



PROCURADORIA GERAL DA REPUBLICA

Data de 10/02/2014

CRIMINAL

Procedimento Administrativo - PA

1.00.000.002205/2014-88

Capa:

Relatório sobre a participação na conferência Octopus, de 4 a 6 de dezembro de 2013, em Estrasburgo, França.

Partes:

INTERESSADO - PR-SP - PR-SP - PROCURADORIA DA REPUBLICA - SAO PAULO

Câmara:

2ª Câmara - Criminal e Controle Externo da Atividade Policial

Tema:

DIREITO PENAL,



MINISTÉRIO PÚBLICO FEDERAL
PROCURADORIA DA REPÚBLICA EM SÃO PAULO

Ofício PR/SP-GABPR28MGBAS- nº 21.944/2013

Etiqueta: 84.529/2013

São Paulo, 19 de dezembro de 2013.

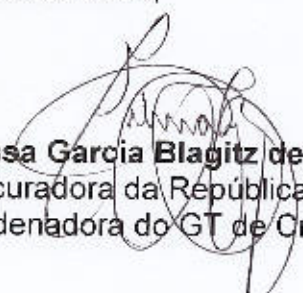
DESPACHO 005

Exma. Sra. Coordenadora

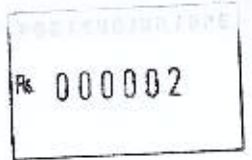
1. Intuar.
2. Ao relator do tema
na 2ª Câmara, o DR
Oswaldo Silva, membro titular.
Brasília, 07 de 02, 2014.
Rafael Costa

Encaminho a Vossa Excelência relatório sobre a participação na Conferência Octopus, de 4 a 6 de dezembro de 2013, em Estrasburgo, França.

Atenciosamente,


Melissa Garcia Blagitz de Abreu e Silva
Procuradora da República em São Paulo
Coordenadora do GT de Crimes Cibernéticos

À Exma. Subprocuradora-Geral da República
Raquel Elias Ferreira Dodge
Coordenadora da 2ª CCR
SAF/Sul - Q. 04 - Conj. C - Asa Sul
Brasília/DF - CEP 70050-900



MINISTÉRIO PÚBLICO FEDERAL
PROCURADORIA DA REPÚBLICA EM SÃO PAULO

Ofício

São Paulo, 19 de dezembro de 2013.

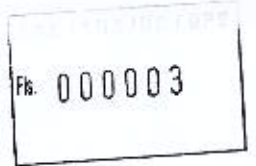
Exmo. Senhor Procurador-Geral,

As Procuradoras da República abaixo assinadas, autorizadas por Vossa Excelência e pelo Egrégio Conselho Superior do Ministério Público Federal a participar nos dias 4 a 6 de dezembro de 2013 da Conferência Octopus contra Cibercriminalidade, promovida pelo Conselho da Europa, vêm pelo presente apresentar relatório do evento, bem como conclusões sobre a participação do Ministério Público Federal.

Dia 4 de dezembro de 2012

A abertura do evento foi feita por *Thorbjorn Jagland*, Secretário-Geral do Conselho da Europa, que destacou os avanços dos últimos anos, não apenas no número de países que aderiram à Convenção de Budapeste, mas também no número de países que a utilizam como marco, mesmo sem adesão formal. Afirmou que a luta contra os crimes cibernéticos não pode desrespeitar os Direitos Humanos, em clara referência aos problemas criados pela revelação dos casos de espionagem comandados pelos Estados Unidos.

Foram feitos breves relatos com atualizações dos fatos ocorridos desde a última conferência, em junho do ano passado, incluindo informações sobre os países que aderiram à Convenção de Budapeste.



MINISTÉRIO PÚBLICO FEDERAL
PROCURADORIA DA REPÚBLICA EM SÃO PAULO

Foram ouvidos relatos da Áustria e da Romênia, tendo este último enfatizado o apoio recebido do Conselho da Europa para a implementação da Convenção de Budapeste.

Em seguida, foram feitos relatos sobre os desafios para 2014. Houve explanação da Rússia (*Group IB* – empresa privada especializada em segurança cibernética), sobre as principais ameaças e fraudes verificadas naquele país em 2013. Foi ressaltado pelos especialistas que, cada vez mais, é perceptível a colaboração entre criminosos de diversos países, o que exige aumento da cooperação entre autoridades responsáveis pela persecução penal dos crimes.

A Coreia do Sul expôs detalhes sobre a Conferência sobre Cyberspace, realizada em Seul, em outubro de 2013, com um mil e oitocentos participantes de oitenta e sete países. O escopo dessa conferência foi bem amplo, com discussões que abrangeram desde economia a benefícios culturais e sociais da rede, passando por crimes e segurança cibernética.

A empresa *Microsoft* enfatizou que, após a quebra de confiança provocada pelas ações da *National Security Agency* - NSA, dos Estados Unidos, as empresas privadas estão investindo na segurança dos usuários.

Por fim, o Deputado Federal Eduardo Azeredo apresentou breve exposição sobre a situação legislativa no Brasil, incluindo as Leis nº 12.737¹ e 12.735², ambas de 2012.

Na terceira seção do período da manhã do primeiro dia, foram expostas ações para a implementação da Budapeste. Enfatizou-se a

1 http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm

2 http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12735.htm



MINISTÉRIO PÚBLICO FEDERAL
PROCURADORIA DA REPÚBLICA EM SÃO PAULO

necessidade de se aprimorar o acesso transfronteiriço (discussão mais detalhada em item próprio, abaixo) e as ações realizadas na África, que tem recebido constante auxílio do Conselho da Europa.

No período da tarde foram realizadas quatro seções, que podem ser assim resumidas:

I – Workshop 1: Policies, activities and initiatives on cybercrime of international organizations

Exposição da *Interpol* sobre os problemas encontrados para a investigação de crimes cibernéticos. Foi destacado que esses crimes têm como característica principal a não obediência a fronteiras, o que dificulta o trabalho das polícias locais e mesmo da *Interpol*. É necessário, com urgência, harmonizar as legislações, para facilitar a atuação policial (hoje, além de se preocupar com a investigação, o policial precisar verificar a legislação de vários países para apurar se elas criminalizam ou não a conduta e como podem ajudar).

Descreveu-se o funcionamento da rede 24/7 e sua utilização na rápida comunicação entre autoridades de países diferentes para a obtenção de provas e troca de informações.

II – Workshop 2: Cybercrime legislation in the Asia/Pacific region

Foram descritos os avanços e os desafios. Há grande interesse por parte do Conselho da Europa de que outros países, além do Japão, também ratifiquem a Convenção de Budapeste. O Japão, forte personagem da região, tem aportado dinheiro para a implementação da Convenção e tem claro interesse na adesão de outros países da região.

III – Working Group: Cybercrime legislation in Latin America

Após uma breve exposição sobre a convenção e sobre a Lei 109/2009 de Portugal³, que não apenas incluiu dispositivos da Convenção de

³ http://www.enpd.pt/bin/legis/nacional/LEI109_2009_CIBERCRIME.pdf



Fb 000005

MINISTÉRIO PÚBLICO FEDERAL
PROCURADORIA DA REPÚBLICA EM SÃO PAULO

Budapeste, como foi além em diversas previsões, cada país presente foi chamado a fazer uma pequena exposição.

