Atuação do Ministério PúblicoFederal no Combate aos *Crimes Cibernéticos*

MPF
Ministério Público Federal

1. Atuação do MPF

Criação dos Grupos especializados no Combate aos Crimes Cibernéticos em 2003 (SP) e em 2006 (RJ)

Motivação: aumento da criminalidade incentivado pela insegurança da rede.

Atribuições:

- Atuação em processos judiciais/extrajudiciais.

- Celebração de Termos de Compromisso de Integração Operacional, de Cooperação, recomendações e TAC.

- Atividades repressivas (Operações da PF).

- Atividades preventivas (apoio às Oficinas para educadores sobre o uso seguro e responsável da Internet).

MPF
Ministério Público Federal

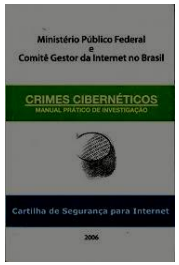
Grupo de Apoio sobre Criminalidade Cibernética da Câmara Criminal do MPF – 2011

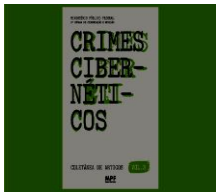
- Composição: 8 PRs e 2 PRRs de diferentes estados.

-**Responsável por uma política institucional de atuação e capacitação para os membros do MPF voltada para a efetiva repressão dos crimes cibernéticos.**

-Aprimoramento é feito por meio de cursos de treinamento para novos procuradores (CIV); os já integrante na carreira, anualmente, e, desde 2015, convidamos juízes federais.

- Organização da 1ª edição e atualização da 2ª edição do "Roteiro de Atuação sobre Crimes Cibernéticos", distribuído para o MPF e Judiciário Federal e demais autoridades quando ministramos cursos.





MPF
Ministério Público Federal

Grupo de Apoio sobre Criminalidade Cibernética (GACC - 2011)

- Acompanhamento do legislativo nacional e internacional sobre o tema, com apresentação de Notas Técnicas.

- Participação em cursos e seminários interdisciplinares nacionais e internacionais.

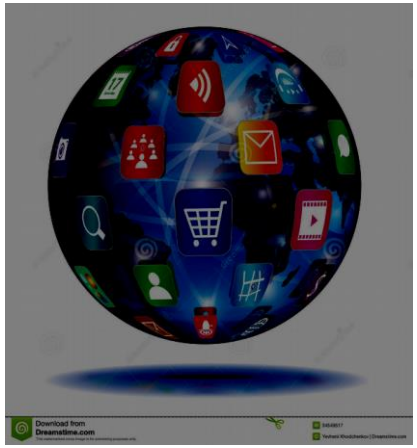
- Representação nacional (audiência pública no STF sobre o bloqueio do WhatsApp; reunião no STF sobre ADC 51/STF; audiências públicas das CPIs dos Crimes Cibernéticos e da Pedofilia) e internacional (IGF; OEA; Octopus; ONU; etc);

- Intensa mobilização no SAFERINTERNET DAY (fev) - PARCERIAS: CGI; PF; ONGs; setor privado.

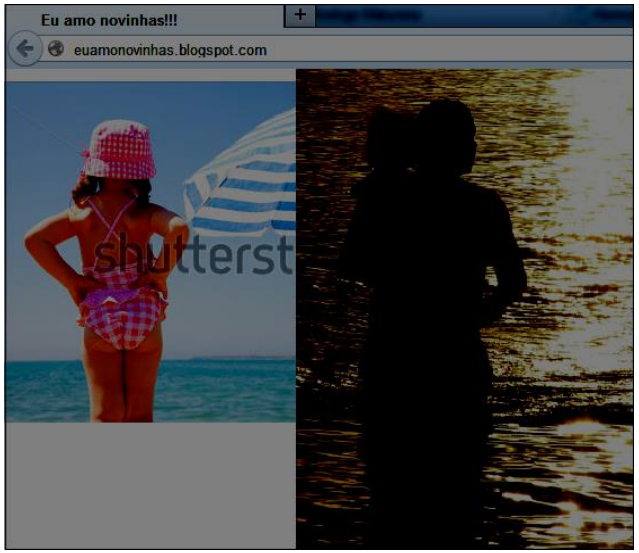
- Ministra palestras (no Brasil e exterior), cursos e seminários.

