**A CIBERSEGURANÇA, CIBERCRIMINALIDADE E CRIMINALIDADE**

**ORGANIZADA TRANSNACIONAL**

## 1) CONCEITO DE CIBERSEGURANÇA

A Cibersegurança diz respeito a um conjunto de ações e técnicas destinadas a proteger o ciberespaço que envolve sistemas, programas, redes e equipamentos de invasões de cibercriminosos em busca de ativos e de informações disponíveis em dispositivos eletrônicos tais como computadores e smartfones bem como em meios de armazenamento na rede mundial de computadores em nuvens, a fim de obter vantagens ilícitas no cometimento de crimes de diversos tipos: Falsificação e supressão de dados; Estelionato e furto eletrônicos *(fraudes bancárias);* Invasão de dispositivo informático e furto de dados; Armazenamento; posse; produção; troca; publicação de vídeos e imagens contendo pornografia infanto juvenil; Assédio e aliciamento de crianças; Ciberterrorismo; Ameaça; Divulgação de estupro/pornografia adulta; Interrupção de serviço; Cyberbullying (criação e publicação de perfis falsos, veiculação de ofensas em blogs e comunidades virtuais); Incitação e apologia de crime; Crimes de ódio; Crimes contra a propriedade intelectual e artística; Venda ilegal de medicamentos.

Com efeito, a segurança pública por meio de seus agentes necessita se preparar ao enfrentamento dessa modalidade de crime organizado e transnacional, razão de estarmos unidos como promotores da justiça, a bem da segurança pública, conjugando esforços de todo sistema de justiça em defesa do estado de direito democrático, dos direitos humanos e da cooperação internacional para assegurar rápida e defensiva resposta aos ataques dos criminosos cibernéticos.

Com a chegada da Era da Informação e dos cibercrimes, foi necessário se preocupar com condutas ilícitas já existentes e novas condutas praticadas no ciberespaço, que alteraram limites geográficos e ressignificaram fronteiras.

No ano de 2020, é aprovada a Estratégia Nacional de Segurança Cibernética, ou a E-Ciber, por meio do Decreto 10.222 de 05 de fevereiro de 2020. Ela funciona mais como um documento orientador de políticas públicas no âmbito do Poder Executivo, um aprimoramento do arcabouço legal sobre Segurança Cibernética.

## 2) OS CRIMINOSOS CIBERNÉTICOS

Conforme a UNODC – Escritório das Nações Unidas sobre Drogas e Crimes os criminosos cibernéticos têm sido hábeis em capitalizar as ansiedades e medos de suas vítimas, explorando o fato de que muitas pessoas

estão trabalhando de forma remota, frequentemente com sistemas de segurança desatualizados. Essa situação também levou a um maior abuso e exploração de mulheres e crianças na ciberesfera.

Esses criminosos agem de forma isolada e também em organizações criminosos, por vezes em organizações transnacionais.

Inclusive grupos terroristas utilizam-se de novos métodos e tecnologias para diversificar seus modos de financiamento, comunicação e operações, o que inclui o uso de moedas cibernéticas, drones e plataformas seguras de envio de mensagens, a Deepweb/Darkweb.

## 3) O CRIME ORGANIZADO

O crime organizado nacional e transnacional se articula em rede para a prática de aumentar sua eficiência em cometer os crimes e na cooptação de agentes públicos para facilitar sua prática criminosa e proteger seus membros das forças de segurança e justiça. Essa rede atua de forma coordenada na lavagem de dinheiro e utilizam a rede mundial de comunicação, a internet, com o intuito de facilitar o uso dos recursos monetários obtidos com os crimes, distribuindo benefícios para todos os envolvidos, inclusive os corruptos agentes públicos necessários para proteger e dificultar o trabalho das autoridades honestas.

## 4) O DELITO TRANSNACIONAL E SUAS IMPLICAÇÕES NA ORDEM ECONÔMICA E NA SEGURANÇA JURÍDICA

Esses crimes praticados pelas organizações criminosas e seus agentes em diversos países tem causado prejuízos bilionários ao sistema econômico lícito, de forma direta quando os agentes econômicos são objetos dos ataques, a exemplo de fraudes bancárias e ataques hackers aos bancos, e de forma indireta quando transacionam mercadorias ou serviços obtidos por meio de crimes cibernéticos.