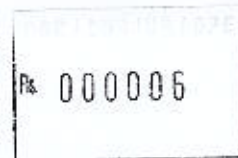
O Brasil, representado pelas colegas Melissa e Adriana, fez uma breve exposição comparando o capítulo de Crimes Cibernéticos do projeto de Código Penal de relatoria do Senador Pedro Taques⁴, com os dispositivos da Convenção, identificando pontos de contato e outros em que a legislação proposta é mais avançada.

Importante relatar que, nessa seção, um advogado de São Paulo, que possui escritório especializado em responsabilização civil por danos morais, que não atua com crimes cibernéticos e nem possui qualquer tipo de ligação com o setor público, mas há anos, em razão da ausência de acompanhamento próximo das autoridades brasileiras em eventos dessa natureza, tem se apresentado como representante do Brasil, tomou a palavra para fazer exposição desconexa, como se fosse oficial. O mal estar gerado por sua postura foi contornado ao final da sessão, com pedidos de desculpas formais dos organizadores, que somente então tomaram conhecimento de que tal profissional não representa o Brasil e não está habilitado, por absoluta falta de conhecimento e de ligação com as autoridades competentes, a falar em nome do país.

Nessa seção foi exposta proposta de convênio apresentada pela COMJIB – Conferência de Ministros da Justiça dos países Iberoamericanos (documentos em anexo). Não se trata de uma convenção, mas de documento que prevê auxílio e colaboração para a persecução penal de crimes cibernéticos, incluindo mecanismos mais ágeis de cooperação internacional e de troca de provas e informações. A proposta de convênio é acompanhada de sugestão para a tipificação de crimes cibernéticos, em sintonia com a Convenção de Budapeste e também com os delitos tipificados no Projeto de Código Penal já mencionado.

Como instrumento de cooperação entre países, entendemos que a proposta de convênio é útil para a repressão de crimes cibernéticos e

4 <http://www12.senado.gov.br/noticias/Arquivos/2013/08/veja-a-integra-do-relatorio>



MINISTÉRIO PÚBLICO FEDERAL
PROCURADORIA DA REPÚBLICA EM SÃO PAULO

sugerimos que a Procuradoria-Geral da República se posicione favoravelmente à assinatura do documento pelo Exmo. Ministro da Justiça.

IV – Working Group: Updating Electronic Evidence Guide and training materials

Seção voltada para a apresentação de material de treinamento voltado a Juízes e Promotores.

Após exposição sobre a necessidade de constante atualização e sobre as falhas de compreensão do tema crimes cibernéticos e provas informatizadas por Promotores e Juízes, em especial estes últimos, foi apresentado guia elaborado a pedido do Conselho da Europa e voltado para a capacitação de autoridades.

O guia, elaborado por professores e especialistas do Reino Unido, da Alemanha e da Sérvia, está disponível, em versão resumida, no endereço eletrônico do Conselho da Europa⁵. A colega Priscila, que participou dessa seção e de sua continuação na manhã do dia 5 de dezembro, obteve cópia integral do guia, que ficará à disposição no Núcleo Técnico de Combate a Crimes Cibernéticos da Procuradoria da República em São Paulo, único do país destinado ao apoio técnico desse tipo de investigação.

Dia 5 de dezembro de 2012

No período da manhã foram realizados dois *workshops*, além da continuação do *working group* sobre prova informatizada mencionada no item anterior.

V – Workshop 3: Capacity building on cybercrime: good practices, success stories, lessons learnt and upcoming programmes

Nesta seção foi destacada a natureza mutante dos crimes cibernéticos, a necessidade de constante aprimoramento e treinamento das

⁵ http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Electronic%20Evidence%20Guide/2467_FFG_v18_short.pdf



MINISTÉRIO PÚBLICO FEDERAL
PROCURADORIA DA REPÚBLICA EM SÃO PAULO

autoridades responsáveis pela repressão. Enfatizou-se a necessidade de conjugar esforços com o setor privado.

Em período de abalo da confiança mundial com o escândalo de espionagem envolvendo os Estados Unidos e outros países, criticou-se os efeitos negativos que tais revelações tiveram na cooperação entre países. Crimes cibernéticos são, em regra, internacionais e precisam ser combatidos de forma global, fortalecendo-se os laços de confiança entre os países.

VI – Workshop 4: Transborder access to data

Esta seção teve por objetivo avançar nas discussões para aperfeiçoamento do artigo 32 da Convenção de Budapeste⁶ que cuida do acesso transfronteiriço. Esse artigo tem sido objeto de forte resistência por alguns países, como Rússia, que se recusou a aderir à Convenção principalmente em razão dessa previsão, mas é considerado essencial para o adequado enfrentamento dos crimes cibernéticos por autoridades de diversos outros países.

Foi novamente exposta a legislação portuguesa, que contém previsões mais avançadas e que permitem acesso maior à prova armazenada em outros países do que a própria convenção.

Também foi exposto que a maioria dos pedidos de cooperação entre países envolve o simples fornecimento de *logs* de acesso (endereço IP com data e hora), questionando-se se para medida tão simples não poderia ser encontrado mecanismos mais célere, talvez até mesmo automatizado de cooperação.

Professores universitários presentes à seção levantaram questionamentos sobre a proteção da intimidade, nos termos da Convenção 108

6 Artigo 32 – Acesso transfronteiriço a dados informáticos armazenados, com consentimento ou quando são acessíveis ao público

Uma Parte pode, sem autorização de outra Parte:

a) Aceder a dados informáticos armazenados acessíveis ao público (fonte aberta), seja qual for a localização geográfica desses dados; ou

b) aceder ou receber, através de um sistema informático situado no seu território, dados informáticos armazenados situados no território de outra Parte, se obtiver o consentimento legal e voluntário da pessoa legalmente autorizada a divulgar esses dados, através deste sistema informático.



MINISTÉRIO PÚBLICO FEDERAL
PROCURADORIA DA REPÚBLICA EM SÃO PAULO

do Conselho da Europa⁷, novamente tendo em vista a divulgação dos atos de vigilância dos Estados Unidos. Alertou-se que, embora a legislação americana diferencie nacionais e estrangeiros para fins de acesso a dados, permitindo, para o segundo grupo, que autoridades tenham acesso praticamente irrestrito, essa diferenciação não é reconhecida pelas convenções internacionais.

Foram expostas as dificuldades crescentes enfrentadas pela atualmente quase impossível identificação do local de armazenamento da prova (*cloud computing*) e a necessidade urgente de se encontrar alternativa, sendo sugerido que seja considerado o local de residência da pessoa com disponibilidade sobre o dado (algo semelhante ao utilizado no Brasil, que por força do artigo 88 do Código de Processo Civil, considera submetida à jurisdição brasileira as pessoas jurídicas aqui constituídas, incluindo aí provedores estrangeiros com filiais locais).

Ao final, concluiu-se pela necessidade urgente de ampliação das previsões do citado artigo 32, com a exclusão do conceito de consenso, considerado redundante e desnecessários. Qualquer nova previsão deverá observar as salvaguardas na obtenção de dados, seja ao direito à intimidade seja à soberania de cada país, incluindo naquelas a possibilidade de comunicação posterior ao país onde o dado está, garantindo-se a preservação e a rápida obtenção, com formalidades posteriores.

No período da tarde, foram realizadas outras três seções:

VI – Workshop 5: Protecting children against online sexual exploitation: legislation and law enforcement challenges

Nessa seção foi exposta rapidamente a Convenção de Lanzarote do Conselho da Europa⁸, de 2007, que define crimes relacionados à exploração sexual de crianças e adolescentes.