SERVIÇOS MAIS COMUNS PRESTADOS NA INTERNET

- ✓**world wide web** (www)
- ✓**e-mail**
- ✓**hospedagem e compartilhamento de arquivos** (redes P2P, Gigatribe)
- ✓**troca instantânea de mensagens** (Whatsapp, Telegram)
- ✓**voip** (voz sobre IP)
- ✓**chat** (salas de bate-papo)
- ✓**fóruns de discussão**
- ✓**formação de redes e comunidades virtuais** (Facebook, Instagram, Twitter)
- ✓**e-commerce**



2. Os Crimes Cibernéticos



MPF
Ministério Público Federal

FORMAS MAIS COMUNS DE CRIMINALIDADE CIBERNÉTICA

✓**Fraudes bancárias (estelionato e furto eletrônicos) -** Arts. 155, §§ 3º e 4º, II, e 171 do CP

✓ **Falsificação e supressão de dados -** Arts. 297, 298, 299, 313-A, 313-B do CP

✓**Invasão de dispositivo informático e furto de dados** - Art. 154-A do CP

✓**Publicação; posse; obtenção; troca de vídeos e imagens contendo pornografia infantil -** Arts. 241-A, 241-B e 241-C do ECA

✓**Assédio e aliciamento de crianças** - Art. 241-D do ECA

✓**Ciberterrorismo –** Art. 2º, § 1º, inc. IV, da Lei 13260/16.

2. Os Crimes Cibernéticos

- ✓**Ameaça** - Art. 147 do CP
- ✓**Interrupção de serviço telemático**-Art. 266, § 1ºdo CP
- ✓***Cyberbullying/revenge porn* (criação e publicação de perfis falsos visando a veiculação de ofensas em blogs e comunidades virtuais, inclusive fotos íntimas não autorizadas)** – Arts. 138, 139, 140, 218-C e 218-C, § 1º, do CP
- ✓**Incitação e apologia de crime** – Arts. 286 e 287 do CP
- ✓**Crimes de ódio** – Art. 20 da Lei 7.716/89
- ✓**Injúria racial** – Art. 140, § 3º, do CP
- ✓**Crimes contra a propriedade intelectual e artística -** Art. 184 do CP e Lei 9609/98
- ✓**Venda ilegal de medicamentos** – Art. 273 do CP

MPF
Ministério Público Federal

Discriminação e Preconceito *online*

Art. 20, § 2º, da Lei 7716/89 – prática, induzimento ou incitação da discriminação ou do preconceito por motivo de raça, cor, etnia, religião ou procedência nacional quando cometidos por intermédio dos meios de comunicação social ou publicação de qualquer natureza.

Pena – 2 a 5 anos de reclusão e multa – crime grave, não cabe nem transação penal nem suspensão do processo. A Convenção sobre Eliminação de todas as Formas de Discriminação Racial obriga o Estado brasileiro a proibir a discriminação racial, ou seja, proibir qualquer forma de distinção, exclusão, restrição ou preferência por razão de raça, cor, etc. Competência da Justiça Federal.

Injúria Racial

Art. 140, § 2, do CP – ofensa a dignidade e do decoro utilizando-se de elementos referentes a raça, cor, etnia, religião, origem, condição de pessoa idosa ou portadora de deficiência.

Delito contra a honra subjetiva do indivíduo, mesmo pela Internet, a competência é da JE.

Terrorismo Cibernético

Lei 13.260/2016

• Prática de atos terroristas utilizando mecanismos cibernéticos
Art. 2º, IV – praticado por razões de xenofobia, discriminação ou preconceito de raça, cor, etnia e religião – finalidade: provocar terror social ou generalizado.

