.br). Acesso em: 1 maio. 2022.

NUNES, Luiz A. R.; **Guerra Cibernética E O Direito Internacional: Aplicabilidade Do Jus Ad Bellum E Do Jus In Bello**. Rio de Janeiro, 2015. Disponível em: Luiz Artur RODRIGUES Nunes.pdf (esg.br). Acesso em: 1 maio. 2022.

SCHMITT, Michael N.; **Wired warfare: computer network attack and jus in bello**. International Review of the Red Cross, Suíça, 2012. Disponível em: Wired warfare: Computer network attack and jus in bello (icrc.org). Acesso em: 23 maio. 2022.

SUZUKI, Shin. **A guerra cibernética paralela entre Rússia e Ucrânia**. BBC News Brasil, São Paulo, 1 de mar. 2022. Disponível em: A guerra cibernética paralela entre Rússia e Ucrânia - BBC News Brasil. Acesso em: 30 abr. 2022.

VITORINO, Luã G.; **Direito Internacional E Ciberguerra: Ataques Cibernéticos Entre Nações, Manual De Tallinn, Por Que É Mais Fácil Regular Uma Ciberguerra Do Que Regular Uma Cibersegurança?**. Goiás, 2021. Disponível em: \*TCCG - Direito - Luã Gonçalves Vitorino - 2021.pdf (ufg.br). Acesso em: 1 maio. 2022.

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.