Protocolo Fênix-PGR
2ª CCR 2030
Data: 05/02/12

MINISTÉRIO PÚBLICO FEDERAL
PROCURADORIA DA REPÚBLICA NO ESTADO DO RIO DE JANEIRO

OFÍCIO PR/RJ GAB N. C. Nº 60

Rio de Janeiro, 16 de fevereiro de 2012.

Ref.: VII Reunião de Trabalho em Delito Cibernéticos da REMJA/OEA

MINISTÉRIO PÚBLICO FEDERAL
PROCURADORIA GERAL DA REPÚBLICA
1.00.000.002746/2012-44

Senhora Coordenadora,

Cumprimentando-a, as Procuradoras da República, ora subscritoras, enviam, em anexo, o relatório que elaboraram em razão da participação na VII Reunião de Trabalho em Delito Cibernético da REMJA, convocada pela Organização dos Estados Americanos – OEA, ocorrida nos últimos dias 06 e 07 de fevereiro, em Washington/EUA.

Outrossim, informam que todos os documentos citados no referido relatório foram encaminhados à V. Exa., via *e-mail* institucional.

Atenciosamente,

NEIDE M. C. CARDOSO DE OLIVEIRA **PRISCILA COSTA SCHREINER**

Procuradoras da República

DESPACHO 221
1. Autue-se.
2. Volte-me.

Brasília, 2 / 3 / 2012
2ªCCR/MPF

A Sua Excelência a Senhora
Dra. **RAQUEL ELIAS FERREIRA DODGE**
Subprocuradora-Geral da República
Coordenadora da 2ª Câmara de Coordenação e Revisão do MPF
SAF Sul Quadra 4 Conjunto C – Brasília/DF
CEP 70050-900

Relatório VII Reunião de Trabalho em Delito Cibernético da REMJA (Washington, 06 e 07 de fevereiro de 2012)

A COOPERAÇÃO JURÍDICA HEMISFÉRICA CONTRA O DELITO CIBERNÉTICO

Neide M. C. Cardoso de Oliveira e Priscila Costa Schreiner

Primeiramente cumpre tecer alguns esclarecimentos sobre as a REMJA e as reuniões que ocorrem a cada dois anos para discussão de assuntos relacionados à cooperação jurídica internacional em matéria penal e problemas afetos a delitos transnacionais, bem como os motivos que culminaram na nossa participação na VII Reunião de Trabalho em Delito Cibernético da OEA, através da REMJA, ocorrida em 06 e 07 de fevereiro de 2012 em Washington D.C.

A _Reunião de Ministros da Justiça ou de Outros Ministros ou Procuradores-gerais das Américas (REMJA)_ são realizadas no âmbito da Organização dos Estados Americanos (OEA) e se destinam principalmente ao compartilhamento das experiências e soluções encontradas nos diversos países integrantes da OEA com vistas a melhorar e fortalecer a cooperação jurídica e judicial entre os Estados do Hemisfério.

De acordo com o site oficial da OEA (http://www.oas.org/pt/sla/dlc/remja/antecedentes.asp) dentre esses mecanismos de cooperação jurídica e judicial destaca-se principalmente o processo de Reuniões de Ministros da Justiça e de Outros Ministros ou Procuradores-Gerais das Américas (REMJA), inclusive os grupos de trabalho e as reuniões técnicas que nelas vêm se realizando. E onde se discutem desde a existência de legislação transnacional e interna de cada país sobre os temas de maior relevância no âmbito internacional na atualidade, os problemas mais graves e de maior repercussão enfrentados, assim como os diversos mecanismos e soluções que os países vem adotando, seja em seu próprio território, seja através de cooperações jurídicas internacionais, a fim de obter maior eficácia e efetividade ante a união de esforços e coordenação de ações entre si.

A proposta de criar, no âmbito da OEA, um foro hemisférico para abordar os temas relacionados com a justiça e a cooperação jurídica e judicial por meio das REMJA foi apresentada em 1996, sendo que foi organizada a primeira reunião das autoridades (REMJA-I) em Buenos Aires no ano de 1997, e desde então ficou evidenciada a importância de dar continuidade à realização periódica dessas reuniões, as quais ocorreram em 1999 em Lima/Peru (REMJA-II); em 2000 em San José/Costa Rica (REMJA-III); em 2002 em Port of Spain/Trinidad e Tobago (REMJA-IV); em 2004 na sede da OEA, em Washington, D.C./Estados Unidos da América (REMJA-V); em 2006 em São

Domingos/República Dominicana (REMJA-VI), em 2008 novamente em Washington/Estados Unidos da América (REMJA-VII); em 2010 em Brasília/Brasil (REMJA VIII), na qual se aceitou o oferecimento de sede de El Salvador para a REMJA-IX, em 2012.

No endereço eletrônico da OEA (www.oas.org), já citado acima, há referências à criação, objetivos e reuniões ocorridas no âmbito das REMJA, havendo também o reconhecimento de que "*o processo das REMJA transformou-se no foro político e técnico de maior importância no plano hemisférico sobre temas relacionados com o acesso à justiça e à cooperação jurídica internacional, bem como com seu fortalecimento, em áreas relativas ao auxílio mútuo em matéria penal, extradição, políticas penitenciárias e carcerárias, delito cibernético, ciências forenses, entre outras*".

Dando prosseguimento aos trabalhos desenvolvidos pela OEA através das REMJA, houve a realização em Washington nos dias 06 e 07 de fevereiro do corrente ano a VII Reunião de Trabalho em Delito Cibernético para tratar especificamente da cooperação jurídica hemisférica e os progressos que cada país vem obtendo no combate a tais delitos.

O Brasil foi então convidado através do Ministério da Justiça (MJ) e Ministério das Relações Exteriores (MRE) a participar da VII Reunião da REMJA sobre Delitos Cibernéticos, sendo então o convite encaminhado também ao Setor de Delitos Cibernéticos da Polícia Federal e à Procuradoria Geral da República para que enviassem seus representantes para compor a delegação brasileira na referida reunião.

Neste contexto e por se tratar de assunto diretamente relacionado aos delitos cibernéticos, fomos convidadas (Dra. Neide na qualidade de Coordenadora adjunta do GT de Crimes Cibernéticos e integrante do Grupo de Combate a Crimes Cibernéticos no RJ e a Dra. Priscila na qualidade de integrante do Grupo de Combate aos Crimes Cibernéticos em SP) pelo Procurador Geral da República, Dr. Gurgel, e pelo Coordenador da Cooperação Jurídica Internacional na PGR, DR. Edson Oliveira, a representar o Ministério Público Federal e o Procurador Geral da República no VII Encontro da REMJA na OEA sobre Delitos Cibernéticos.

Esclarecemos por oportuno que apenas fomos contatadas pela PGR e pelo Setor de Cooperação Internacional na PGR para participarmos do referido Encontro na semana anterior ao evento, no dia 30/01/2012, e a partir de então dada a importância do Encontro e o reconhecimento da necessidade de o Ministério Público Federal participar ativamente da Delegação Brasileira na Reunião juntamente com representantes do Ministério das Relações Exteriores e da Polícia Federal, não poupamos esforços para obtermos, no curto espaço de tempo que possuíamos, as autorizações e documentação necessárias, o que felizmente conseguimos, sendo que os resultados e as nossas impressões a respeito da reunião e das discussões encetadas constam do presente relatório e de suas conclusões, complementados por meio dos documentos (DOC´s)

referentes a questionário, palestras e textos apresentados, além das Recomendações resultantes da VII Reunião da REMJA sobre Delitos Cibernéticos.