•**Ransomware -**

•Sequestro de dados mediante utilização de malware para obtenção de resgate em valores, em geral, Bitcoins
Art. 154-A, caput, CP
Art. 154-A, §1º, CP
Art.158, CP - extorsão (?????????)

Direitos humanos relacionados a atribuição do MPF

- Brasil é signatário da ***Convenção da ONU sobre os Direitos da Criança*** (1989).

- Brasil também é signatário da ***Convenção Internacional sobre a Eliminação de todas as Formas de Discriminação Racial*** (1968).

Fraudes bancárias contra bancos federais ou inserção de dados em sistemas de órgãos federais são violações de interesse da União, mas não é objeto de trabalho dos grupos.

Com base na Convenção de Belém sobre violência contra mulheres, há uma decisão recente do Superior Tribunal de Justiça de que ameaças contra mulheres nas redes sociais de grande alcance que começam no estrangeiro e o resultado ocorra no Brasil ou vice-versa, a competência deve ser da Justiça Federal.

Brasil: sem legislação criminal específica, mas tipos esparsos espalhados no Código Penal; aplica-se nos demais casos a legislação comum (Código Penal e leis extravagantes).

- **Preservação de registros**: antes do MCI, era feita segundo termos de cooperação assinados com cada provedor individualmente – não havia prazo mínimo previsto na legislação.

- **Acesso a dados**: previsões do Código de Processo Penal (busca e apreensão) e CR + Lei nº 9296/96 (interceptação de dados telemáticos).

Agente Infiltrado Online

a ineficácia dos tradicionais métodos de investigação para enfrentar o cibercrime;

novo meio de investigação fundamental para enfrentar as novas formas de delinquência;

o agente deve agir exatamente dentro do estipulado pela decisão judicial;

no pedido e na decisão judicial devem estar claras e delimitadas as ações do agente infiltrado.

4. Legislação

Lei 13.441/17 - Infiltração na Internet para investigar arts. 240, 241, 241-A, 241-B, 241-C, 241-D ECA (pornografia infantil); 217-A, 218, 218-A e 218-B do CP (crimes contra a dignidade sexual de vulneráveis) e 154-A do CP (invasão de dispositivo informático).

Lei 12.850/2013 - Infiltração na investigação prevista na Lei de Organizações Criminosas.

MPF
Ministério Público Federal

WHATSAPP/ TELEGRAM/ FACEBOOK MESSENGER

•quebra de sigilo da criptografia ponto a ponto? *Man-in-the-middle* mediante colaboração da empresa

• **Meios de Investigação** – infiltração, clonagem de chip, inoculação de *spyware* nas pontas, Pegasus.

• backdoors: controvertido (direito à privacidade)

MARCO CIVIL DA INTERNET - LEI Nº 12.965/2014

•define termos técnicos, direitos e garantias dos usuários, e diretrizes do Poder Público;

•estabelece que as informações dos provedores de conexão e de aplicação à Internet somente poderão ser obtidas por ordem judicial (Art. 10, §1º);

•para autoridades, o acesso a dados cadastrais (qualificação pessoal, filiação e endereço, na forma da lei) dispensa a ordem judicial (Art. 10, § 3º);

•provedores com representação no Brasil ou prestando serviços no País devem cumprir a legislação nacional (Art.11,§ 2º).

MARCO CIVIL DA INTERNET - LEI Nº 12.965/2014

PRAZOS DE RETENÇÃO:

registros de acesso a aplicações de Internet: 6 meses (Art.15).

registros de conexão: 1 ano (Art. 13).

PEDIDO DE PRESERVAÇÃO por PRAZO SUPERIOR: pode ser feito pelo MP, polícia ou autoridade administrativa.

