

Council of Europe	Cybercrime training workshop for prosecutors Belo Horizonte, Brazil, 26 August 2008	I Encontro Internacional de Capacitação de Promotores de Justiça no enfrentamento aos Crimes Cibernéticos Belo Horizonte, Brasil, 26/8/2008
<p><u>I. About cybercrime</u></p> <p><u>II. International standards</u></p> <p><u>III. Procedural tools and international cooperation</u></p> <p><u>IV. Law enforcement/ service provider cooperation</u></p> <p>Alexander Seger Economic Crime Division, Council of Europe Strasbourg, France alexander.seger@coe.int</p>		<p>I. Sobre o cibercrime</p> <p>II. Normas Internacionais</p> <p>III. Ferramentas procedimentais e cooperação internacional</p> <p>IV. Cooperação entre as autoridades responsáveis pela aplicação da lei e o fornecedor de serviços</p> <p>www.coe.int/cybercrime</p>

1

Council of Europe	Cybercrime training workshop for prosecutors Belo Horizonte, Brazil, 26 August 2008	I Encontro Internacional de Capacitação de Promotores de Justiça no enfrentamento aos Crimes Cibernéticos Belo Horizonte, Brasil, 26/8/2008
<p>I. About cybercrime</p> <ul style="list-style-type: none"> ➤ Why worry? ➤ What is cybercrime? <p>Alexander Seger Economic Crime Division, Council of Europe Strasbourg, France alexander.seger@coe.int</p>		<p>I. Sobre o cibercrime</p> <ul style="list-style-type: none"> ➤ Porquê preocupar-se? ➤ O que é o cibercrime? <p>www.coe.int/cybercrime</p>

2

Why worry about cybercrime?

- Opportunities provided by information and communication technologies
- Information society
- Confidentiality, integrity, and availability of your computer data
- Reliance of public infrastructure on ICT
- Reliance of business on ICT
- Dependency of societies on ICT = vulnerability to cybercrime
- Need for secure and accessible ICT

3

Porquê preocupar-se com o cibercrime?

- Oportunidades proporcionadas pelas tecnologias da informação e da comunicação
- Sociedade da informação
- Confidencialidade, integridade e disponibilidade dos seus dados informáticos
- Dependência das infra-estruturas públicas das TIC
- Dependência das empresas das TIC
- Dependência das sociedades das TIC = vulnerabilidade ao cibercrime
- Necessidade de TIC seguras e acessíveis

3

What is cybercrime?

- Offences against the confidentiality, integrity and availability of computer data and systems
- Computer-related forgery and fraud
- Content-related offences
- Offences related to intellectual property rights and similar rights

4

Definições

- Infracções contra a confidencialidade, integridade e disponibilidade de sistemas informáticos e dados informáticos
- Infracções relacionada com computadores: Falsidade informática, Burla informática
- Infracções relacionadas com o conteúdo
- Infracções relacionadas com a violação do direito de autor e direitos conexos

4

What is cybercrime?**Offences against the confidentiality, integrity and availability of computer data and systems (CIA offences)**

- Illegal access to a computer system
- Illegal interception
- Data interference
- System interference
- Misuse of devices

O que é o cibercrime?**Infracções contra a confidencialidade, integridade e disponibilidade de sistemas informáticos e dados informáticos**

- Acesso ilegítimo
- Intercepção ilegítima
- Interferência em dados
- Interferência em sistemas
- Uso abusivo de dispositivos

5

5

What is cybercrime?**Computer-related forgery and fraud**

Shift in the threat landscape: from broad, mass, multi-purpose attacks to specific attacks on specific users, groups, organisations or industries, increasingly for economic criminal purposes

- Security breaches and financial losses in companies
- Credit card fraud and other financial crime
- Advance fee fraud
- Extortion
- Internet marketing and retail fraud
- Auction fraud and stock market manipulation
- Phishing and other forms of identity theft
- Etc.

O que é o cibercrime?**Infracções relacionadas com computadores: Falsidade informática, Burla informática**

Alteração no cenário das ameaças: desde grandes ataques em massa e com fins múltiplos a ataques específicos a utilizadores, grupos, organizações ou indústrias específicas, cada vez mais para efeitos económicos criminosos.

- Infracções de segurança e perdas financeiras em empresas
- Fraude envolvendo cartões de crédito e outros crimes financeiros
- Fraude envolvendo pagamentos antecipados
- Extorsão
- Fraude através de marketing e vendas na Internet
- Fraude em leilões e manipulação do mercado de acções
- Phishing e outras formas de roubo de identidade. Etc.