Antes de dar início ao Relatório propriamente dito, anexamos o Questionário com as Respostas do Brasil para subsidiar a VII Reunião da REMJA em Delitos Cibernéticos **(DOC.1)**, com informações a respeito da legislação interna e da persecução penal aos crimes cibernéticos, encaminhados pelo MRE tanto à Polícia Federal quanto ao Ministério Público Federal e compiladas as respostas, sendo que, no âmbito do Ministério Público Federal o questionário foi encaminhado pela Cooperação Internacional da PGR a Dra. Priscila Costa Schreiner, integrante do Grupo de Combate aos Crimes Cibernéticos em São Paulo, para apresentação de respostas, e na Polícia Federal pelo Dr. Carlos Eduardo Miguel Sobral, Chefe da Delegacia Especializada em Crimes Cibernéticos.

APRESENTAÇÃO DA VII REUNIÃO DE TRABALHO EM DELITO CIBERNÉTICO DA REMJA NA OEA:

(hyperlink: "mailto:legalcooperation@oas.org"legalcooperation@oas.org)

O Grupo de Trabalho sobre Delito Cibernético das REMJA (Reuniões de Ministros da Justiça ou de Outros Ministros ou Procuradores-Gerais das Américas) realizou sua Sétima Reunião na sede da OEA, em Washington, D.C., Estados Unidos da América, nos dias 6 e 7 de fevereiro de 2012, conforme apresentações e discussões e acordou formular as Recomendações, em anexo, das quais o Brasil, por meio de seu diplomata Segundo Secretário, Luiz Marfil, e sua delegação (composta pelas Procuradoras da República, Neide M. C. Cardoso de Oliveira e Priscila Costa Schreiner; DPF Carlos Eduardo Sobral e o funcionário do Ministério da Justiça, Diogo Monteiro) contribuíram com a elaboração do parágrafo 12 e alteração da redação do parágrafo 14 da Recomendação da VII Reunião da REMJA sobre Delito Cibernético.

1º DIA - 06.02.2012

9:30 h - Sessão de abertura com menção aos países integrantes da OEA, representados pelas suas respectivas delegações e saudação do Presidente do Grupo de Trabalho sobre Delito Cibernético - Albert C. Rees Jr.

- Houve discurso realizado pelo Secretário Geral da OEA - José Miguel Insulza, no qual se ressaltou a importância do tema já que a era da informação

trouxe uma nova geração de delitos, em relação aos quais o agente não precisa estar presente para sua prática e tem caráter transnacional por natureza, do que se extrai a imprescindibilidade da cooperação internacional, bem como a capacitação e treinamento dos agentes para enfrentar tais delitos (como ocorreu em Miami e outros lugares). Também foi observado pelo Presidente do Grupo de Trabalho e pelo Secretário Geral o fato de haver muitos casos nos quais a ausência de legislação leva à impunidade, citando exemplos de países, como Brasil, México e Paraguai, que possuem legislação própria, porém enfatizou a importância de se ter na legislação a tipificação de crimes específicos de internet como a invasão e/ou destruição de dados, de aumentar a cooperação entre os países e e destes com as empresas privadas, destacando que estariam presentes fazendo exposições representantes dos provedores Yahoo e Microsoft. Agradecimento ao final.

- Eleição da Presidência do Grupo de Trabalho: inicialmente houve requerimento da delegação do Chile para presidir os trabalhos, no entanto, a delegação do Canadá agradeceu o apoio técnico oferecido pelos EUA e pediu para que os EUA, através de sua delegação, assumisse a presidência da VII Reunião, o que foi acolhido pelos demais e aceito o encargo pela delegação dos EUA.

- Posteriormente houve a aprovação da agenda **(DOC.2)** e do calendário **(DOC.3)** da reunião, e, como não houve objeção, foram ambos aprovados.

<u>**10 h às 11 h**</u> - *Apresentação do Diretor do Departamento de Cooperação Jurídica da Secretaria de Assuntos Jurídicos da OEA*: <u>*A cooperação jurídica hemisférica contra o delito cibernético - "Desarrollos en el marco de la OEA"*</u> **(Apresentação na íntegra – DOC.04)**

- Houve a apresentação sobre os antecedentes e evolução dos mandatos do Grupo de Trabalho, resultados do questionário preparatório da reunião e Portal Interamericano de Cooperação em Delito Cibernético, este último resultado da VI Reunião da REMJA sobre Delitos Cibernéticos, portanto, da reunião anterior.

- Apesar da criação e evolução da REMJA constar do site da OEA, como já referido na introdução deste Relatório, destacamos a menção na apresentação ao processo das REMJA, nas qual se ressaltou o seguinte:

- Em 1997 houve a necessidade de se instalar um foro político e técnico com temas de justiça e decidiu-se que seria uma reunião de Ministros da Justiça dos diversos países membros da OEA, as REMJA, sendo que a primeira reunião ocorreu na Argentina. Posteriormente, se somaram aos Ministros da Justiça as autoridades máximas representantes das Polícias e Ministérios Públicos nos países, sendo que a próxima reunião da REMJA já foi aprovada e será em San Salvador. Destaque para as reuniões de grupos de trabalho no âmbito das

REMJA, específicos sobre temas de preocupação atual e que ultrapassam os limites das fronteiras de uma país, tais como o combate aos crimes cibernéticos, motivo daquela VII Reunião do Grupo de Trabalho.

- Nos desdobramentos da cooperação jurídica internacional para o combate aos crimes cibernéticos na OEA destacou-se o Programa de Capacitação com patrocínio dos EUA, para investigadores e peritos, em um primeiro momento, e procuradores e juízes, em um segundo e terceiro momentos. É uma estratégia na qual estão envolvidas três instâncias da OEA.

- Ênfase à importância da sistematização da legislação dos Estados na matéria, tanto a legislação substantiva como a processual: neste ponto esclareceu-se que o questionário, anexo (DOC.1) enviado foi aos países membros para se ter uma noção da situação normativa de cada país em matéria cibernética (no Brasil o questionário foi respondido pelo MPF através da procuradora da República Priscila Costa Schreiner; pela Polícia Federal através do DPF Carlos Eduardo Miguel Sobral e pelo Ministério da Justiça através do Terceiro Secretário o diplomata Leonardo Wester).

