Excelências

Senhora Ministra da Justiça

Senhor Procurador-Geral da república

Senhora Coordenadora Residente das nações Unidas

Exma Senhora Coordenadora Nacional Sênior da UNODC Cabo Verde,

Senhor Embaixador da CEDEAO

Senhora Embaixadora da República de Angola

Senhora Embaixadora de Espanha

Senhora Diretora Nacional da Polícia Judiciária

Senhor Diretor Nacional Adjunto da Polícia Nacional

Senhoras e senhores Magistrados Judiciais e do Ministério Público

Senhor Diretor da UIF

Senhor Presidente da Comissão Nacional de Proteção de Dados

Senhor Presidente do Comitê Executivo da Comissão Interministerial de Coordenação das Políticas em Matéria de Prevenção e Combate à Lavagem de Capitais, ao Financiamento do Terrorismo e ao Financiamento da Proliferação das Armas de Destruição em Massa

Senhores Oficiais de ligação de Portugal e Espanha

Senhores Representantes dos EUA

Senhora Secretária Executiva da Comissão de Coordenação do Álcool e Outras Drogas

Senhoras e senhores agentes dos OPCs

Distintas e distintos convidados

Minhas senhoras e meus senhores

Em nome do Conselho Superior da magistratura Judicial e em meu nome próprio gostaria de saudar a todos os participantes a esta cerimónia de abertura do curso de formação sobre **Investigação de cibercrimes e provas digitais,** financiado pelo Escritório das Nações Unidas sobre Drogas e Crime. Queremos fazer o uso desta oportunidade para desejar a todos vós votos de boas vindas a este ambiente formativo e agradecer o facto de terem aceite o nosso convite, o que muito nos honra.

Mas também temos que o afirmar, a pertinência e atualidade deste horizonte temático *qua tale* já se trata de um convite que dificilmente deixaria o público alvo em situação de indiferença.

Na verdade, o ciberespaço facilitou em muito o nosso quotidiano, desde logo: no comércio, na compra de produtos e serviços sem necessidade de deslocação; permitiu efetuar transações bancárias e controlar investimentos financeiros; agilizou comunicações e o acesso à informação; e possibilitou a prestação de serviços públicos ao cidadão, que pode ser notificado através desses meios se assim o desejar, e tudo isto, a um custo reduzido.

Em suma, conceitos de Tempo e de Espaço estão em transmutação: uma sociedade em rede, planetarizada e digitalizada, quer económica, quer culturalmente, era - há bem poucos anos - apenas ficção científica...

Hoje, mais do que uma realidade, é - para além de tudo o que consigo traz de bom e de bem - fonte de problemas para o funcionamento de uma sociedade cujas regras não estavam preparadas para estes desenvolvimentos.

A área da tutela penal da cibercriminalidade é um bom exemplo deste desafio. Como o é a adaptação das regras do processo penal à recolha de prova no universo digital.

E sobre tudo isso é necessário reflectir, criar inquietações e abrir pistas de solução.

O legislador pátrio, na linha da normativa internacional, com ênfase na Convenção sobre o Cibercrime, tem vindo a manifestar uma crescente preocupação no combate ao Cibercrime. Neste intuito, a Lei 8/IX/2017, de 20 de março, que aprova a Lei do Cibercrime, fornece um elenco de novas disposições processuais sobre os meios de obtenção de prova, direcionadas precisamente para crimes previstos nessa lei, cometidos por meio de um sistema informático, ou em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico (artigo 13.º).

O Direito relativo à criminalidade relacionada com o mundo digital tem trazido nos últimos anos novos problemas que a ciência jurídica e, em concreto, os tribunais têm que resolver.

A aquisição da prova é um momento essencial do processo penal, mas também, e por isso mesmo, das garantias fundamentais dos cidadãos.

O debate sobre estas questões deve ser acompanhado, mas também promovido nas ações de formação de que este evento formativo é um exemplo.

A reflexão é essencial, a inquietação é necessária e, assim, as pistas de solução irão surgir (num contexto que só pode passar pelo respeito do direito constitucional).