⁷ <http://www.cnpd.pt/bin/legis/internacional/Convencao108.htm>

⁸ http://www.coe.int/t/dghl/standardsetting/children/Source/LanzaroteConvention_por.pdf



MINISTÉRIO PÚBLICO FEDERAL
PROCURADORIA DA REPÚBLICA EM SÃO PAULO

Houve apresentações por organismos e entidades internacionais voltados à proteção de crianças, como a ECPAT⁹, que possui agência no Brasil, na cidade do Rio de Janeiro, e desenvolve projetos contra a prostituição infantil e a pornografia infantil.

Discutiu-se o aumento de casos em que o abuso de crianças é transmitido ao vivo pela rede mundial de computadores (*live stream*) e a dificuldade de coibir esse tipo de conduta, muitas vezes incentivada pela própria família, que explora a criança com transmissões de dentro de casa. Igualmente, há dificuldade na punição a esse tipo de visualização, considerando que a maior parte das legislações não pune o acesso, mas apenas a posse ou a redistribuição de material pornográfico (na situação descrita, punir-se-ia os autores da transmissão, mas não as pessoas que acessam o material e pagam por ele, já que as imagens não ficam armazenadas em nenhum lugar).

Houve exposição sobre o caso *Sweetie*, criança criada digitalmente pela organização holandesa *Terre des Hommes* e que era utilizada como isca para atrair abusadores interessados em exposição por meio de *live stream*¹⁰. Em cerca de seis semanas de experiência, foram identificados **um mil** abusadores, de oitenta e sete países diferentes.

Criticou-se, em parte, a iniciativa, pois a utilização de simulação poderia dificultar a punição dos abusadores. Entretanto, pelos autores da iniciativa foi enfatizado que o objetivo era demonstrar como é fácil identificar abusadores e como é necessária postura pró-ativa das autoridades: buscar os responsáveis ao invés de esperar tomar conhecimento dos fatos por outros meios.

VII – Workshop 6: International cooperation: data preservation workshop for 24/7 points of contact and MLA authorities

⁹ <http://www.ecpat.net/>

¹⁰ <http://www.publico.pt/sociedade/noticia/sweetie-a-menina-virtual-que-ajudou-a-encontrar-predadores-sexuais-na-internet-1611401>



MINISTÉRIO PÚBLICO FEDERAL
PROCURADORIA DA REPÚBLICA EM SÃO PAULO

Nesta seção, fechada a policiais e autoridades responsáveis pelo cumprimento de tratados de cooperação, foram feitas três apresentações, da Romênia, dos Estados Unidos e da República Dominicana sobre o funcionamento da Rede 24/7, prevista na Convenção de Budapeste¹¹. Foram discutidas medidas para o aprimoramento da rede, incluindo:

- a designação de um especialista em crime cibernético como ponto de contato e não apenas de um policial; e
- a melhoria dos canais de coordenação e dos canais informais de cooperação.

Sugeriu-se que fosse permitido, quando possível, o contato direto entre a polícia de um país e os provedores de outros, bem como a implementação de um protocolo básico de pedidos de auxílio, de modo a evitar a falta de cumprimento em razão de falhas no pedido.

VIII – Working group: Joint EU/COE project “Global Action on Cybercrime” (GLACY)

Nessa seção foi apresentado o projeto GLACY, coordenado pelo Conselho da Europa e cujo objetivo é colher informações precisas junto aos países que necessitam de ajuda no combate a crimes cibernéticos, repassar esses dados ao Conselho e, a partir daí, elaborar estratégias para melhorias, incluindo treinamentos apropriados.

11 Artigo 35 – Rede 24/7

1. Cada Parte designará um ponto de contato disponível 24 horas sobre 24 horas, 7 dias por semana, a fim de assegurar a prestação de assistência imediata a investigações ou procedimentos respeitantes a infrações penais relacionadas com dados e sistemas informáticos, ou a fim de recolher provas, sob forma eletrônica, de uma infração penal. O auxílio incluirá a facilitação, ou se o direito e práticas internas o permitirem, a aplicação direta das seguintes medidas:

- a) A prestação de aconselhamento técnico;
- b) A conservação de dados em conformidade com os artigos 29 e 30; e
- c) A recolha de provas, informações de caráter jurídico e localização de suspeitos.

2. a) O ponto de contato de uma Parte deve ter capacidade técnica para corresponder-se com o ponto de contato de outra Parte de uma forma rápida;

b) Se o ponto de contato designado por uma Parte não depender da autoridade ou autoridades dessa Parte responsáveis pela cooperação internacional ou extradição dessa Parte, o ponto de contato assegurará que pode agir em coordenação com essa ou essas autoridades de forma rápida.

3. Cada Parte assegurará que pode dispor de pessoal formado e equipado a fim de facilitar o funcionamento da rede.



MINISTÉRIO PÚBLICO FEDERAL
PROCURADORIA DA REPÚBLICA EM SÃO PAULO

Fs 000011

Para 2014, foram selecionados os seguintes países para o projeto: Marrocos, Filipinas, Senegal, África do Sul e Ilhas Maurício, todos eles recentemente signatários da Convenção de Budapeste.

Dia 6 de dezembro de 2012

Na seção de encerramento, após breve exposição das conclusões dos diversos grupos e *workshops*, foram feitas apresentações sobre o tema Justiça Criminal *versus* Segurança Nacional.

As iniciativas de espionagem foram unanimemente criticadas, bem como o repasse das provas colhidas dessa forma, por mecanismos de "inteligência", não submetidos às salvaguardas do Devido Processo Legal, para a persecução penal de crimes. Defendeu-se a necessidade de alteração dos tratados para a inclusão de proteção específica a dados de cidadãos, independente da nacionalidade. O Conselho da Europa, hoje, busca soluções práticas imediatas para a questão, tendo em vista que cidadãos europeus, considerados "estrangeiros" pela legislação americana, são alvo frequente da iniciativa.

Ao final, foram chamados representantes das Filipinas, do Quênia, e a colega Melissa como representante do Brasil para o fechamento da conferência, sendo feita breve exposição sobre a posição brasileira, sobre nossos avanços na matéria e sobre a Conferência¹².

¹² "Obrigada por estarmos de novo aqui. Essas duas edições da Conferência Octopus (2012/2013) foram uma grande oportunidade para nós compartilharmos conhecimento, impressões, e também para nos comunicarmos mundialmente com aqueles que trabalham com o tema.

Embora o Brasil não tenha até agora ratificado a Convenção de Budapeste, há tempos que tentamos trabalhar e propor leis baseadas nos princípios, finalidades e fundamentos da referida Convenção, que é, indubitavelmente, um documento primordial e orientador no combate à cibercriminalidade.

Atualmente o Brasil tem duas propostas de leis sobre o tema. É certo que o marco civil da internet (primeira proposta) tem problemas no seu conteúdo e elaboração por se tratar de uma legislação cujas definições advêm da área técnica. Entretanto, nosso Congresso tem adotado, louvavelmente, uma postura aberta a discussão, sobretudo dispondo-se a ouvir os expertos sobre o tema.

Além disso, há um novo Código Penal em votação que contém um capítulo exclusivo para definir cibercriminalidade e tipos penais a ela correlatos. Estes novos tipos mais que transcreverem os conceitos da Convenção de Budapeste, adequam-na às necessidades dos dias atuais (diga-se hoje, diante da volatilidade do meio), o que, a toda evidência, representa um avanço do Brasil em relação aos demais países. O Capítulo dispõe sobre novos conceitos e ideias no intuito de abarcar as novas e futuras (breves) tecnologias.