Foi esclarecida a forma de divisão do questionário, em 4 áreas temáticas, tecendo-se comentários a respeito de cada um deles no decorrer da exposição:

1 – Legislação (delitos substantivos e processual) – houve a apresentação através de gráficos e estatísticas com a percentagem de países que possuía tipificação de delitos cibernéticos, e, dentre estes, quais possuíam tipificação de crimes estritamente cibernéticos (ex. furto de dados telemáticos), e, na parte processual quais os países que responderam que podiam ter acesso à informação sem autorização judicial (5%) e quais possuíam leis para regular a interceptação telemática (só 4 países da OEA não possuem legislação sobre o tema)

2 – existência de setores e áreas especializadas, tanto na Polícia Federal quanto no Ministério Público Federal, para tratar de crimes cibernéticos: apresentação dos resultados obtidos com os questionários também em forma de gráficos e percentagens

3 - área temática – destaque para a cooperação internacional em matéria de crimes cibernéticos e para a criação de um Portal com esclarecimentos e informações dos países membros que deveria ser sempre alimentado pelas suas respectivas autoridades.
- O Portal pode ser encontrado na página da OEA sob a denominação de Cyberacess (Portal), cuja senha de acesso é Cyb7cri$

O conteúdo deste Portal (em idioma inglês, francês, espanhol e português) refere-se a: a.) Legislações nacionais; b.) Direitos Autorais; c.)

Conclusões e d.) Crimes; sendo que há uma página para cada país membro com informações sobre o próprio país, a sua luta contra os delitos cibernéticos, publicações periódicas e legislação, e, além desses, agora também sobre cooperação internacional entre os países.

- também pode ser encontrada no Portal uma *Rede Hemisférica de Intercâmbio de Informações para o Auxílio Mútuo em Matéria Penal e Extradição* (Cooperação Internacional), formada por um grupo de especialistas, que reúne um conjunto de ferramentas eletrônicas para facilitar a informação entre os países.

O propósito da Rede Hemisférica é a troca de informações e é formada por:

a - *Componente público*:

- Biblioteca virtual - os aspectos jurídicos dos Estados, como está sendo aplicada a legislação na doutrina e jurisprudência;

- Assistência em matéria penal – Tratados e Convenções (não há aspectos políticos, pois seria muito complicado dada a soberania de cada Estado)

- OBS: para facilitar a consulta e dar um apoio aos Estados, podem ser colocadas palavras chaves para a busca

b - *Componente privado:* informações de reuniões ocorridas; de acordos bilaterais ou multilaterais celebrados, cursos de capacitação que ocorreram ou vão ocorrer.

c - *Componente seguro* (sistema de comunicação eletrônico seguro) – é um sistema desenvolvido que facilita a comunicação de forma segura. Outras aplicações:

- Formulário de Assistência Mútua – importante destacar que o formulário não foi criado unicamente pelos EUA; foi resultado de matéria de discussão com outros países;
- Formulário de extradição
- Diretório de contatos seguro
- Comunicação de áudio e vídeo seguro, ao qual o público não tem acesso

(há também a garantia de um sistema de vídeo conferência seguro) - 6 países estão participando no momento: Argentina; Brasil; Chile; Colômbia; Uruguai e Peru

4 - área temática: destaque para os cursos de capacitação na investigação, persecução penal e processamento dos crimes cibernéticos ministrado por

instituições como o FBI, a pedido das autoridades dos países membros interessados

<u>11h às 11h 30</u> - **Apresentação da Seção de Delito Cibernético e Propriedade Intelectual, do Departamento de Justiça dos Estados Unidos** - Anthony Teelucksingh

- Apresentação dos resultados dos *workshops* regionais de capacitação sobre provas eletrônicas e legislação em delito cibernético, destacando-se o Curso de Investigação realizado em 2010, na Cidade do México/México e em Lima/Peru

Em 2010: foco do curso Initial Investigation and folllow up (Início da investigação e seus seguimentos/desdobramentos) – como deve ser feita a correta colheita de provas/evidências eletrônicas:

- Computer Forensics and Colleting Digital Evidences (Perícia e Colheita de provas na área de informática)
- International assistence – assistência técnica e jurídica internacionalmente
- Intelectual property/computer crime/credit card fraud exemples – crime contra a propriedade intelectual e fraudes por meio de cartão magnético

- Cybersecurity and cybercrime (Segurança e criminalidade cibernética) - em maio/2011 foram ministrados cursos em Miami, EUA - Fomentar o desenvolvimento de estratégias nacionais

- Cybersecurity track and Terrorist use of internet (segurança e riscos na internet, uso terrorista da internet) – em novembro/2011 em Bogotá, Colômbia – Treinamento físico e técnico e trabalho com a força-tarefa de cada país

Foi exposto que nos cursos há um foco na legislação interna especialmente para para aqueles países cujos representantes queriam desenvolver e aprimorar suas legislações – há uma introdução de como é a legislação do país e a investigação dos crimes cibernéticos. Mencionou-se que alguns países tinham experiência suficiente em relação ao conceito e modalidades de crimes cibernéticos, mas uns 10% não possuíam tal conhecimento nem legislação sobre crimes cibernéticos – havia uma escolha do que era considerado crime cibernético baseada na cultura de cada país e no bem jurídico que se queria proteger; em 80% dos casos no curso há um foco na base da legislação de como deve ser o crime cibernético e o resto cada país adapta à sua própria legislação, no caso de aplicação de uma legislação transnacional por exemplo

Contato:
HYPERLINK:
"mailto:anthony.teelucksingh@usdoj.gov"anthony.teelucksingh@usdoj.gov.
tel: + 1(202) 514-1026

No encerramento da palestra foi apresentado o tema para trabalho bilateral (agentes treinadores/EUA e agentes a serem treinados): um curso do Departamento de Estado nos EUA com foco em um programa de delitos cibernéticos e terrorismo a ser ministrado por uma agência (TAP) dentro do Departamento de Justiça formado seus agentes e procuradores ("fiscales") que farão cursos de capacitações nacionais como na Colômbia e Guatemala, proporcionando capacitação física e técnica (cursos como desarmar computadores por exemplo), dependendo da necessidade e da análise do que cada país precisa

- Foi aberto para perguntas aos Países presentes, tendo sido formulados questionamentos, dos quais se destacaram os seguintes:

1. Pelo Paraguai: Como atraem os participantes para capacitação?

R.: Pelo Departamento de Estado: Nós dependemos da Embaixada de cada país que deve fazer a indicação das pessoas a serem treinadas, após há entrevistas. Inicia-se com o básico para ver como o grupo, em número sempre pequeno, reagirá.

2. Pela Colômbia: Se a capacitação pode ser só sobre crimes de cibernéticos?

R.: Sim.

3. Pelo Panamá: Se para juízes há capacitação?

R.: É um desafio atrair a atenção dos juízes, inclusive os norte americanos, para manter a sua independência e distanciamento, dificilmente aparecem em reuniões com policiais e promotores.

4. Pela Argentina: Se há preocupação em formar cursos de capacitação para difundir, "formar formadores" (treinadores)?

R.: No México, foi feito para peritos que se tornaram multiplicadores/treinadores, mas depende do país, financiar cursos como estes é difícil, mas há um projeto piloto deste tipo de curso no México.

5. Pelo Peru: Se há algum projeto específico para MP e Juízes ou para ser ministrado em faculdades de direito, advogados, ou melhor, como se pode introduzir tal curso na faculdade?

R.: Nunca foi pensado em um curso para advogados, mas seria interessante e poderia ser pensado em um curso para advogados, que exigiria nova preparação para os treinadores.