É o que relata o presidente da ARME, Agência Reguladora Multisetorial da Economia, de Cabo Verde. Ele diz haver um aumento exponencial a nível mundial dos crimes cibernéticos e que Cabo Verde não se diferencia. Alega que em 2015 o mundo perdeu cerca de três

trilhões de dólares com problemas de cibersegurança e cibercrime e complementa dizendo que em 2021 a perda é estimada em seis trilhões de dólares.

## 5) FORMAS DE SEU ENFRENTAMENTO

Capacitação dos agentes de law enforcement em investigação em redes abertas e em Deepweb/Darkweb.

Criação de grupos especializados nas unidades dos Ministérios Públicos Federal e Estaduais e nas Polícias e de núcleos técnicos com treinamento e capacitação de servidores.

Maior comprometimento dos provedores – desenvolvimento de filtros e ferramentas.

Adesão do Brasil à Convenção de Budapeste – Intensificação da cooperação entre os países para facilitação na obtenção de provas.

## 6) A PREVENÇÃO AO CRIME E JUSTIÇA CRIMINAL

Conforme a UNODC desenvolvimento e implementação de estruturas legais, políticas e programas mais eficazes para combater o crime organizado transnacional, em conformidade com a Convenção das Nações Unidas contra o Crime Organizado Transnacional e seus Protocolos.

Atuação em PREVENÇÃO ao crime, tanto na área social (oficinas/seminários para professores escolares e universitários; campanhas etc.) quanto legislativa (grupos de estudo e nas Comissões Parlamentares de Inquéritos).

## 7) A QUESTÃO DAS PARCERIAS

O trabalho articulado entre os agentes públicos promotores da justiça, da segurança pública e do sistema de justiça com o setor privado, sociedade civil, academia e comunidade científica, e com outras partes interessadas relevantes mostra-se essencial para o combate às organizações criminosas.

Promover, nos níveis nacional, regional e internacional, com o devido respeito para os quadros jurídicos nacionais e os princípios do direito internacional, parcerias público-privadas com a indústria digital, o setor financeiro e prestadores de serviços de comunicação para reforçar a cooperação internacional para combater o cibercrime

## 8) O TRATAMENTO DO TEMA PELAS NAÇÕES UNIDAS

**A Declaração de Kyoto sobre o Avanço da Prevenção ao Crime, Justiça Criminal e Estado de Direito: Rumo à Conquista da Agenda 2030 para o Desenvolvimento Sustentável apresenta a importância do tema para a ONU. Esse documento assevera:**

> 1. Expressamos profunda preocupação com o impacto negativo do crime no Estado de direito, direitos humanos, desenvolvimento socioeconômico, saúde e segurança pública, meio ambiente e patrimônio cultural;
>
> 2. Também expressamos profunda preocupação com o fato de o crime estar se tornando cada vez mais transnacionais, organizados e complexos e que os criminosos estão explorando cada vez mais tecnologias novas e emergentes, incluindo a Internet, para realizar suas atividades ilícitas, criando assim desafios sem precedentes na prevenção e combate aos crimes existentes, bem como novas e emergentes formas de crime;
>
> 3. Comprometemo-nos a contribuir para alcançar a Agenda 2030 para a Sustentabilidade Desenvolvimento por meio de nossos esforços na prevenção do crime e justiça criminal, com o firme reconhecimento de que o desenvolvimento sustentável e o Estado de Direito estão interligados e se reforçam mutuamente, que o crime é um impedimento ao desenvolvimento sustentável e que alcançar o desenvolvimento sustentável é um fator que permite aos Estados efetivamente prevenir e combater a criminalidade;
>
> (...)

5. Comprometemo-nos a intensificar os esforços globais concentrados em prevenir e combater criminalidade, facilitando e fortalecendo a cooperação internacional em matéria penal;

## 9) O SEU ENFRENTAMENTO, NO BRASIL, PELO MPF

Atuação do MPF no tema. Destaque do laborioso desempenho do Grupo de Apoio sobre Crimes Cibernéticos da 2ª Câmara de Coordenação e Revisão – Criminal – do Ministério Público Federal.

Essa Câmara publicou dois trabalhos robustos sobre o assunto:

1 - CRIMES CIBERNÉTICOS. COLETÂNEA DE ARTIGOS. Volume 3, de 2018.