MINISTÉRIO PÚBLICO FEDERAL
PROCURADORIA DA REPÚBLICA EM SÃO PAULO

Conclusões

Do exposto, percebe-se que a participação na conferência foi extremamente proveitosa e também esclarecedora, em especial após o episódio acima narrado.

Além do fortalecimento dos contatos com organizações internacionais, membros dos Ministérios Públicos de outros países, e pessoas responsáveis pela cooperação internacional em alguns países, a intervenção do Ministério Público Federal foi crucial para esclarecer a posição do Brasil, informar sobre os avanços do país, inclusive em projetos de lei, e também sobre os procedimentos do Ministério Público Federal, que por conta própria tem mantido iniciativas visando o treinamento de promotores e juízes para a investigação e processamento dos crimes cibernéticos, como o recém-publicado Roteiro de Atuação sobre Crimes Cibernéticos.

Por essas razões, e considerando a insistência de particulares em tomar para si a representação do país, é indispensável que o Ministério Público Federal continue participando desses eventos, de modo a integrar cada vez mais suas atividades de investigação com Ministérios Públicos estrangeiros, não deixando que suas atividades e conquistas fiquem desconhecidas e sejam deixadas em segundo plano, em benefício de iniciativas de escritório particular, não envolvido com a persecução penal de crimes cibernéticos. O Ministério Público Federal está atuando nos mesmos termos e

Para o futuro próximo, acreditamos que a aprovação dessas duas legislações nos levará a desenvolvimento não só interno, mas principalmente à criação de instrumentos de mão dupla, únicos e hábeis para o bom desenvolvimento de uma rede de comunicação internacional, imprescindível para o sucesso desse tipo de investigação. Frisamos que para isso, é imperioso a harmonização das legislações de todos os Países. Para terminar, reiteramos que os Procuradores da República do Brasil estão e estarão sempre abertos a novas ideias e instrumento com o fim de atingirmos esse desiderato e sempre estaremos abertos para ajudar todos os Países que necessitem da cooperação do Brasil em suas investigações."



MINISTÉRIO PÚBLICO FEDERAL
PROCURADORIA DA REPÚBLICA EM SÃO PAULO

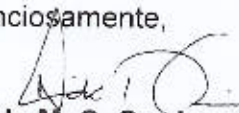
condições dos países europeus, na vanguarda da atividade, e o seu espaço precisa ser respeitado e reconhecido.

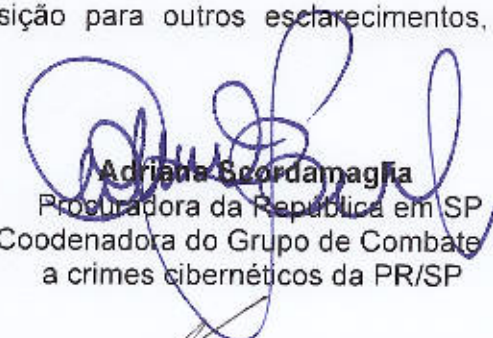
Para a continuidade das atividades e aprofundamento das discussões, sugerimos as seguintes medidas:

- 1- Aprofundamento dos contatos com os grupos responsáveis pela elaboração de material de treinamento, não apenas para a troca de informações, como também para o aprimoramento dos instrumentos já elaborados pela instituição, como o Roteiro de Combate a Crimes Cibernéticos, publicado pela 2ª Câmara de Coordenação e Revisão, já citado;
- 2- Posicionamento favorável à assinatura, pelo Exmo. Sr. Ministro da Justiça, do convênio proposto pela COMJIB;
- 3- Estreitamento dos laços com membros do Ministério Público dos países iberoamericanos, em razão da crescente necessidade de cooperação para a apuração de crimes cibernéticos.

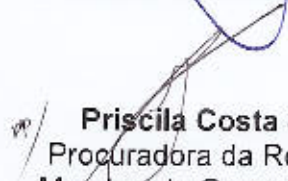
Informamos que além do presente relatório, há texto maior, de cerca de cinquenta laudas, contendo todas as anotações feitas nas diversas seções, que pode ser encaminhado aos colegas que tiverem interesse.

Colocando-nos à disposição para outros esclarecimentos, atenciosamente,


Neide M. C. Cardoso de Oliveira
Procuradora Regional da República
Coordenadora-adjunta do GT de
Crimes Cibernéticos da 2ª CCR


Adriana Scordamaglia
Procuradora da República em SP
Coordenadora do Grupo de Combate
a crimes cibernéticos da PR/SP


Melissa Garcia Blagitz de Abreu e Silva
Procuradora da República em São Paulo
Coordenadora de GT de Crimes
Cibernéticos da 2ª CCR


Priscila Costa Schreiner
Procuradora da República em SP
Membro do Grupo de Combate a
crimes cibernéticos da PR/SP

SECRETARÍA GENERAL

CONFERENCIA DE MINISTROS DE
JUSTICIA DE LOS PAÍSES
IBEROAMERICANOS**RECOMENDACIÓN DE LA CONFERENCIA DE MINISTROS DE JUSTICIA DE
LOS PAÍSES IBEROAMERICANOS (COMJIB) RELATIVA A LA TIPIFICACIÓN Y
SANCIÓN DE LA CIBERDELINCUENCIA**

Los Ministros de Justicia y representantes de los Estados Iberoamericanos reunidos en... los días..., con motivo de la Reunión Plenaria de la Conferencia de Ministros de Justicia de los Países de Iberoamérica,

VISTO el artículo 3º, apartado c), del Tratado constitutivo de la Conferencia de Ministros de Justicia de los Países Iberoamericanos del 7 de octubre de 1992;

RECORDANDO los valiosos intercambios técnicos y político criminales llevados a cabo en el marco del Seminario Iberoamericano sobre Ciberdelito desarrollado los días 6 y 7 de septiembre de 2011 en la ciudad de Buenos Aires; en la reunión del Grupo de trabajo sobre "Delincuencia Organizada Transnacional y Cooperación Jurídica Internacional" del 8 y 9 de septiembre de 2011 en la misma ciudad; en los talleres convocados en Montevideo del día 17 al 19 de septiembre de 2012, y en Madrid del 4 al 6 de febrero de 2013; en la reunión de coordinadores llevada a cabo en Bogotá el 4 y 5 de marzo de 2013, y en el taller desarrollado en Lima los días 24, 25 y 26 de junio de 2013.

TENIENDO PRESENTE que en la Comisión Delegada de la COMJIB celebrada en Río de Janeiro el día 23 de marzo de 2012 se aprobó una importante "Declaración sobre el ciberdelito" en la que se acordó: "respaldar los primeros pasos que se han dado en la línea de lucha contra la delincuencia organizada para iniciar el debate sobre la elaboración y firma de un documento internacional iberoamericano, capaz de dar respuesta a las necesidades arriba referidas, e impulsar la modificación de las legislaciones penales de manera armonizada". Razón por la cual se dictaron unas líneas generales "con la finalidad de concretar un borrador de Convenio Iberoamericano para regular el Ciberdelito".

ATENDIENDO a que en la Plenaria llevada a cabo en Viña del Mar se acordó, sobre el borrador aportado, elaborar un Convenio Iberoamericano sobre cooperación, prueba, jurisdicción y competencia en materia de ciberdelincuencia, así como una Recomendación que albergaría los principios relativos a los aspectos sustantivos que deberían encontrar acomodo en las legislaciones nacionales.