Neste ponto houve intervenção do Brasil, através da Procuradora da República Priscila Costa Scheiner que questionou a pertinência de se estender o curso aso advogados de defesa vez que estes poderiam repassar as técnicas de investigação aos seus clientes e contatos destes, o que poderia implicar em um esvaziamento ou ineficácia do próprio curso dirigido aos agentes da persecução penal. Ao final foi então questionado que se eventualmente fosse ministrado um curso também aos advogados e defensores, este deveria ser pensado cuidadosamente e de maneira específica para eles, para que não viessem a atrapalhara a atrapalhar a própria investigação e acusação em casos futuros.

R. A este questionamento respondeu-se que realmente tratava-se de uma questão delicada e que cada país internamente deve decidir quem enviar para o curso de capacitação, inclusive se deveria enviar ou não advogados.

6. Pelo México: Expôs o problema dos provedores de serviços, que alegam sigilo e proteção de dados, quais os limites então que poderíamos "invadir" ou investigar?

R.: No setor privado, o tema não poderia ser ignorado, mas o questionamento deveria ser colocado na parte da tarde quando então haveria uma apresentação específica das empresas provedoras YAHOO e MICROSOFT através de seus representantes para abordar este e outros temas.

Foi dito pela Nicarágua que esta compartilhava com o Brasil, Panamá e México esse comportamento dos provedores de serviço de impedir ou dificultar o acesso aos seus dados e serviços em determinadas hipóteses.

- **<u>11h30 às 12h30</u>** – Exposição sobre o *Andamento da Implantação da Estratégia Interamericana Integral de Segurança Cibernética. Apresentações a cargo da Secretaria Executiva da Comissão Interamericana de Telecomunicações (CITEL); da Secretaria do Comitê Interamericano contra o Terrorismo (CICTE) e da Presidência do Grupo de Trabalho sobre Delito Cibernético das REMJA*

<u>SOBRE A CITEL</u> (apresentação Clovis Baptista): mandato para os representantes da CITEL- Estudar os aspectos de segurança da comunicações e papel importante do setor privado nas comunicações e segurança

Há um plano de trabalho (CITEL *work plan*) - desenvolvimento doméstico e regional a fim de ajudar a aplicação de técnicas seguras nas comunicações, a fim de proteger nossas estruturas em relação às informações que recebemos e protegemos (segurança na internet)

- Desenvolvimento de um manual técnico – objetivo – aumentar a consciência cibernética

- Outro produto de trabalho – CITEL *workshops* no Equador, Argentina - conscientizar a comunidade internacional

OBS: informação sobre a CITEL e seu trabalho disponível na pagina web http://www.oas.org/citel

A CITEL trata da seguridade e proteção de telecomunicações, associados à união internacional com vistas a se utilizar as melhores práticas e estabelecer estratégias nesta área de telecomunicações e de segurança cibernética, tendo como principal objetivo servir como foro a permitir uma constante cooperação entre Estados membros e setor privado. A CITEL cuida também da segurança de infraestrutura e são ligados aos Ministérios de Comunicação, para ajudar a seguridade cibernética.

Durante a palestra foi ressaltado que devido à autonomia das empresas na área cibernética e telemática, os ataques são crescentes, inclusive nos meios de telecomunicações, sendo necessário tomar medidas para implementar a segurança na internet, daí a criação deste grupo (CITEL), no qual as entidades privadas são parte importante, e que possui como representantes especialistas; resumidamente, o grupo CITEL é, basicamente, um centro de informações, inclusive internacionalmente.

Contato:
CONTATO: Clovis Baptista (Secretário Executivo)
cbaptista@oas.org

SOBRE A CICTE: A CICTE atua apenas nos atos e crimes de terrorismo

- objetivo: prevenir, combater e eliminar qualquer forma de terrorismo

- treinamento e capacitação especificamente na área cibernética

- devido aos crescentes ataques terroristas, incrementado pelo uso da internet, há necessidade de comunicação eficaz e imediata entre os países afetados por um determinado incidente – essencial a segurança nas comunicações e confiança entre os países afetados e que irão compartilhar

informações

HYPERLINK "http://www.cicte.oas.org"www.cicte.oas.org

- **12h30 às 14 h** - Intervalo para o almoço

- **14h às 15h30** - ***Cooperação entre as autoridades responsáveis pela investigação e processo penal do delito cibernético e o setor privado.*** Apresentações a cargo de Christopher Bubb, Conselheiro Jurídico Geral Associado, Yahoo!, Inc.; Freddy Karprzykowski, Assessor em matéria de segurança da Microsoft Corporation; Pablo Martinez, Agente Especial do Serviço Secreto dos Estados Unidos; e Anthony Teelucksingh, da Seção de Delito Cibernético e Propriedade Intelectual do Departamento de Justiça dos Estados Unidos.

A exposição iniciou-se pela apresentação de Freddy Karprzykowski, da empresa Yahoo, onde ele ressaltou que participava com o FBI, da seção americana para combate a delitos cibernéticos e quando havia um ataque, a rapidez era muito importante. Às vezes, apenas adquirir mais teconologia não é suficiente para coibir os avanços dos delitos cibernéticos, o que adianta é trabalhar com cooperação. Basicamente, quanto mais computadores os criminosos controlem, mais poderão atacar.

Mecanismos usados para conduzir males na internet (spams, denial of service, click fraud, more malware distribution)

Em seguida o Representante da MICROSOFT falou sobre ação da força-tarefa (law enforcement action) com menção aos denominados BOTNETS = robot NETworks e o Projeto da MICROSOFT chamado de Projeto MARS (caso estudado)

OBS: Sobre a Yahoo! e a cooperação entre as autoridades responsáveis pela investigação e persecução (Cooperation between the Authorities responsable for investigating and Prosecuting) - contato na Yahoo nesta área Christopher Bubb

CONTATOS:
General Compliance Line: +1 408 439 36 87
Para questões emergenciais: + 1 408 349 54 00
HYPERLINK "mailto:legalpoc@Yahoo-inc.com"legalpoc@Yahoo-inc.com

Na América Latina (Latin american)
HYPERLINK "mailto:ha-legalpoc@Yahoo-inc.com"ha-legalpoc@Yahoo-inc.com

Aberta a palavra aos membros das delegações presentes, houve a intervenção da Procuradora da República Priscila Costa Schreiner, que expôs o caso emblemático da Google do Brasil, que culminou com a assinatura de Termo de Ajustamento de Conduta entre o MPF e a referida empresa, e questionou aos representantes das empresas Yahoo e Microsoft em que período são fornecidas as necessárias informações solicitadas pelas autoridades para a persecução criminal dos delitos cibernéticos, inquirindo-os também a respeito da possibilidade de realização de interceptação telemática e a quais leis, se realizada, a interceptação deve se submeter (se do país da filial da empresa provedora de serviço ou do pa[is onde foi cometido o delito e emanda a ordem para interceptação), ao que os representantes da empresa responderam em ambos os questionamentos que deveria ser visto o problema caso a caso.

Outros questionamentos surgiram tais como: Nos países em que não há escritórios ou representações das empresas, como se deve proceder?

R.: As empresas mantém escritório em Miami para responder à América Latina e pretendem estender os escritórios das empresas para mais países.