CONTEÚDO: não há obrigação de guarda, mas fornecimento somente ordem judicial. Pode ser feito pedido de preservação também. Conteúdo armazenado – Art. 7, inc. III, do MCI. Conteúdo *online* (tempo real) – Art. 7, inc. II, do MCI (na forma da L. 9296/96).

PROVEDORES SEM REPRESENTAÇÃO NO BRASIL

1. Provedores **sem representação** no Brasil, mas que oferecem seus serviços ao público em território nacional, devem cumprir a legislação brasileira:

- Targeting Test:

. serviço oferecido em português;

. publicidade voltada para o público em território nacional;

. vendas na moeda nacional.

2. **Provedores que NÃO oferecem seus serviços ao público no Brasil**, mas que são utilizados a partir do território nacional: para obtenção dos dados, a menos que eles estejam acessíveis às autoridades nacionais (art 240 CPP), será necessário o pedido de cooperação internacional – MLAT.

PROVEDORES SEM REPRESENTAÇÃO NO BRASIL

SUGESTÃO:

Obrigação por parte dos provedores que oferecem serviços no Brasil de indicar um representante legal em território nacional que receba e possa cumprir decisões e ordens legais. (Semelhante à Proposta do E-evidence em discussão na Comissão Europeia e no Conselho da União Europeia)

Marco Civil da Internet – Lei 12.965/14

SANÇÕES do ART. 12: descumprimento arts. 10 e 11 do MCI

I - **ADVERTÊNCIA** COM INDICAÇÃO DE PRAZO PARA ADOÇÃO DE MEDIDAS CORRETIVAS

II - **MULTA** ATÉ 10% DO FATURAMENTO DO GRUPO ECONÔMICO NO BRASIL - condição econômica do infrator + princípio da proporcionalidade entre a gravidade da falta e a intensidade da sanção;

III - **SUSPENSÃO TEMPORÁRIA DAS ATIVIDADES** – que envolvam os atos previstos no art. 11

IV - **PROIBIÇÃO DE EXERCÍCIO DAS ATIVIDADES** - que envolvam os atos previstos no art. 11.

Marco Civil da Internet – Lei 12.965/14

SANÇÕES do ART. 12: descumprimento arts. 10 e 11 do MCI

SUGESTÃO:

Rejeição do Projeto de Lei nº5.130 que pretende proibir o bloqueio ou suspensão de serviços de internet, notadamente mensageiros eletrônicos: legislador não pode prever todas as hipóteses/judiciário deve decidir com proporcionalidade

EX: Um serviço de aplicações de Internet pode escolher pagar as multas e continuar operando um serviço criminoso

Projeto de lei nº 236/2012

Projeto de lei do Senado nº 236/2012, que altera o Código Penal, da relatoria do então senador Pedro Taques, no qual a parte de crimes cibernéticos (artigos 213 a 219) corrige falhas da Lei Carolina Dieckmann. Essa parte foi elaborada pelo GT de SP, que acatou sugestões do grupo Garoa Hacker Clube/SP.

Projeto de lei nº 236/2012

O artigo sobre acesso indevido (Art. 214) melhora o art. 154-A da Lei Carolina Dieckmann: ele fala em "acesso" em vez de "invasão" e retira a exigência anterior de que o sistema informático seja "protegido" – algo que é facilmente questionável e pode desqualificar o computador de um usuário comum, que muitas vezes não conta com medidas de segurança adequadas.

O artigo 214 inclui a obtenção de dados privados e sua divulgação, exatamente o que ocorreu no caso da atriz Carolina Dieckmann, e que ensejou a edição da lei apelidada com seu nome, a qual, entretanto, não tipificou tal conduta.

Projeto de lei nº 236/2012

No artigo 219 - que trata sobre a punição de quem produz, comercializa, manipula ou vende artefatos maliciosos, foram incluídas algumas excludentes para evitar a punição de profissionais, pesquisadores e desenvolvedores que trabalham com segurança e que investigam artefatos maliciosos para aperfeiçoamento dos sistemas de segurança (parágrafo único que prevê as excludentes de ilicitude).