O cardápio apresentado em matéria de temas escolhidos para este evento formativo, com ênfase no contacto com a experiência de outras latitudes, no que concerne ao uso de provas digitais em casos de cibercrime, o capítulo alusivo a avaliação da autenticidade e da confiabilidade das evidências digitais, o domínio da proteção de dados, o conhecimento das ferramentas ligadas ao uso da informática e da *internet*, o conhecimento de aspetos ligados ao uso de criptomoedas em contexto criminais, entre outros temas de significativa relevância dá-nos algum conforto quanto ao cumprimento do desiderato a que subjaz esta ação formativa – o Reforço das capacidades de intervenção dos magistrados e OPCs nesta matéria específica.

A par disto não se pode perder de vista as recomendações feitas a Cabo Verde no âmbito do combate à cibercriminalidade, que se prendem com a criação de uma unidade policial especializada, reforço da formação, alterações legislativas sobre conservação de provas digitais e sistematização de dados estatísticos, o diálogo permanente, através de uma unidade de referência, com as operadoras de comunicações e com os bancos para a obtenção de provas digitais, vigilância e prevenção em matéria de pornografia infantil e abuso sexual de menores através da *Internet*.

Na parte que diz respeito à responsabilidade do CSMJ passaremos a conferir uma atenção especial na coleta de dados estatísticos procurando especificar os dados relativos à cibercriminalidade de forma muito precisa, ou mesmo através da criação de uma base de dados de cibercrimes que permita construir um perfil do criminoso.

Podemos afirmar que o nosso país está preparado com uma legislação excelente de luta contra o cibercrime. Tem uma estratégia

nacional que vai sendo operacionalizada, tem uma legislação moderna, de vanguarda e em consonância com a convenção de Budapeste".

Na fase em que nós nos encontramos assume particular importância a aposta na formação de recursos humanos, a especialização de todos os *stakeholders* que tenham uma conexão com a luta contra o cibercrime.

Se me fosse solicitado que indicasse os maiores desafios ao combate contra o fenómeno da cibercriminalidade, elencava 3: primeiro a Facilidade, em segundo lugar, a Diversidade e em terceiro lugar a deslocalização.

Facilidade, no sentido de que é fácil disponibilizar os conteúdos *on line* e a velocidade com que os conteúdos circulam entre os diversos países no mundo potencia a emergência de novos tipos de criminalidade, bem como a prática dos crimes tradicionais com recurso às novas tecnologias. Além disso, as consequências do comportamento de índole criminosa poderão ser mais extensas e ter um maior alcance uma vez que não são restringidas por quaisquer limites geográficos ou fronteiras nacionais. A recente disseminação de vírus informáticos prejudiciais, um pouco por todo o mundo, comprova esta realidade.

Diversidade, no sentido de que globalizou-se tudo mas não se globalizou os valores, ou seja, o que constitui crime no nosso país poderá não ser num outro país, e o contrário também é verdade. O que se acaba de afirmar pode ser facilmente comprovado com os crimes de opinião.

Deslocalização: No domínio da deslocalização há que perguntar: Onde está o que postamos no *facebook*? É claro que se formos fazer uma pequena pesquisa vamos ver que o *facebook* tem um centro de servidores para a Europa, localizado na Suécia, próximo de uma pequena cidade que se chama Lulea, que é onde guarda toda a informação que é postada.

O *facebook* anunciou esta informação, mas as outras redes não o fizeram. Apesar de, o *facebook* ter anunciado esta informação, o certo é que para se aceder a ela, é necessário credenciais que estão nos EUA. Mas se só se pode aceder a uma informação que está na Suécia através de uma credencial que está nos EUA, em termos jurídicos, onde está a informação? Que país tem jurisdição sobre esta informação? Que país pode investigar e julgar crimes que ocorrem com esta informação? Em termos de *locus delicti*, o crime pode ter ocorrido em Cabo Verde, mas, como posso pedir ajuda ao outro país para investigar e julgar esse crime, se a informação principal está a "CÁ" e está a "LÁ", como disse o nosso famoso Casimiro?