15h30 às 17h30 - Marcos Jurídicos internacionais para combater o delito cibernético. Apresentações a cargo de Cristina Schulman, do Conselho da Europa; Normand Wong do Departamento de Justiça do Canadá; Anthony Teelucksingh, da Seção de Delito Cibernético e Propriedade Intelectual do Departamento de Justiça dos Estados Unidos e **Delegação do Brasil por meio do Representante do MRE na OEA, Luis Marfil.**

Primeiramente, houve a apresentação de Normand Wong do Departamento de Justiça do Canadá, no qual foi exposto o contexto canadense (Canadian Context) a respeito de cibercriminalidade, observado que o Canadá é um dos quatro países for a do Conselho da Europa que ratificaram a Convenção de Budapeste, e são um dos seus fortes colaboradores atuais.

- Menção a Bill C-51 Investigative Powers for 21 st century act (artigo de lei)

- Já há uma lei de 1995, o projeto de lei 52 vai prever a questão da posse de dados telemáticos

- As Nações Unidas recentemente começaram um estudo sobre a questão dos crimes cibernéticos, e também indicaram um interesse na realização de workshops em crimes cibernéticos

A segunda apresentação foi da representante do Conselho da

Europa, Cristina Schuman que discorreu a respeito da Convenção de Budapeste, esclarecendo que foi o primeiro texto transnacional sobre crimes cibernéticos, e já conta com mais de 10 anos (a Convenção é de 2001), um trabalho para o qual, à época, não foram chamados todos os países, como por exemplo o Brasil, porém não se teria mais como retroceder no tempo, mas sim sim pensar para o futuro, observando que não devem ser disperdisados dez anos de trabalho.

Conclamou, assim, que todos os países ratificassem a Convenção, assinalando que cada vez mais será necessária a cooperação entre os países, assim, conluiu defendendo a existência outras ferramentas como por exemplo acordos regionais tendo como ponto de partida a Convenção de Budapestee observando que desde 2006 há atividades de cooperação com muitos países – 146 países aderiram à Convenção, e houve a incorporacão da OEA; dos EUA e Canadá.

Em anexo a apresentação na íntegra do Conselho da Europa na VII Reunião do GT Delitos Cibernéticos da REMJA **(DOC. 5)**

Aberta a palavra ao Diplomata brasileiro na OEA - Luiz Marfil o qual procede à leitura do texto enviado pelo Itamaraty defendendo e justificando a posição do governo brasileiro contrária à ratificação da Convenção de Budapeste pelo Brasil.

Segue abaixo o texto na íntegra:

> *"O interesse dos Estados em buscar atualizações legais no plano internacional que possam melhor instrumentalizar as autoridades competentes para aplicar a lei no espaço cibernético tem resultado em acaloradas discussões políticas, surgidas em diversos foros e iniciativas.*
>
> *Atento a essa nova realidade, o Governo brasileiro atribui importância e prioridade ao tema de combate ao crime cibernético no plano internacional. Nos últimos anos, iniciativas que visam a buscar soluções ao problema têm surgido em diversos foros, sejam regionais, plurilaterais ou multilaterais.*
>
> *Embora seja, até hoje, o único instrumento jurídico internacional voltado à questão do crime cibernético, a Convenção do Conselho da Europa sobre Crime Cibernético, comumente denominada Convenção de Budapeste, não pode ser considerada como um acordo de abrangência universal. Tal foi o entendimento a que se chegou durante a Cúpula Mundial sobre a Sociedade da Informação, realizada em 2005, cuja Declaração reconhece, no parágrafo 40, a Convenção de Budapeste como um instrumento regional.*
>
> *No âmbito interno, o Governo brasileiro analisou, em 2009,*

de forma abrangente, a Convenção de Budapeste, por meio de grupo de trabalho informal constituído com a finalidade de identificar os méritos e imperfeições do documento, à luz das eventuais necessidades de aperfeiçoamento dos dispositivos de combate ao crime cibernético existentes no ordenamento jurídico interno, na prática e interpretação jurídicas e na jurisprudência brasileira no assunto. Constatou-se, na ocasião, a incompatibilidade de dispositivos da Convenção de Budapeste ao ordenamento jurídico interno, em razão da impossibilidade de reservas ou declarações interpretativas a artigos específicos

A principal restrição brasileira à Convenção de Budapeste, embora não a única, refere-se ao seu artigo 10, que trata de propriedade intelectual. O Grupo de Trabalho concluiu que não havia disposição do Governo em expor o País a possível pressão internacional na matéria e ver-se coagido a aplicar princípios dos quais discordamos. Em 2011, a Convenção foi novamente considerada em encontro que reuniu grupo ainda maior de representantes do Governo brasileiro. Dentre as conclusões do encontro está a confirmação de que não é interesse do Brasil aderir à Convenção de Budapeste, e sim unir esforços com toda a comunidade internacional no sentido de discutir, de maneira ampla e participativa, meios efetivos para combater o crime cibernético.

A lógica subjacente à negociação que resultou na Convenção de Budapeste, ao tentar encontrar solução para determinado aspecto do problema – propriedade intelectual – como prioridade irrenunciável no combate à criminalidade cibernética, talvez ajude a explicar por que, dez anos após a conclusão do texto, a Convenção está em vigor apenas em 32 países. Entre os que o fizeram, apenas um não integra o Conselho da Europa.

Em busca de alternativa que atenda às necessidades da comunidade internacional de modo amplo, e no marco das Nações Unidas, os Estados participantes do XII Congresso sobre Prevenção do Crime e Justiça Criminal, realizado em abril de 2010, em Salvador, no Brasil, estabeleceram mandato à Comissão das Nações Unidas sobre Prevenção ao Crime e Justiça Criminal a convocar grupo de especialistas intergovernamentais para realizar estudo abrangente sobre o crime cibernético e as respostas ao problema por parte Estados-membros, da comunidade internacional e do setor privado. Esse exercício deverá incluir o intercâmbio de informações sobre legislações nacionais, melhores práticas, assistência técnica e cooperação internacional, com vistas a examinar opções para a proposição de novas respostas legais, internas e internacionais ao problema. Esse mandato foi posteriormente referendado pelo Conselho Econômico e Social das Nações Unidas (Resolução 2010/18) e adotado pela 66a. Assembléia-Geral da ONU (Resolução 65/230), o que deu renovado impulso à busca de um equacionamento

global e inclusivo sobre opções de combate ao crime cibernético com base em processos negociadores multilaterais das Nações Unidas. O grupo de trabalho foi, então, constituído em janeiro de 2011, no âmbito do Escritório das Nações Unidas sobre Drogas e Crimes (UNODC), em Viena.

A criação do Grupo de Trabalho no âmbito do UNODC alterou, portanto, a perspectiva internacional sobre o combate ao crime cibernético desde que nos reunimos da última vez, em 2010, aqui em Washington, durante a VI Reunião do Grupo. A cooperação jurídica internacional, portanto, deve ter como parâmetro as discussões no âmbito das Nações Unidas, onde todos os Estados podem participar ativamente das discussões e apresentar, de forma democrática, suas perspectivas para o combate eficaz do crime cibernético.