Projeto de lei nº 236/2012

Prevê, assim, um artigo específico com conceitos (art. 213), crimes como o acesso indevido; o acesso indevido qualificado; sabotagem informática; dano a dados informatizados; fraude informatizada; obtenção indevida de credenciais de acesso a dados e artefato malicioso.

COOPERAÇÃO INTERNACIONAL

Somente necessária quando o provedor não tem filial no Brasil ou não presta serviços para brasileiros (Art. 11 do MCI e Art. 21 do NCPC). Ex.: Telegram, Signal etc.

- baseada em tratados internacionais:
- cartas rogatórias
- pedidos de cooperação direta
- MLATs (pode levar, em média, 2 anos)

cooperação espontânea (ex. Reports NCMEC)

Rede 24/7: possibilidade de solicitar a preservação imediata de dados em outros países, até o pedido de cooperação ser formulado.

5. Cooperação Internacional

CONVENÇÃO DE BUDAPESTE – Conselho da Europa - 2001
âmbito internacional e aberta a outros países

- **Harmonização da legislação no âmbito da cooperação internacional;**

- **Participação nas discussões dos T-CY (Cybercrime Conventions Committee);**

- **Cooperação eficiente e confiável de parceiros e disponibilidade da rede 24x7;**

- **Compartilhamento de experiências em programas de capacitação (C-Proc).**

MPF
Ministério Público Federal

CONVENÇÃO DE BUDAPESTE

Conselho da Europa – aberta aos demais países

Previsões:

1.Signatários devem estabelecer como crime:

- **acesso/interceptação ilegal de dados;**
- **destruição de dados/interferências e danos a sistemas;**
- **criação e uso de programas maliciosos;**
- **falsificação de dados;**
- **estelionato via sistema;**
- **pornografia infantil (produção, publicação, posse, obtenção) conceito inclui “imagens realistas”;violação de direitos autorais**

CONVENÇÃO DE BUDAPESTE – âmbito internacional

2. Signatários devem estabelecer procedimentos mínimos de investigação:

- **mecanismos de preservação e obtenção de provas – preservação por 90 dias prorrogáveis por mais 90;**
- **busca e apreensão;**
- **interceptação de dados;**
- **possibilidade de acesso a provas localizadas em outro país através de um sistema ligado a outro mediante concordância do usuário do sistema ou do país onde a prova está localizada.**

CONVENÇÃO DE BUDAPESTE – âmbito internacional

3. Principais Vantagens para o Brasil em aderir:

a) Melhoria e Harmonização da legislação – incentivo para aprovação de tipos penais específicos e lei processual em geral. Harmonização da legislação torna mais ágil a cooperação internacional

b) Cooperação Internacional mais rápida e eficiente – a possibilidade de em situações urgentes(art. 27.9.a) a autoridade judicial pedir a preservação de dados e o auxílio diretamente à autoridade congênere, até mesmo por e-mail, o que garante a integridade da prova até que seja processado o pedido formal

CONVENÇÃO DE BUDAPESTE – âmbito internacional

3. Principais Vantagens para o Brasil em aderir:

(c) Ampliação da rede 24/7 – atualmente já são 63 o países que ratificaram a Convenção, 19 não são membros do Conselho da Europa, dentre os quais países da América Latina como Argentina, Chile, Costa Rica, República Dominicana, Panamá, Paraguai, países da África, como Cabo Verde, Gana, Marrocos, Senegal, países da Asia, como Filipinas, Siri Lanka, Tonga e até Malásia e Singapura estudando aderir.

