

DIREITO PENAL E CRIMES CIBERNÉTICOS: A INFLUÊNCIA DA ERA DIGITAL

Autor(res)

Rafaela Benta De Almeida
Thamyes Lorrane Silva Leal

Categoria do Trabalho

Trabalho Acadêmico

Instituição

FACULDADE ANHANGUERA DE BRASÍLIA

Introdução

A cibersegurança e os crimes cibernéticos configuram áreas que demandam crescente conhecimento devido à expansão do uso da internet e das tecnologias digitais. Atualmente, a sociedade está constantemente exposta a diversas questões relacionadas à segurança digital e à prática de delitos no ambiente virtual, muitas vezes sem o devido preparo para lidar com essas situações. Grande parte da população desconhece aspectos básicos e avançados de cibersegurança, o que impacta tanto a vida pessoal quanto o ambiente profissional, uma vez que o ciberespaço tornou-se parte integrante da rotina cotidiana. O acesso a redes sociais, a realização de transações bancárias e comerciais por meio digital são exemplos da dependência crescente dessas tecnologias.

Objetivo

O objetivo geral é analisar a influência da era digital na prática e no enfrentamento dos crimes cibernéticos sob a perspectiva penal. Objetivos específicos: 1. Identificar os principais tipos de crimes cibernéticos; 2. Descrever os procedimentos legais de denúncia; 3. Destacar a importância da conscientização digital como forma de prevenção.

Material e Métodos

O Brasil figura entre os países mais atacados ciberneticamente, com mais de 700 milhões de incidentes registrados em um período de 12 meses. Os crimes mais comuns incluem invasões de sistemas, fraudes financeiras, vazamento de dados e crimes contra a honra. O setor financeiro é o principal alvo, com mais de 20% dos ataques. Grupos como o Babuk têm operado com o modelo Ransomware as a Service, o que amplia sua atuação. A conscientização e a denúncia são fundamentais, mas ainda há carência de conhecimento e preparo técnico por parte da população. Os dados apontam que o país carece de estrutura preventiva sólida e de políticas públicas eficazes na proteção de suas infraestruturas críticas. De acordo com especialistas da área, a ausência de uma cultura de segurança digital e a falta de governança cibernética tornam o ambiente virtual brasileiro vulnerável à atuação de criminosos. Além disso, a formação técnica ainda é deficitária, mesmo entre profissionais da área de segurança pública. A pesquisa indicou que há iniciativas importantes em andamento, como a criação de delegacias especializadas e canais digitais de denúncia, mas elas ainda não são suficientes diante do volume e da complexidade dos ataques. A pós-graduação e os cursos especializados se revelam fundamentais para preparar profissionais que possam atuar de forma eficiente. Também se destacou a importância da cooperação internacional e da articulação entre os setores público e privado para combater ameaças que são, em sua



essência, transnacionais. A inclusão digital, a educação para o uso seguro da tecnologia e o fortalecimento institucional são elementos centrais para enfrentar o cenário atual.

Resultados e Discussão

O Brasil figura entre os países mais atacados ciberneticamente, com mais de 700 milhões de incidentes registrados em um período de 12 meses. Os crimes mais comuns incluem invasões de sistemas, fraudes financeiras, vazamento de dados e crimes contra a honra. O setor financeiro é o principal alvo, com mais de 20% dos ataques. Grupos como o Babuk têm operado com o modelo Ransomware as a Service, o que amplia sua atuação. A conscientização e a denúncia são fundamentais, mas ainda há carência de conhecimento e preparo técnico por parte da população.

Conclusão

A pesquisa demonstrou a necessidade urgente de políticas públicas, investimentos em tecnologia, capacitação profissional e conscientização social para o enfrentamento dos crimes cibernéticos. A formação técnica e a cooperação entre instituições públicas e privadas são pilares fundamentais para mitigar os impactos da criminalidade digital no Brasil. Além disso, observou-se que a ausência de uma cultura de segurança digital favorece a atuação de criminosos e fragiliza o sistema de proteção de dados pessoais. O Brasil, sendo um dos países mais atacados ciberneticamente no mundo, requer uma governança cibernética mais eficiente, integrada e voltada à prevenção. Conclui-se que o enfrentamento eficaz dos delitos virtuais exige uma resposta jurídica articulada com políticas públicas sólidas, educação digital e fortalecimento das instituições, de modo a garantir a proteção da privacidade, dos dados e dos direitos fundamentais no ambiente virtual.

Referências

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos. Diário Oficial da União, Brasília, 2012.
MARTINS, Isabela Ferrari. Crimes Cibernéticos: aspectos penais e processuais. São Paulo: Saraiva, 2021.
SOUZA, Carlos Affonso; LEMOS, Ronaldo. Marco Civil da Internet: construção e aplicação. Rio de Janeiro: Zahar, 2016.