Tendo presente o interesse do Conselho da Europa em buscar soluções efetivas para o problema do crime cibernético em escala global, seria importante considerar o apoio firme daquele Conselho à iniciativa do UNODC, caminho que poderá levar a solução construída de modo verdadeiramente global, participativo e transparente.

A atuação internacional dos países não deve limitar-se à negociação de novo instrumento internacional como única alternativa para a busca de soluções ao problema da criminalidade cibernética. Ao estudar opções efetivas para combater esse crime, o objetivo é o de contribuir para um paradigma de gestão do espaço cibernético que seja inclusivo, centrado na pessoa e orientado ao desenvolvimento, em linha com as conclusões emanadas da Cúpula Mundial sobre a Sociedade da Informação.

Por fim, destaco um conjunto de diretrizes que não pode ser afastado de qualquer debate relativo à Internet. São elas:

i) o direito à segurança em equilíbrio com os demais direitos humanos, como os direitos à liberdade de expressão e associação, à comunicação, ao acesso ao conhecimento e à cultura, ao devido processo legal, à presunção de inocência, à privacidade dos cidadãos e à transparência da administração pública;

ii) a proteção da funcionalidade e estabilidade da própria Internet como ferramenta aberta, continuamente inovadora e destinada a múltiplos usos sociais;

iii) o envolvimento, no processo de discussão, dos diversos atores interessados na Internet, desde aqueles que podem ser afetados pelo crime cibernético como aqueles afetados pelas medidas destinadas a combatê-lo. Dessa forma, além das autoridades policiais e de proteção dos direitos humanos, a comunidade técnica e a sociedade civil são agentes que devem participar de qualquer processo negociador sobre a matéria; e

iv) a identificação do procedimento mais adequado no âmbito

das Nações Unidas que privilegie a coordenação e a participação dos países e das sociedades."

<u>2º Dia: 07 de fevereiro de 2012</u>

Inicialmente observamos que a Delegação Brasileira se reuniu na sede da missão brasileira na OEA, no edifício Watergate, às 8 h30, na qual conversou por telefone, no viva voz, com o 3º Secretario no Brasil, o diplomata Leonardo Wester, que redigiu o texto lido pelo diplomata brasileiro na OEA, Luiz Marfil, no dia anterior e reforçou o posicionamento do Brasil.

- 9h30 às 11 h - *Cooperação e assistência internacional em matéria de delito cibernético.* Apresentações a cargo de Janice Traver, Escritório de Assuntos Internacionais do Departamento de Justiça dos Estados Unidos; Andrew Fobert, do Departamento de Justiça do Canadá; Michael G. Shanahan, do Escritório Federal de Investigações (FBI) do Departamento de Justiça dos Estados Unidos; Marcos Salt, da Universidade de Buenos Aires, Argentina.

Houve uma primeira apresentação do FBI, mais especificamente da Divisão do FBI de Crimes Cibernéticos sobre o PROGRAMA DE TREINAMENTO EM CRIMES CIBERNÉTICOS (FBI Cyber Alert Program), no qual há um trabalho dos países interessados com o FBI, através de seus escritórios situados na América Latina.

- logística para trabalhar com o FBI: ter uma vítima no país

<u>MECANISMO DE COOPERAÇÃO (Mechanics of Cooperation)</u>
<u>Etapas para o sucesso do trabalho/parceria com o FBI:</u>

1) Obtenção legal da informação – a lei protege a privacidade, sendo que, quando se precisar de determinada informação, há de se pedir uma autorização para que a informação possa ser obtida e compartilhada. Por exemplo: se há um caso em que é necessária a obtenção de informação dos EUA deve-se primeiramente entrar em contato com representante do FBI (consultar o escritório para assuntos legais) e se fornece a conta de email investigada no país para ver se já esta sendo investigada nos EUA nos casos em que o servidor for dos EUA (regras jurídicas: Title 18, estatuto 27 e 15 – quando da obtenção de decisão judicial pode haver compartilhamento com outros países)

2) Arquivos gravados (record checks): idenficar se existe investigações no FBI, coordenar tais investigações com as partes envolvidas e possibilidade de se trocar ou compartilhar estas informações

3) Preservação das evidências – as evidências são preservadas por no máximo até 90 (noventa) dias, então atentar para ver se precisa por prazo superior para se fazer um pedido complementar antes de expirar o vencimento dos noventa dias. Há opção nos casos urgentes de utilizar a rede 24/7 (plantão 24 horas, 07 dias por semana)

4) Identificação pertinente das evidências/provas: fornecer o máximo de elementos que o país dispõe sobre o objeto da investigação.

OBS – este intercâmbio de trabalho e informações pode ser feito através da Polícia Federal de seu país (que tem acordos com o FBI), e, se não houver, o pedido de cooperação pode ser feito por cooperação internaciona, ou, ainda, carta rogatória (mais demorado)

- CASOS DE EXTRADIÇÃO: através de MLAT/Letter Rogatory Process

- Comentários a respeito dos pedidos de cooperação:

– do ponto de vista de força-tarefe é preferível *receber* pedidos, que devem ser realizados através das Embaixadas de cada país e em inglês para que sejam preservados os dados pelos provedores nos EUA, não se esquecendo que nas situações em que há risco de vida pode ser utilizada a rede 24/7.

– Assim, em resumo:

a) pedidos de cooperação devem ser emitidos por sua autoridade central, ou melhor, pela autoridade responsável por cooperação no seu pais;

Início no Escritório Internacional de Assuntos Jurídicos nos EUA - Departamento de Justiça dos Estados Unidos - é o escritório internacional , a autoridade central (US Department of Judice - DOJ, Office of International).

b) pedidos devem vir em inglês – e levar em consideração que demoram aproximadamente de uma semana a um mês para serem apreciados

c) especificação do pedido: identificação do provedor de serviço de internet; como e de que forma ocorreu o crime, do que se trata o delito, a narração a explicação dos fatos *(incluir os conco "w" - (who, where, what, when, why)* – isto se exige para evitar que haja atrasos, e tenha que se mandar de volta os pedidos incompletos (na Colômbia estão organizando um curso para explicar estes detalhes para que nao sejam devoividos os pedidos). Por exemplo do ponto de vista de serviço de provedor de internet (Google; Yahoo etc), o pedido deve ser formulado em inglês, e o mais importante é não

perder a informação e preservar a conta instantaneamente (lembrar que será por no máximo 90 dias), e, junto com o pedido para preservação da informação, prover o pedido com as informações básicas (IP etc) – PORTANTO: em se tratando de Serviço de Internet (Internet Service) o mais importante é preservar a informação, os registros de IP, *e-mail*, lembrando-se que os provedores não fazem nada sem uma decisão judicial.