Portanto, a questão da jurisdição sobre as infracções relacionadas com a tecnologia da informação, *maximé*, a determinação do local onde a infracção foi cometida (*locus delicti*) e qual a legislação aplicável em consonância com tal facto, incluindo o problema do princípio *ne bis idem* em caso de multiplicidade de competências e a questão de como resolver os conflitos de jurisdição positiva e evitar os de jurisdição negativa, são desafios candentes ao princípio da territorialidade.

No fundo para mostrar que a investigação e julgamento dos crimes cibernéticos coloca muitas inquietações a todos os *stakeholders* que

intercedem nesta luta, mas o que nos deve mover é a convicção segura de que é uma luta necessária.

Movido por este espírito de luta o CSMJ tem já em fase de finalização dois volumes da obra intitulada "**Compilação de Legislação sobre Cibercrime**" a qual tem no seu bojo estabelecer um ponto de situação atualizado e consolidado sobre o quadro normativo vigente em matéria de cibercrime e prova digital.

O Volume I contem:

✍ Lei Sobre Cibercrime

✍ Regime Jurídico Aplicável às Redes e Serviços de Comunicações Eletrónicas

✍ Regime Jurídico Geral De Proteção De Dados Pessoais Das Pessoas Singulares

✍ Regime Jurídico de Cibersegurança

✍ Estratégia Nacional para a Cibersegurança

✍ Princípios gerais de cooperação judiciária internacional em matéria penal

✍ Uma decisão do Supremo Tribunal de Justiça sobre este domínio.

O Vol. II contém:

✍ Convenção sobre Cibercrime e respetivo Relatório Explicativo;

✍ Notas de Orientação do Comité da Convenção sobre o Cibercrime;

✍ Primeiro Protocolo Adicional à Convenção Sobre o Cibercrime Relativo à Criminalização de Actos de Natureza Racista e Xenófoba

Praticados Através de Sistemas Informáticos e o respetivo Relatório Explicativo.

✍ Segundo Protocolo Adicional à Convenção Sobre o Cibercrime Relativo ao Reforço da Cooperação e da Divulgação de Provas sob Forma Eletrónica e o respetivo Relatório Explicativo.

✍ Convenção da União Africana Sobre Cibersegurança e Proteção de Dados Pessoais

✍ Convenção Para a Proteção das Pessoas Relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal

✍ Alterações à Convenção para a proteção das pessoas relativamente ao tratamento automatizado de dados de caráter pessoal

✍ Protocolo Adicional à Convenção para a proteção das pessoas relativamente ao tratamento automatizado de dados de caráter pessoal

✍ Decisões Judiciais

A seleção dos elementos coligidos foi determinada em função de critérios de pertinência teórica e relevância prática que visam dar a conhecer aos interessados nesta área do saber jurídico alguns dos elementos imprescindíveis para o desenvolvimento do estudo e da prática do direito penal e processual penal no horizonte temático em tela.

Para além de proporcionar uma visão desejavelmente panorâmica e compreensiva sobre o quadro normativo vigente neste domínio, a obra faculta finalmente aos práticos do Direito acesso fácil, imediato

e sistematizado ao quadro normativo essencial aplicável no meio forense, e que assumirá interesse e acuidade, em particular, no contexto de realização de diligências processuais de cariz intrusivo.

Acreditamos que com esta ação formativa estaremos a dar um passo significativo no longo caminho que temos de percorrer em ordem a reforçarmos a capacidade interventiva dos magistrados e OPCs em razão desta específica matéria.

Resta-nos de facto agradecer vivamente o convite da UNODC para participar nesta iniciativa louvável e igualmente engrandecer o esforço despendido na árdua tarefa de formação dos magistrados e OPCs no domínio de cibercriminalidade.

Peço permissão à mesa para também agradecer o projecto Glacy+ pela colaboração e financiamento da Compilação de legislação sobre cibercrime.

Um bem-haja

Um muito obrigado a todas e a todos.