CIBERTERRORISMO E DIREITO PENAL INTERNACIONAL: DESAFIOS DA COOPERAÇÃO ENTRE PAÍSES NO COMBATE AO USO DA TECNOLOGIA PARA FINS TERRORISTAS

Autor(res)

Rafaela Benta De Almeida
Alysson Felipe De Oliveira Celestino

Categoria do Trabalho

Trabalho Acadêmico

Instituição

FACULDADE ANHANGUERA DE BRASÍLIA

Introdução

A transformação digital, embora traga avanços significativos, também gerou novos desafios no campo da segurança pública e do Direito Penal. Dentre os problemas emergentes, destaca-se o ciberterrorismo, que se caracteriza pelo uso da internet e de recursos tecnológicos para realizar atos de violência motivados por ideologias políticas, religiosas ou sociais.
O impacto de ataques cibernéticos a infraestruturas críticas, como redes de energia, sistemas financeiros e órgãos governamentais, evidencia a gravidade da ameaça. A natureza transnacional desses crimes torna a atuação estatal isolada insuficiente, exigindo a cooperação entre países. Entretanto, a falta de padronização legislativa e a relutância no compartilhamento de informações comprometem a eficácia do combate ao ciberterrorismo, revelando a necessidade de estratégias conjuntas e coordenada entre os entes internacionais.

Objetivo

O objetivo principal deste trabalho é analisar os desafios da cooperação internacional no combate ao ciberterrorismo. De forma específica, este trabalho busca, identificar os principais obstáculos jurídicos e diplomáticos que comprometem a cooperação internacional entre os estados, analisar as principais convenções e tratados internacionais sobre crimes cibernéticos, destacando suas limitações, e encontrar soluções para o aprimoramento da cooperação jurídica e técnica entre os países no combate ao ciberterrorismo.

Material e Métodos

O trabalho utiliza uma abordagem qualitativa, fundamentada na revisão bibliográfica e na análise de doutrinas. Foram consultados documentos normativos internacionais, como a Convenção de Budapeste (2001) e relatórios da ONU sobre segurança cibernética. Além disso, foram analisados estudos acadêmicos publicados entre 2018 e 2024, que discutem a cooperação jurídica no combate a crimes digitais. A metodologia abrange a comparação entre legislações nacionais e tratados internacionais, destacando as lacunas jurídicas e os obstáculos para a colaboração entre estados estrangeiros no combate aos cibercrimes.

Resultados e Discussão

Os resultados indicam que a falta de harmonização legislativa é um dos principais entraves à cooperação internacional no combate ao ciberterrorismo, eis que não há a existência de legislação comum ou poder coercitivo único nesse campo. A Convenção de Budapeste, embora relevante, aborda crimes cibernéticos de forma genérica, sem firmar um entendimento robusto sobre atos terroristas digitais. Assim, os países que aderiram a esta convenção enfrentam dificuldades para enquadrar ataques de motivação política como ciberterrorismo.

Outro aspecto relevante é a resistência ao compartilhamento de dados sensíveis entre países, especialmente devido à proteção de dados pessoais prevista por normas como o GDPR europeu. Essa situação é agravada quando os ataques envolvem possíveis ligações com governos, configurando casos de ciberterrorismo patrocinado pelo Estado, o que gera impasses diplomáticos.

Um exemplo emblemático foi a Operação Dark Web, na qual a ausência de um consenso internacional sobre a troca de provas digitais comprometeu a efetividade das ações judiciais. O estudo conclui que, para enfrentar essas barreiras, é fundamental criar um tratado internacional específico sobre ciberterrorismo, com diretrizes claras sobre a coleta, preservação e compartilhamento de provas digitais, além de estabelecer mecanismos de cooperação ágeis e seguros.

Além disso, a criação de um Tribunal Penal Internacional Digital é proposta para julgar ataques cibernéticos de grande impacto que podem abalar a ordem internacional, sendo este tribunal uma forma de coordenar esforços entre países, garantindo que os responsáveis por ações terroristas digitais sejam efetivamente processados, independentemente da jurisdição de origem.

Conclusão

Conclui-se que o ciberterrorismo representa um risco significativo para a segurança global, demandando respostas coordenadas entre os países. A ausência de um tratado internacional específico e a falta de uniformidade na legislação cibernética dificultam o combate a esses crimes. Para superar esses obstáculos, é essencial promover a criação de mecanismos jurídicos que fortaleçam a cooperação internacional e garantam maior eficiência na identificação e responsabilização dos autores de ataques cibernéticos com motivações terroristas.

Referências

Bezerra, Clayton da Silva/Agnoletto, Giovani Celso
Combate ao Crime Cibernético / Clayton da Silva Bezerra
1.ed.- Rio de Janeiro; Mallet Editora, 2020. 269p.; 16 x 23 cm. (Doutrina e Prática – A visão do delegado de polícia 3).

BARRETO, Alessandro Gonçalves; BRASIL, Beatriz Silveira. Manual de investigação cibernética à luz do Marco Civil da Internet. Rio de Janeiro: Brasport, 2016.

Cibernética jurídica: estudo sobre o direito digital. Claudio Joel Brito Lóssio Luciano Nascimento, Rosangela Tremel (Organizadores). – Campina Grande: EDUEPB, 2020. 294 p.: il.

Convenção de Budapeste sobre Crimes Cibernéticos, 2001.

ONU. Relatório sobre Segurança Cibernética e Terrorismo Digital, 2023.