2 – ROTEIRO DE ATUAÇÃO. CRIMES CIBERNÉTICOS E PROVAS ELETRÔNICAS, 4ª edição atualizada e ampliada, 2021.

## 10) MODALIDADE DE CRIMES CIBERNÉTICOS

Antes mesmo do Brasil aderir à Convenção de Budapeste a legislação brasileira apresenta os seguintes tipos de crimes: Falsificação e supressão de dados; Estelionato e furto eletrônicos *(fraudes bancárias);* Invasão de dispositivo informático e furto de dados; Armazenamento; posse; produção; troca; publicação de vídeos e imagens contendo pornografia infanto juvenil; Assédio e aliciamento de crianças; Ciberterrorismo; Ameaça; Divulgação de estupro/pornografia adulta; Interrupção de serviço; Cyberbullying (criação e publicação de perfis falsos, veiculação de ofensas em blogs e comunidades virtuais); Incitação e apologia de crime; Crimes de ódio; Crimes contra a propriedade intelectual e artística; Venda ilegal de medicamentos.

Deve-se acrescer a esses as tipificações criminais da Convenção de Budapeste.

## 11) A IMPORTÂNCIA DA COOPERAÇÃO INTERNACIONAL

A cooperação internacional é essencial no combate ao crime e a adesão do Brasil à Convenção de Budapeste insere o país na legislação internacional para a rápida resolução dos crimes que envolvem a internet

## 12) A CONVENÇÃO DE BUDAPESTE E O CONSELHO DA EUROPA, A INTERPOL E A OCDE

A ADESÃO DO BRASIL À CONVENÇÃO SOBRE O CRIME CIBERNÉTICO, CELEBRADA EM BUDAPESTE, EM 23 DE NOVEMBRO DE 2001, FOI APROVADA PELO DECRETO LEGISLATIVO Nº 37, DE 17 DE DEZEMBRO DE 2021.

A Convenção do Cibercrime, que já conta com mais de 65 países aderentes, é atualmente o principal dispositivo para a harmonização da tipificação de crimes cibernéticos, para a previsão dos instrumentos necessários à efetiva persecução de crimes cibernéticos, bem como de cooperação entre países para obtenção de provas eletrônicas.

A Convenção, assim, por meio do Comitê da Convenção do Cibercrime (T-CY) e de diversos subcomitês, possibilita a constante discussão e evolução de suas provisões, mantendo sua interpretação atualizada. Por intermédio do escritório de capacitação, o C-PROC, disponibiliza diversos treinamentos dirigidos aos países membros e observadores, tudo visando à harmonização da persecução penal de crimes cibernéticos e da obtenção da prova eletrônica, em especial entre países, de modo a melhorar a efetividade da resposta estatal aos crimes cibernéticos.

A Convenção possui 48 artigos, divididos em quatro capítulos, que versam sobre terminologia, disposições penais e processuais penais e cooperação internacional. Grande ênfase é dada à harmonização da legislação penal, pedra fundamental para ampliação da cooperação entre países, ao estabelecimento de ferramentas para que autoridades possam investigar e processar crimes cibernéticos e outros dependentes de provas eletrônicas de forma mais efetiva, e à cooperação entre países, seja para a troca

de provas, seja para extradição de pessoas, em reconhecimento da natureza transnacional dos crimes cibernéticos e das peculiaridades das provas eletrônicas.

## CONCLUSÃO

**Despertado pelo espírito público do bem comum envidamos esforços na construção da agenda com o tema do Seminário A CIBERSEGURANÇA, CIBERCRIMINALIDADE E CRIMINALIDADE ORGANIZADA TRANSNACIONAL, crédulos em disseminar o conhecimento e a discussão de tema central no interesse da humanidade devido a repercussão que a vulnerabilidade do ciberespaço perpetra em todas as pessoas do mundo hodierno.**

**O Ministério Público Brasileiro se alinha aos organismos internacionais vinculados à ONU e em parceria com Universidades Portuguesas apresentam ideias ao debate a fim de promover o enriquecimento de instrumentos legislativos, persecutórios e investigativos de combate aos criminosos que utilizam a rede mundial de computadores para cometerem todo tipo de crime contra a humanidade, ruindo as democracias e a paz mundial.**