SIGNIFICANDO que en Viña del Mar se acordó, también, convocar un taller para terminar "de definir el contenido final" de los dos documentos acabados de referir, con el objetivo de elevar, para su firma, los dichos textos a la Cumbre Iberoamericana de Jefes de Estado y de Gobierno a celebrar en Panamá el próximo mes de octubre,

CONSIDERANDO, que buena parte de las legislaciones penales iberoamericanas tienen importantes carencias en los tipos penales referidos al ciberdelito, y que estas lagunas permiten tanto a la delincuencia individual como a la organizada lesionar o poner en

SECRETARÍA GENERAL

CONFERENCIA DE MINISTROS DE
JUSTICIA DE LOS PAÍSES
IBEROAMERICANOS

grave peligro a bienes jurídicos esenciales.

CONSCIENTES de que en otras regiones del mundo se han ido aprobando, o se está en trámite de hacerlo, Convenciones sobre ciberdelincuencia para una mejor protección de sus ciudadanos, lo que todavía no se ha efectuado en el ámbito iberoamericano.

MANTENIENDO el propósito de establecer criterios mínimos y comunes en la prevención y lucha contra el ciberdelito, y sin menoscabar los avances alcanzados en los respectivos ordenamientos jurídicos así como de las obligaciones internacionalmente asumidas por cada Estado,

CONVENCIDOS de que todos los esfuerzos para la prevención y lucha contra el cibercrimen son necesarios

ENTENDIENDO que la presente Recomendación debe estar abierta a futuros desarrollos y ampliaciones a nuevos delitos y mecanismos de cooperación.

MANIFESTANDO la voluntad de que la presente Recomendación resulte compatible con otros análogos, así como con reconocidas buenas prácticas en el ámbito internacional,

ENTENDIENDO CONVENIENTE, incorporar o, en su caso, armonizar, en el marco de las políticas criminales que cada país adopte en la materia, las legislaciones penales sustantivas nacionales en la tipificación de las conductas que más adelante se identificarán, a los efectos de buscar mayor eficacia en la prevención, persecución y, eventualmente, sanción de los dichos comportamientos, así como para facilitar la cooperación judicial entre los distintos países y tratar de impedir la existencia de espacios de impunidad.

RECOMIENDAN, en relación a las siguientes conductas

I. Acceso no autorizado a sistemas.

Tipificar como infracción penal el acceso no autorizado a un sistema informático siempre que se realice con vulneración de medidas de seguridad establecidas para impedirlo.

Considerar infracción penal el acceso a un sistema informático más allá de lo autorizado.

Podrá considerarse infracción penal agravada si los sistemas a los que se accede se refieren a estructuras o servicios esenciales para la comunidad.

II. Daños informáticos o atentados contra la integridad de los datos.

Tipificar como infracción penal cualquier acto consistente en introducir, borrar,

SECRETARÍA GENERAL



CONFERENCIA DE MINISTROS DE
JUSTICIA DE LOS PAÍSES
IBEROAMERICANOS

deteriorar, alterar, suprimir o hacer inaccesibles de forma grave datos informáticos, realizado a través de las tecnologías de la información y de la comunicación,

Podrá considerarse infracción penal agravada si los atentados afectan a datos informáticos referidos a estructuras o servicios esenciales para la comunidad o si causan un grave daño económico.

III. Daños o Atentados contra la integridad o disponibilidad de los sistemas informáticos.

Tipificar como infracción penal la conducta realizada a través de las tecnologías de la información y de la comunicación consistente en la inutilización, total o parcial, de un sistema informático cuando impidiese el acceso al mismo o imposibilitase el desarrollo de alguno de sus servicios.

Podrá considerarse infracción penal agravada si los sistemas se refieren a estructuras o servicios esenciales para la comunidad o si se causa un grave daño económico.

IV. Abuso de dispositivos

Tipificar como infracción penal la fabricación, importación, venta, facilitación, obtención para su utilización, de dispositivos, incluidos los programas informáticos, así como contraseñas o códigos de acceso, específicamente destinados a la comisión del delito de acceso no autorizado a sistemas o del delito de daños a datos informáticos y daños a sistemas de información.

V. Conductas vinculadas a la pornografía infantil.

Tipificar como infracción penal:

- . a) La producción de pornografía infantil
- . b) La oferta o puesta a disposición de pornografía infantil
- . c) La difusión o transmisión de pornografía infantil
- . d) La adquisición para sí o para otro de pornografía infantil
- . e) La posesión de pornografía infantil
- . f) El acceso intencional a pornografía infantil por medio de las tecnologías de la información

VI. Propositiones a menores con fines sexuales por medios tecnológicos.

Tipificar como infracción penal la conducta realizada, a través de las tecnologías de la información y la comunicación, consistente en contactar con un menor que no haya

SECRETARÍA GENERAL

CONFERENCIA DE MINISTROS DE
JUSTICIA DE LOS PAÍSES
IBEROAMERICANOS

alcanzado la edad del consentimiento sexual para solicitar u obtener de él material pornográfico.

También será considerada infracción penal la conducta realizada a través de las tecnologías de la comunicación y la información consistente en contactar con un menor que no haya alcanzado la edad del consentimiento sexual para llevar a cabo actividades sexuales con él, cuando dicha proposición se haya concretado en actos materiales conducentes a dicho encuentro.

VII. Conductas relativas a la afectación de los derechos de propiedad intelectual

Tipificar como infracción penal la conducta realizada por medio de las Tecnologías de la Información y la Comunicación consistente en explotar ilícitamente o plagiar en todo o en parte, una obra literaria, artística o científica o la transformación, interpretación o ejecución artística de la misma, con ánimo de lucro y en perjuicio de tercero.

VIII. Difusión de mensajes con contenidos xenófobos, racistas o relativos a los crímenes contra la humanidad.

Tipificar como infracciones penales las siguientes conductas realizadas a través de las Tecnologías de la Información y Comunicación:

a) La incitación pública a la violencia o al odio mediante la difusión de escritos, imágenes u otros materiales, dirigidos contra un grupo de personas o un miembro de tal grupo, definido en relación con la raza, el color, la religión, el sexo, la orientación sexual, la identidad de género, la enfermedad o discapacidad, la ascendencia o el origen nacional o étnico.

b) La expresión o difusión de informaciones injuriosas referidas a grupos de personas, o miembros de las mismas, en relación con la raza, el color, la religión, el género, la orientación sexual, la enfermedad o discapacidad, la ascendencia o el origen nacional o étnico.

Podrá considerarse infracción penal agravada la apología pública, la negación o la trivialización flagrante de los crímenes de genocidio, crímenes de lesa humanidad y crímenes de guerra.

IX. Suplantación de identidad

Tipificar como infracción penal la conducta realizada por medio de las Tecnologías de la Información y la Comunicación y con ánimo defraudatorio consistente en suplantar

la identidad de una persona física o jurídica.

X. Estafa informática

Tipificar como infracción penal la conducta consistente en manipular el ingreso, procesamiento o resultado de los datos de un sistema de información, por medio de las Tecnologías de la Información y la Comunicación, y valiéndose de alguna operación informática, en perjuicio de tercero y con ánimo de lucro.

Podrá considerarse infracción penal agravada cualquiera de las siguientes:

- . a) Cuando se cometa contra estructuras o servicios esenciales para la comunidad o si se causa un grave daño económico.
- . b) Cuando el autor, por sus funciones asignadas o por ser encargado de administrar o dar soporte al sistema o red informática o telemática, tenga posibilidad de tener acceso a los mismos.