(d) Ampliação das hipóteses de cooperação – mesmo se o Brasil não tiver acordo bilateral específico pode utilizar o arcabouço da CB

CONVENÇÃO DE BUDAPESTE – âmbito internacional

3. Principais Vantagens para o Brasil em aderir:

(e) Capacitação e treinamento – intercâmbio de técnicas investigativas, soluções legislativas e tecnologia (C-PROC , programa específico destinado a capacitar as equipes técnicas, os agentes de investigação, ministérios públicos e magistrados na obtenção de provas digitais)

(f) A Convenção já existe e vai (melhor) atender às necessidades atuais e presentes do acesso à prova digital

7. Dificuldades

1. Ausência de legislação (só 2 artigos no Código Penal sobre crimes cibernéticos próprios - Projeto de alteração do Código Penal (PLS nº 236/2012), de relatoria do então senador Pedro Taques) ou deficiência de legislação (Lei Carolina Dieckmann)

2. Ausência de legislação nos Estados Unidos sobre crimes contra a honra (Ementa nº 1- proteção da liberdade de expressão).

3. Cooperação internacional pouco eficiente (insistência dos provedores pela aplicação do MLAT, sem respeitar nossa Lei). Pouco comprometimento dos provedores.

4. Darkweb – dificuldade da investigação nesse ambiente pelas Polícias brasileiras (ausência de capacitação).

MPF
Ministério Público Federal

7. Dificuldades

5. Falta de estrutura e integração entre os órgãos de repressão e julgamento - não há especialização suficiente nem treinamento dos agentes envolvidos.

6. Falta de estrutura na área pericial nos órgãos da PF e do MPF (falta de um núcleo de apoio técnico pelo o menos nas 5 Regiões, temos em SP, desde 2009; no RS e DF (recentes com um servidor cada); RJ (3 servidores revesamento) e PE (2 servidores não exclusivos)

7. Constante capacitação e evolução dos criminosos: *hackers*

MPF
Ministério Público Federal

8. Estratégias e soluções

1.Criação de Grupos especializados nas unidades das Procuradorias da República e dos MPEs.

2. Criação de delegacias especializadas com maior capacitação e estrutura.

3. Treinamento e capacitação dos setores periciais e criação dos núcleos técnicos nas 2 Regiões (RJ e PE) e aperfeiçoamento dos do DF e RS, no MPF, a exemplo do NTCCC da PR/SP.

4. Maior integração do MP com a Polícia e o Judiciário - cooperação para otimização dos resultados.

5. Intensificação da comunicação entre os países - facilitação na obtenção de provas.

MPF
Ministério Público Federal

8. Estratégias e soluções

6. Necessidade de ratificação pelo Brasil da Convenção de Budapeste (acesso às provas transnacionais facilitado)

7. Aprovação destacada do Projeto de Lei sobre Crimes Cibernéticos

8. Maior comprometimento dos provedores e respeito ao MCI.

9. Rejeição do Projeto de Lei nº5.130 que pretende proibir o bloqueio ou suspensão de serviços de internet, notadamente mensageiros eletrônicos: legislador não pode prever todas as hipóteses/judiciário deve decidir com proporcionalidade

8. Estratégias e soluções

10. Atuação na área de PREVENÇÃO ao crime, tanto na área social (Projeto "*Ministério Público pela Educação Digital nas Escolas*") e na área legislativa (grupos de estudo e participação em CPIs).

11. Obrigação por parte dos provedores que oferecem serviços no Brasil de indicar um representante legal em território nacional que receba e possa cumprir decisões e ordens legais. (Semelhante à Proposta do E-evidence em discussão na Comissão Europeia e no Conselho da União Europeia)

12. Implementação do artigo 4º,IV da Lei Geral de Proteção de Dados: legislação específica para tratar os dados pessoais descritos no inciso III: a)segurança pública; b) defesa nacional; c)segurança do estado; d) atividades de investigação e repressão de infrações penais.

MPF
Ministério Público Federal

CONTATOS

Grupo de Apoio sobre Criminalidade Cibernética – GACC da Câmara Criminal do MPF

Neide Cardoso de Oliveira — **neidec@mpf.mp.br**
Coordenadora

Fernanda Domingos — **fernandadomingos@mpf.mp.br**
Coordenadora Adjunta

OBRIGADA!!!

MPF
Ministério Público Federal