TREINAMENTO PELO ESCRITÓRIO DE AGREGADOS JURÍDICOS (FBI)

- é um programa de capacitação de 10 semanas abrangendo temas diversos – trabalhar com os investigadores de cada país para ver do que necessitam em determinada situação – o treinamento o FBI proporciona (oportunidades de capacitação)
- os agentes que farão o treinamento devem saber inglês e para testar sua aptidão no idioma se sujeitam a uma prova oral e escrita
- alguns sucessos recentes internacionais do treinamento do FBI

  - na Ucrânia difundiu-se um software com sendo um antivirus, mas não havia um antivírus real, havia uma fraude – o FBI trabalhou com todos os países afetados por este caso cibernético, sendo que a única forma de êxito foi a cooperação;

- desmantelamento do grupo chamado *megaupload* – relacionado a violação de direito autoral e direito a propriedade intelectual

- **SOBRE O MLAT (Mutual Legal Assistence Cooperation)** –
  - prática entre Estados para que um auxilie o outro

Tipos de MLAT:

1- Police-to-Police Cooperation – (diretamente entre Polícias ou através da INTERPOL); é a mais comum, nenhum país impede a troca de informações entre forças policiais. As vantagens: fácil e rápido se comparado aos casos de pedidos formais ou baseados em tratados, porém a desvantagem é que em determinados é necessária ordem judicial para o fornecimento ou compartilhamento de determinada informação;

2- Letters Rogatory Requests (EXEQUATURS) - Requerimentos através de Cartas Rogatórias - os requerimentos ocorrem entre os tribunais (requests made between courts, includes taking of commissing). As vantagens: assistência avalizada que pode ser usado tanto pela acusação quanto pela defesa, tanto para matéria penal quanto civil; está em formato certificado/oficial para uso em procedimentos judiciais. Porém são tipos limitados de assitência

3- Non-treaty Letters of Request – casos em que não há Tratados entre os Estados e a cooperação Polícia-Polícia não está disponível

4 - Treaty Request - Requerimento com base em Tratado – é a base dos pedidos no Canadá já que o país faz parte de 35 tratados bilaterais de assitência legal mútua, e vem aumentando. Também o Canadá faz parte de vários tratados multilaterais.

OBS: A exposição mostrou interesse na medida em que está diretamente ligado aos pedidos relacionados a internet e "blackberry"

A vantagem é que há uma vasta extensão de medidas disponíveis neste tipo de cooperação.

Quais os recursos oferecidos através dos requerimentos via tratado? Tipos de Assistência Mútua:

1. Para Procurados – ordens de busca(s. 15); evidence gathering orders/ordem para receber provas físicas (pode compelir ao depoimento de testemunhas ou a fornecer prova documental – ex. Registros bancários) – a ordem deve ser enviada antes da prova ser transmitida/transferida;

2. Transferência de pessoas, aplicar multas ou de embargo

3. Outras ordens criminais (orther criminal orders) - Ex.: uma pessoa pode ser compelida a aparecer no Estado estrangeiro via video link

4. Rito processual - passa pelo autoridade central, que no Canadá é o Ministro da Justiça (s. 18 e 22 do MLAT Act) - tem que se demonstrar as circunstâncias do fato dado como criminoso - depois que se recorrer às provas para tal demonstração, pedir ao juiz que envie à jurisdição estrangeira (exigido no Canadá - o juiz canadense decide se pode e em que condições mandar as provas)

Quem pode solicitar Assistência Mútua baseada em Tratado? Qualquer autoridade competente (policial, promotor/procurador, juiz) conforme definido no MLAT

Apresentação da Argentina – Professor Marcos Salt, da Universidade de Buenos Aires, Argentina

O Professor Marcos fez apresentação relacionada à cooperação entre setor publico e privado em matéria cibernética - necessidade da existência

de um guia comum entre os países, para não se deixar nas mãos do setor privado o que será considerado como urgente ou não. Estes "guidelines" devem ser feitos pela OEA segundo o Professor.

Observou que os crimes digitais hoje abrangem três formas: os que envolvem o ataque a sistema informático propriamente dito; os crimes comuns cometidos pela internet e os que não são cometidos pela internet mas deixam evidências/provas em computadores. E neste ponto, torna-se mais imprescindível que nunca que o setor público com o privado trabalhem juntos e em cooperação – é preciso de um sistema integrado de cooperação, em nível de OEA e não de país por país.

Ressaltou ainda que a violação ao direito à intimidade é uma desculpa que algums Estados apresentam para não fornecer as provas digitais – na sua visão o equilíbrio entre eficiência da prova e garantismo no mundo digital vai ser palco de muita discussão ainda.

Ele acredita que a Convenção de Budapeste é o caminho/pode vir a ser este "guideline" - para ele, a adesão do país à Convenção deveria ser um marco da reunião nesta VII Reunião da REMJA na OEA para que haja uma justiça globalizada, cooperação igualitária e ferramentas fortes de investigação em nível global. Propôs a assinatura em bloco de todos os países da OEA à Convenção de Budapeste.

Houve intervenção do Brasil através de Diogo Machado, funcionário do Ministério da Justiça (órgão que atrua no Brasil como autoridade central), o qual prestou esclarecimentos sobre a situação do Brasil em relação à cooperação jurídica internacional, conforme os dados abaixo:

Alemanha – 1 pedido ativo em andamento
Argentina – 1 pedido passivo em andamento
Canadá – 1 pedido ativo em andamento
EUA – 40 pedidos, todos ativos
31 em andamento
5 totalmente cumpridos
4 não cumpridos
Holanda – 1 pedido ativo em andamento
Itália – 1 pedido passivo em andamento
Japão – 1 pedido passivo em andamento
Reino Unido – 1 pedido passivo cumprido totalmente
Suíça – 1 pedido passivo em andamento

Total de pedidos: 48

Ativos: 43 (quase 90%)

Passivos: 5 (10%)
Cumpridos: 6
Em andamento: 38
Não cumpridos: 4

Dos pedidos passivos, 4 estão em andamento e 1 foi cumprido.

Em termos proporcionais, o Brasil é país demandante da cooperação jurídica internacional para persecução do crime cibernético.

Principais instrumentos multilaterais que balizam a cooperação internacional brasileira em crime cibernético: Convenção das Nações Unidas contra a Corrupção – Convenção de Mérida; a Convenção das Nações Unidas contra o Crime Organizado Transnacional – Convenção de Palermo; a Convenção sobre o Combate da Corrupção de Funcionários Públicos Estrangeiros em Transações Comerciais Internacionais – OCDE; e o Protocolo de Assistência Jurídica Mútua em Assuntos Penais do Mercosul: Argentina, Uruguai e Paraguai.

17 Acordos de cooperação jurídica internacional em matéria penal (instrumentos bilaterais): Canadá, China, Colômbia, Coréia do Sul, Cuba, Espanha, Estados Unidos da América, França, Itália, México, Nigéria, Panamá, Peru, Portugal, Suíça, Suriname e Ucrânia. 3 acordos aguardam promulgação (Angola, Honduras e Líbano). Outros 9 acordos já estão negociados e 22 estão em processo de negociação.

Em seguida, a Delegação do Paraguai formulou questionamento a respeito do funcionamento da cooperação internacional indagando que o tempo de 90 dias de preservação que for a mencionado, começa a contar de que data? Em resposta, foi dito que a partir do momento em que chega a informação ao provedor. Mencionou-se ainda na resposta que se o país for membro da rede 24/7, cerca de 20 minutos a 01 (uma) hora depois da solicitação a informação já está preservada por 90 dias e esta evidência é gravada em uma forma digital (cd ou memória), esperando que chegue uma solicitação formal, e assim seja originada uma ordem judicial para que a prova preservada seja entregue, com a garantia de que esta prova se encontra da mesma forma que no dia em que foi solicitada a preservação.