SECRETARÍA GENERAL

CONFERENCIA DE MINISTROS DE
JUSTICIA DE LOS PAÍSES
IBEROAMERICANOS

**CONVENIO IBEROAMERICANO DE COOPERACION
SOBRE INVESTIGACION, ASEGURAMIENTO Y
OBTENCION DE PRUEBA EN MATERIA DE
CIBERDELINCUENCIA**

Los Ministros de Justicia y representantes de los Estados Iberoamericanos reunidos en... los días..., con motivo de la Reunión Plenaria de la Conferencia de Ministros de Justicia de los Países de Iberoamérica,

VISTO el artículo 3º, apartado c), del Tratado constitutivo de la Conferencia de Ministros de Justicia de los Países Iberoamericanos del 7 de octubre de 1992;

RECORDANDO los valiosos intercambios técnicos y político criminales llevados a cabo en el marco del Seminario Iberoamericano sobre Cibercrimen desarrollado los días 6 y 7 de septiembre de 2011 en la ciudad de Buenos Aires; en la reunión del Grupo de trabajo sobre "Delincuencia Organizada Transnacional y Cooperación Jurídica Internacional" del 8 y 9 de septiembre de 2011 en la misma ciudad; en los talleres convocados en Montevideo del día 17 al 19 de septiembre de 2012, y en Madrid del 4 al 6 de febrero de 2013; en la reunión de coordinadores llevada a cabo en Bogotá el 4 y 5 de Marzo y en el taller desarrollado en Lima los días 24, 25 y 26 de junio de 2013.

TENIENDO PRESENTE que en la Comisión Delegada de la COMJIB celebrada en Río de Janeiro el día 23 de marzo de 2012 se aprobó una importante "Declaración sobre el ciberdelito" en la que se acordó: "respaldar los primeros pasos que se han dado en la línea de lucha contra la delincuencia organizada para iniciar el debate sobre la elaboración y firma de un documento internacional iberoamericano, capaz de dar respuesta a las necesidades arriba referidas, e impulsar la modificación de las legislaciones penales de manera armonizada". Razón por la cual se dictaron unas líneas generales "con la finalidad de concretar un borrador de Convenio Iberoamericano para regular el Ciberdelito".

SECRETARÍA GENERAL

CONFERENCIA DE MINISTROS DE
JUSTICIA DE LOS PAÍSES
IBEROAMERICANOS

ATENDIENDO a que en la Plenaria llevada a cabo en Viña del Mar se acordó, sobre el borrador aportado, elaborar un Convenio Iberoamericano sobre cooperación, prueba, jurisdicción y competencia en materia de ciberdelincuencia, así como una Recomendación que albergaría los principios relativos a los aspectos sustantivos que deberían encontrar acomodo en las legislaciones nacionales.

SIGNIFICANDO que en Viña del Mar se acordó, también, convocar un taller para terminar "de definir el contenido final" de los dos documentos acabados de referir, con el objetivo de elevar, para su firma, los dichos textos a la Cumbre Iberoamericana de Jefes de Estado y de Gobierno a celebrar en Panamá el próximo mes de octubre,

CONSIDERANDO, que las legislaciones procesales iberoamericanas deben avanzar de manera coordinada para lograr un desarrollo suficiente que permita afrontar con garantías la lucha contra la cibercriminalidad.

CONVENCIDOS de que todos los esfuerzos para la prevención y lucha contra el cibercrimen son necesarios

ENTENDIENDO que el presente instrumento debe estar abierto a futuros desarrollos y ampliaciones a nuevos delitos y mecanismos de cooperación.

MANIFESTANDO la voluntad de que el presente instrumento resulte compatible con otros análogos, así como con reconocidas buenas prácticas en el ámbito internacional,

MANTENIENDO el propósito de establecer criterios mínimos y comunes en la prevención y lucha contra el ciberdelito, y sin menoscabar los avances alcanzados en los respectivos ordenamientos jurídicos así como de las obligaciones internacionalmente asumidas por cada Estado,

Han convenido en lo siguiente:

SECRETARÍA GENERAL



CONFERENCIA DE MINISTROS DE
JUSTICIA DE LOS PAÍSES
IBEROAMERICANOS

Artículo 1

OBJETO Y ÁMBITO DE APLICACIÓN

El presente convenio tiene por objeto reforzar la cooperación mutua de los Estados Parte para la adopción de medidas de aseguramiento y obtención de pruebas para la lucha contra la ciberdelincuencia.

Artículo 2

DEFINICIONES

A efectos del presente Convenio:

1. Por "ciberdelincuencia" se entiende cualquier forma de criminalidad ejecutada en el ámbito de interacción social definido por el uso de las Tecnologías de la Información y la Comunicación.
2. Por "incautación y depósito de sistemas informáticos o soportes de almacenamiento de datos" se entiende su ocupación física y su aseguramiento por las autoridades.
3. Por "sellado, precinto y prohibición de uso de sistemas informáticos o soportes de almacenamiento de datos" se entiende su bloqueo absoluto o la imposibilidad de su utilización, incluida la congelación de sistemas virtuales.
4. Por "requerimiento de preservación inmediata de datos que se hallan en poder de terceros" se entiende la imposición a particulares o a entidades públicas o privadas del deber de conservación íntegra de información digital que obre en su poder o sobre la que tenga facultades de disposición.

SECRETARÍA GENERAL



CONFERENCIA DE MINISTROS DE
JUSTICIA DE LOS PAÍSES
IBEROAMERICANOS

5. Por "copia de datos" se entiende la reproducción exacta de la información digital recolectada por particulares, entidades públicas o privadas.

6. Por "intervención de comunicaciones a través de las tecnologías de la información y comunicación" se entiende la captación en tiempo real del contenido de dichas comunicaciones sin interrupción de las mismas, así como de los datos de tráfico anexos.

7. Por "obtención de datos de tráfico" se entiende la captación de las informaciones relativas al origen, destino, ruta, hora, fecha, tamaño y duración de una comunicación electrónica en tiempo real y con ocasión de su realización.

8. Por "acceso a sistemas de información" se entiende la entrada a dichos sistemas, incluyendo los accesos remotos.

9. Por "acceso a la información contenida en un dispositivo que permita el almacenamiento de datos" se entiende la extracción de la información contenida en dicho dispositivo.

10. Por "entrega de datos y archivos informáticos" se entiende la transferencia de informaciones y documentos en formato electrónico que obren en poder de particulares, entidades públicas o privadas.

Artículo 3

PRINCIPIO DE COOPERACIÓN MUTUA

1. En el ámbito de aplicación del presente Convenio los Estados Parte se comprometen a cumplir las solicitudes de cooperación formuladas por otro u otros Estados Parte.

2. El Estado requerido podrá negarse a satisfacer, total o parcialmente, la solicitud de cooperación cuando:

- a) Su realización pueda causar grave perjuicio a una investigación o enjuiciamiento en curso.
- b) Los hechos que fundamentan la solicitud de cooperación ya



hubieran sido enjuiciados o archivados de forma definitiva en este Estado.

- . c) El cumplimiento de la actividad de cooperación sea contrario a su derecho interno.
- . d) Entienda que se encuentran afectados su soberanía, seguridad, orden público u otro interés esencial.
- . e) La solicitud se refiera a una infracción que el estado requerido considera de naturaleza política o vinculada a una información de naturaleza política.
- . f) La conducta perseguida no esté contemplada como infracción penal en su ordenamiento.
- . g) Se infrinjan los términos del presente Convenio.

3. El Estado requerido deberá motivar razonadamente su negativa a cumplir la solicitud de cooperación. Esta respuesta podrá realizarse de modo reservado o, en su caso, limitado, cuando se considere que una explicación más detallada podría poner en grave riesgo la investigación o el enjuiciamiento en curso, sin perjuicio de que la justificación se complete con posterioridad.

Artículo 4

RESPETO DE LOS DERECHOS HUMANOS

En la solicitud o ejecución de actividades de cooperación, los Estados Parte serán absolutamente respetuosos con los derechos fundamentales de las personas en los términos previstos en los Tratados y Convenios Internacionales sobre Derechos Humanos.

Artículo 5

ACTIVIDADES DE COOPERACIÓN

1. Cuando, en el curso de la investigación o enjuiciamiento de un delito comprendido en el ámbito de aplicación de este Convenio, las autoridades competentes de un Estado Parte estimen necesaria la adopción de alguna de las medidas de

SECRETARÍA GENERAL

CONFERENCIA DE MINISTROS DE
JUSTICIA DE LOS PAÍSES
IBEROAMERICANOS

aseguramiento de prueba o la práctica de alguna de las diligencias de investigación enumeradas en los artículos 6 y 7 dentro del territorio de otro Estado Parte, podrán solicitar a las autoridades competentes de este último su realización de acuerdo con el procedimiento establecido en el presente Convenio.

2. Los Estados Parte se comprometen a impulsar las iniciativas legislativas y aquellas otras que fueran necesarias para regular en sus ordenamientos internos las actuaciones mencionadas en los artículos 6 y 7.

Artículo 6

MEDIDAS DE ASEGURAMIENTO

Sin perjuicio de cualesquiera otras medidas de aseguramiento que pudieran contribuir a la persecución efectiva de los delitos comprendidos dentro del ámbito de aplicación de este Convenio, se podrán solicitar las siguientes medidas específicas:

1. La incautación y depósito de sistemas informáticos o soportes de almacenamiento de datos.
2. El sellado, precinto y prohibición de uso de sistemas informáticos o soportes de almacenamiento de datos.
3. El requerimiento de preservación inmediata de datos que se hallan en poder de terceros.
4. La copia de datos.

Artículo 7

DILIGENCIAS DE INVESTIGACIÓN

Sin perjuicio de cualesquiera otras diligencias de investigación que pudieran contribuir a la persecución efectiva de los delitos comprendidos dentro del ámbito de aplicación de este Convenio, se podrán solicitar las siguientes diligencias específicas:

SECRETARÍA GENERAL

CONFERENCIA DE MINISTROS DE
JUSTICIA DE LOS PAÍSES
IBEROAMERICANOS

1. La intervención de comunicaciones a través de las tecnologías de la información y comunicación.
2. La obtención de datos de tráfico.
3. El acceso a sistemas de información.
4. Acceso a la información contenida en un dispositivo que permita el almacenamiento de datos.
5. La entrega de datos y archivos informáticos.

Artículo 8

AUTORIDADES CENTRALES

1. Cada uno de los Estados Parte designará una Autoridad Central que canalizará las solicitudes de cooperación.
2. En particular, corresponderá a la Autoridad Central:
 - a) Recibir y verificar la regularidad formal y la legalidad de las solicitudes de cooperación de otros Estados Parte, y dirigirlas a las autoridades competentes para su cumplimiento dentro del Estado.
 - b) Recibir y verificar la regularidad formal y legalidad de las solicitudes de cooperación nacionales, y remitirlas a la Autoridad Central del Estado Parte de cumplimiento correspondiente.
3. Los Estados Parte designarán y garantizarán el funcionamiento continuado de al menos un punto de contacto disponible todos los días del año y durante las 24 horas del día.

Artículo 9



SOLICITUDES DE COOPERACIÓN

1. Las solicitudes de cooperación deberán contener los siguientes extremos:
 - a) Identificación de la autoridad que presenta la solicitud y el Estado Parte destinatario de la misma.
 - b) Descripción somera de los hechos que están siendo investigados o sometidos a enjuiciamiento.
 - c) La eventual calificación jurídica con expresión de los preceptos legales que pudieren haber sido infringidos conforme a la legislación del Estado parte requirente.
 - d) La medida de aseguramiento o diligencia de investigación que se solicita y su justificación.
 - e) Si fuera preciso, las condiciones concretas en que deba llevarse a cabo la medida de aseguramiento o diligencia de investigación solicitada, al objeto de que tenga validez en el Estado Parte requirente.
2. Las comunicaciones se llevarán a cabo a través de cualquier medio seguro que deje constancia de su envío y recepción íntegra y en el idioma del Estado requerido.
3. Por razones de urgencia el solicitante podrá dirigirse directamente a los puntos de contacto formalizando una solicitud abreviada que deberá completarse en el improrrogable plazo de 48 horas.
4. Con carácter previo a la formalización de la solicitud la autoridad requirente podrá elevar por el cauce de su Autoridad Central consultas al Estado requerido sobre la existencia de requisitos específicos con arreglo a su derecho interno para el cumplimiento de la solicitud.
5. Los Estados Parte podrán servirse de cualquier canal de intercambio de información para facilitar la cooperación en el marco de este Convenio, en particular de IberRed.

SECRETARÍA GENERAL

CONFERENCIA DE MINISTROS DE
JUSTICIA DE LOS PAÍSES
IBEROAMERICANOS

Artículo 10

PROCEDIMIENTO PARA LA TRAMITACIÓN DE LAS
SOLICITUDES DE COOPERACIÓN

1. En orden a verificar la regularidad formal y legalidad de la solicitud de cooperación, las Autoridades Centrales atenderán al cumplimiento de los requisitos materiales y procesales establecidos en el presente Convenio, así como a las normas de derecho interno.
2. La Autoridad Central del Estado Parte requerido verificará la regularidad formal y legalidad de la solicitud y adoptará alguna de las siguientes decisiones:
 - a) Rechazar, total o parcialmente, la solicitud motivadamente cuando concurra un defecto insubsanable o cuando por cualquier otra causa no fuera posible su cumplimiento según este Convenio o el ordenamiento jurídico del Estado Parte requerido.
 - b) Devolver la solicitud motivadamente cuando concurra un defecto subsanable, otorgando al solicitante un plazo de corrección.
 - c) Admitir la solicitud remitiéndola a la autoridad competente para su ejecución.
 - d) Admitir la solicitud de modo condicionado a que: 1) Se preserve la confidencialidad de la información o actuaciones interesadas, si la solicitud no puede ser atendida sin esta reserva. 2) No se haga uso de los resultados obtenidos en investigaciones o procedimientos distintos de los indicados en la solicitud.

Si el requirente no acepta las condiciones de cumplimiento, la Autoridad Central del Estado Parte requerido podrá rechazar la solicitud.

3. Los resultados obtenidos, si los hubiere, serán remitidos al Estado Parte requirente a través de su Autoridad Central. Si



MINISTÉRIO PÚBLICO FEDERAL
2ª Câmara de Coordenação e Revisão

Da 2ª Câmara de Coordenação e Revisão
À Coordenadoria de Registro e Informações Processuais

DESPACHO DE AUTUAÇÃO

De ordem da Sra. Coordenadora, remetam-se à DPE/CRIP para a devida autuação. Após, retornem-se para a respectiva distribuição.