O Presidente da OEA mencionou que no projeto de recomendação n. 16 (da VI Reunião) se faz referência à coordenação da OEA para programa de capacitação para todos os participantes/membros – JAMES VIGIL.

11 h às 12h30 - Desdobramentos nacionais recentes em matéria de delito

cibernético. Apresentação a cargo de Nayra Fernanddez Ruiz, Procuradora (Fiscal) Especializada em Delitos contra Propriedade Intelectual e Segurança Informática do Panamá e ***Delegação do Brasil através do Dr. Carlos Eduardo Miguel Sobral, Delegado da Polícia Federal Chefe da Delegacia Especializada em Crimes Cibernéticos no Brasil****; outros Estados membros.*

Após houve a apresentação Panamá pela Procuradora responsável pelo combate aos Delitos Cibernéticos naquele país:

- Deve-se distinguir que existem no âmbito cibernético: Delitos informáticos e delitos que são cometidos por meio informáticos e às vezes a legislação do país não esclarece isso

- Diagnostico do Panamá – atualmente possui três artigos legais (arts. 289, 290 e 291). sobre delitos cibernéticos - há previsão de pornografia infantil, inviolabilidade de segredo; revelação de segredos empresariais; estafa (manipulação de programas, etc) – portanto o diagnóstico é no sentido de que há muito mais a abranger (no Panamá o MP ficou com a tarefa de preparar um projeto de lei, no ponto de vista penal e tb administrativo na área de informática)

- Avanços tecnológicos devem se amparados por leis, temos que fazer uma troca de estrutura judicial quando preciso. A prova digital deve ter um tratamento especial (no ano de 2011 houve 29 investigações a envolvendo delito cibernético, no entanto há apenas 5 peritos no país inteiro - por isso precisa se implementar a cooperação).

- Apoio da OEA, ONU e outros organismos que percebem que o Panamá quer contribuir no combate aos crimes cibernéticos e atualizar sua legislação.

Encerrada a apresentação do Panamá, **o DPF Dr. Carlos E. Miguel Sobral apresentou exposição sobre a *PERSPECTIVA BRASILEIRA PARA COMBATE AO CRIME CIBERNETICO E A SEGURANÇA CIBERNETICO,*** cuja palestra na íntegra/power point consta como anexo, no **DOC.6.**

Durante a palestra, o Dr. Sobral abriu a palavra ao Ministério Público Federal para falar a respeito do trabalho de prevenção realizado no Brasil em Crimes Cibernéticos, quando então houve a Procuradora da República Neide Cardoso de Oliveira discorreu sobre prevenção e prática de crimes cibernéticos, narrando a experiência exitosa de realização de Oficinas, oferecidas pelo MPF em parceria com a ONG SaferNet Brasil, sobre o "Uso Consciente e Seguro da Internet" para as escolas públicas e particulares nos Estados do RJ, SP, PR, PA, MT e PB. Conforme texto lido a seguir:

"Por entender que só a repressão é insuficiente e que a prevenção é o melhor caminho a seguir na conscientização das pessoas, o Ministério Público Federal em parceria com os Ministérios Públicos Estaduais e a ONG SaferNet Brasil tem promovido Oficinas sobre o "Uso Responsável e Seguro da Internet" dirigidas a educadores das redes públicas e particular de ensino dos Estados do RJ e São Paulo. A iniciativa também já ocorreu em Cidades como Curitiba/PR, Belém/PA, Cuiabá/MT e João Pessoa/PB. Nessas Oficinas são entregues materiais pedagógicos para que os professores introduzam o assunto nas salas de aula. A escola foi o meio mais apropriado que encontramos para se tratar o assunto, muitas vezes negligenciado pelos pais.

Os principais riscos de navegar na Internet incluem o aliciamento online, a difusão de imagens pornográficas de crianças ou adolescentes (muitas geradas pelas próprias vítimas) e o cyberbulling. E tais riscos devem ser conhecidos pelas crianças e adolescentes para que aprendam como se prevenir, pois são as vítimas em potencial. "

12 h às 14 h - Intervalo

14h às 17h30 – ***Consideração, discussão e aprovação das Recomendações da VII Reunião do GT Crimes Cibernéticos da REMJA***

Inicialmente foi apresentada a Minuta de *Proposta* de Recomendações pelo Diretor de Coordenação Jurídica (**DOC. 7)**

O **diplomata brasileiro,** Luiz Marfil, leu a proposta de inclusão de um novo parágrafo a ser inserido logo após o parágrafo 11, pasando a figurar portanto como o novo parágrafo 12, renumerando-se os parágrafos subsequentes. Houve muita discussão acerca da inclusão e redação deste novo parágrafo, principalmente entre o Brasil, Canadá, EUA e Argentina, tendo participado das discussões as procuradoras da República presentes, o DPF Carlos Sobral e o funcionário do MJ, Diogo Monteiro, chegando-se ao final a uma redação conciliatória do novo parágrafo 12, que consta do texto de Recomendação aprovadas ao final da Reunião (**DOC. 8**)

Observamos que por sugestão do Brasil também foram alterados o parágrafo 6 (a Coordenação não deve se feita por intermédio da Secretaria Técnica das REMJA, e sim pela Resolução da Assembléia da ONU em conformidade com a Resolução de 2004); no parágrafo 8, alínea *d*, sugeriu-se que a palavra *persecução* deveria substituir *processamento*, mas após algumas argumentações, a expressão anterior prevaleceu por se concluir ser a melhor ("*investigação e processo*"); no parágrafo 13 o Brasil solicitou que quando da citação dos diversos organismos, por uma questão de hierarquia, as

Nações Unidas deveriam vir em primeiro lugar, seguida do Conselho da Europa e assim por diante. Por unanimidade, foram aprovadas as alterações.

17:30 h - Encerramento dos Trabalhos

MINISTÉRIO PÚBLICO FEDERAL
2ª Câmara de Coordenação e Revisão

Fls. 026

Da 2ª Câmara de Coordenação e Revisão
À Coordenadoria de Comunicações Administrativas

AUTUAÇÃO

De ordem da Sra. Coordenadora, remetam-se à DIAPA/CCA para a devida autuação.

Após, retornem-se para a respectiva distribuição.

Brasília, 05 março de 2012.

Ocineide Firmino Araujo
Secretaria da 2ª CCR

MINISTÉRIO PÚBLICO FEDERAL
COORDENADORIA DE COMUNICAÇÕES ADMINISTRATIVAS
DIVISÃO DE AUTUAÇÃO E PROCESSAMENTO ADMINISTRATIVO

Processo PGR/MPF Nº 1.00.000.002746/2012-44

Autuado com 27 (vinte e sete) folhas, incluindo esta, encaminhe-se à Segunda Câmara de Coordenação e Revisão do MPF, conforme despacho de folha retro.

CCA/DIAPA, em 05/03/12

Sandra Florentino da Silva
Chefe da Divisão de Autuação e Processamento Administrativo

Despacho

1. Ciente do relatório.
2. Inclua-o, em meio eletrônico, na página da 2ª Câmara.

04/5/12