Determino o prazo de 3 (três) anos para a conclusão do procedimento.

Brasília, 10 de fevereiro de 2014.

Márcia R.O. Ferradaes

Márcia Rodrigues de Oliveira Ferradaes
Secretaria da 2ª CCR

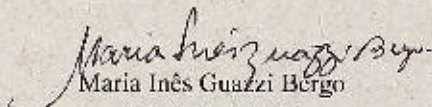


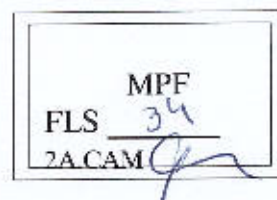
**MINISTÉRIO PÚBLICO FEDERAL
PROCURADORIA GERAL DA REPÚBLICA**

CERTIDÃO

Certifico que, na presente data, nesta Divisão de Processamento Extrajudicial - DPE, autuei o Ofício PR/RS-GABPR28MGBAS nº 21.944/2013, de 19 de dezembro de 2013 (PR-SP-00084529/2013), como Procedimento Administrativo - PA nº 1.00.000.002205/2014-88, com 33 folhas em 1 volume e faço sua movimentação à 2A.CAM - 2ª Câmara de Coordenação e Revisão do MPF, em cumprimento ao Despacho s/nº, de 10 de fevereiro de 2014, exarado por sua Secretaria e acostado à fl. 32.

Brasília - DF, 10/02/2014


Maria Inês Guazzi Berço
Matrícula 19154



MINISTÉRIO PÚBLICO FEDERAL
PGR/2A.CAM - 2A.CAMARA DE COORDENACAO E REVISAO DO MPF
SAF SUL QUADRA 04 CONJ. CASA SUL
CEP: 70050900 - BRASILIA - DF

Procedimento Administrativo - PA - 1.00.000.002205/2014-88 - CRIMINAL
CIÊNCIA

TERMO DE DISTRIBUIÇÃO

1. Nesta data, nos termos do art. 8º, parágrafo único da Resolução nº 20, de 06/02/1996, procedo à distribuição regular deste auto ao(à) Dr(a) Procurador(a) Regional da Republica Carlos Augusto da Silva Cazarre (Titular).

BRASILIA, 11/02/2014

Marcia R.O. Ferradaes
MARCIA RODRIGUES DE OLIVEIRA FERRADAES
TECNICO DO MPU/APOIO TECNICO-ADMINISTRATIVO/ADMINISTRACAO



MINISTÉRIO PÚBLICO FEDERAL
2ª Câmara de Coordenação e Revisão

PROCEDIMENTO MPF Nº 1.00.000.002205/2014-88
ORIGEM: PROCURADORIA DA REPÚBLICA EM SÃO PAULO
RELATOR: CARLOS AUGUSTO DA SILVA CAZARRÉ

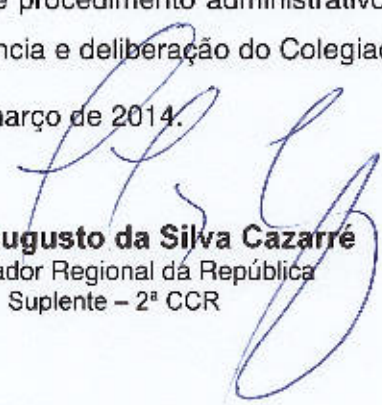
DESPACHO

Trata-se de Procedimento Administrativo instaurado a partir de ofício subscrito pela Procuradora da República Melissa Garcia Blagitz de Abreu e Silva (PR/SP), por meio do qual encaminha Relatório sobre a sua participação na Conferência Octopus contra Cibercriminalidade, provida pelo Conselho da Europa, em Estrasburgo, França, de 4 a 6 de dezembro de 2013.

É o relatório.

Inclua-se o presente procedimento administrativo em pauta da próxima Sessão de Coordenação, para ciência e deliberação do Colegiado.

Brasília/DF, 17 de março de 2014.


Carlos Augusto da Silva Cazarre
Procurador Regional da República
Suplente – 2ª CCR

ALC.



MINISTÉRIO PÚBLICO FEDERAL
2ª Câmara de Coordenação e Revisão

Procedimento: 1.00.000.002205/2014-88

CERTIDÃO DE JULGAMENTO

Certifico que na 79ª Sessão de Coordenação, realizada em 07/04/2014, o colegiado da 2ª Câmara, por unanimidade, resolve encaminhar cópia dos autos à Secretaria de Cooperação Jurídica Internacional e aos Coordenadores Criminais e determina a sua publicação na página da Câmara.

Votaram com a Relator a Dra. Raquel Elias Ferreira Dodge e o Dr. Oswaldo José Barbosa

Brasília, 22 de abril de 2014.

Assinatura manuscrita em azul de Gisele Ramalho Lopes.

Gisele Ramalho Lopes
Técnico Administrativo



MINISTÉRIO PÚBLICO FEDERAL

PROCURADORIA GERAL DA REPÚBLICA

2ª CÂMARA DE COORDENAÇÃO E REVISÃO (MATÉRIA CRIMINAL E CONTROLE EXTERNO DA ATIVIDADE POLICIAL)

Ofício Circular nº 18/2014

Brasília, 24 de abril de 2014

Assunto: Encaminha cópia do P.A 1.00.000.002205/2014-88 para conhecimento.

Senhora Coordenadora Criminal,

Ao cumprimentá-la, de ordem da Coordenadora da 2ª Câmara de Coordenação e Revisão, Dra. Raquel Elias Ferreira Dodge, e conforme deliberação do Colegiado da 79ª Sessão de Coordenação, encaminho a Vossa Excelência, para conhecimento, cópia do P.A 1.00.000.002205/2014-88, o qual contém relatório sobre a Conferência Octopus, realizada em dezembro de 2013, em Estrasburgo na França.

Respeitosamente,


Cláudia de Fátima Roque
Secretária-Executiva

A Sua Excelência a Senhora
Drª. Raquel Branquinho P. M. Nascimento
DD. Procuradora Regional da República
Procuradoria Regional da República da 1ª Região
Brasília/DF

*encaminhado a todos os
Coord. criminais*



MINISTÉRIO PÚBLICO FEDERAL

Procuradoria Geral da República

2ª Câmara de Coordenação e Revisão (Matéria Criminal e Controle Externo da Atividade Policial)

Ofício nº 171E/2014

Brasília, 24 de abril de 2014.

Etiqueta:

Assunto: Encaminha cópia do P.A 1.00.000.002205/2014-88 para conhecimento.

Senhor Secretário de Cooperação Jurídica Internacional,

Ao cumprimentá-lo, de ordem da Coordenadora da 2ª Câmara de Coordenação e Revisão, Dra. Raquel Elias Ferreira Dodge, e conforme deliberação do Colegiado da 79ª Sessão de Coordenação, encaminho a Vossa Excelência, para conhecimento, cópia do P.A 1.00.000.002205/2014-88, o qual contém relatório sobre a Conferência Octopus, realizada em dezembro de 2013, em Estrasburgo na França.

Respeitosamente,


Cláudia de Fátima Roque
Secretária-Executiva

A Sua Excelência o Senhor
Dr. Vladimir Aras
DD. Procurador da República
Secretário de Cooperação Jurídica Internacional
Secretaria de Cooperação Jurídica Internacional do Ministério Público Federal
Procuradoria Geral da República
N E S T A