6

6

What is cybercrime?**Content-related offences**

- Child pornography
- Xenophobia, racism, hate speech

Issue:

- Security and protection versus freedom of expression

O que é o cibercrime?**Infracções relacionadas com o conteúdo**

- Pornografia infantil
- Xenofobia, racismo, incitação ao ódio

Questão:

- Segurança e protecção versus liberdade de expressão

7

7

What is cybercrime?**Offences related to intellectual property rights and similar rights**

- IPR protected by national and international regulations
- Counterfeit products
- Health and safety risks
- Economic loss to companies and unfair competition
- Feeds organised crime

O que é o cibercrime?**Infracções relacionadas com a violação dos direitos de autor e direitos conexos**

- DA protegidos por regulamentos nacionais e internacionais
- Produtos contrafeitos
- Riscos de saúde e segurança
- Perdas económicas para as empresas e concorrência desleal
- Incentiva o crime organizado

8

8

What is cybercrime?**Key issues****Malware**

- Software inserted into an information system that causes harm to this or other systems
- Malware – that is, malicious codes and programmes including viruses, worms, trojan horses, spyware, bots and botnets – is evolving and rapidly spreading

O que é o cibercrime?**Questões essenciais****Software malicioso**

- Software inserido num sistema informático que causa danos a este ou a outros sistemas
- O software malicioso – isto é, códigos e programas maliciosos, incluindo vírus, worms, cavalos de tróia, spyware, bots e botnets – está a evoluir e a espalhar-se rapidamente

9

9

What is cybercrime?**Key issues****SPAM**

- Accounts for a large amount of internet traffic (70%+)
- Vector for malware

O que é o cibercrime?**Questões essenciais****SPAM (Correio Electrónico Não Solicitado)**

- Representa uma grande proporção do tráfego na Internet (70%+)
- Vector para o software malicioso

10

10

What is cybercrime?**Key issues****Bots and botnets**

Covertly installed programmes on a computer to allow unauthorised remote control

Can be used:

- for distributed denial of service (DDoS) attacks
- to harvest confidential information (identity theft)
- to distribute spam, spyware, adware
- for phishing attacks

O que é o cibercrime?**Questões essenciais****Bots e botnets**

Programas instalados de forma dissimulada num computador para permitir o controlo remoto não autorizado

Podem ser utilizados:

- para ataques distribuídos de negação de serviço (DDoS)
- para recolher informação confidencial (roubo de identidade)
- para distribuir spam, spyware e adware
- para ataques de phishing

11

11

What is cybercrime?**Key issues****Phishing and other forms of identity theft**

Obtaining identity information

Illegal access, Illegal interception, Data interference, System interference, Misuse of devices

Possessing, transferring, use

Attempt, aiding, abetting

Fraud and other offences

O que é o cibercrime?**Questões essenciais****Phishing e outras formas de roubo de identidade**

Obtenção de dados de identidade

Acesso ilegal, interceptação ilegal, interferência em dados, interferência em sistemas, uso abusivo de dispositivos

Posse, transferência, utilização

Tentativa e cumplicidade

Fraude e outras infracções

12

12

What is cybercrime?**Key issues****Cybercrime and organised crime**

- Offenders increasingly organising for cybercrime
- Botnets an important tool
- ICT facilitate offences by OC groups and networks, in particular economic crime
- ICT creates vulnerabilities -> exploited by OC
- ICT facilitate logistics, anonymity and reduce risks of OC
- ICT facilitate global outreach of OC
- ICT shape OC -> networks

13

Cibercrime e crime organizado

- Infractores cada vez mais organizados para o cibercrime
- Botnets são uma ferramenta importante
- TIC facilitam infracções por grupos e redes de CO, em particular o crime económico
- TIC criam vulnerabilidades -> exploradas pelo CO
- TIC facilitam a logística e o anonimato e reduzem os riscos de CO
- TIC facilitam a escala global do CO
- TIC moldam o CO -> redes

13

What is cybercrime?**Key issues****Terrorist use of the internet/ICT**

- Possible attacks via internet/ICT on critical information infrastructure and other critical infrastructure, systems and legal interests, including loss of life
- Dissemination of illegal contents, including threats of terrorist attacks, incitement to or promotion of terrorism, recruitment or training
- Use of ICT by terrorists for logistical purposes such as internal communication, gathering intelligence, target analyses

14

Utilização da Internet/TIC pelos terroristas

- Possíveis ataques através da Internet/TIC a infra-estruturas informáticas críticas e a outras infra-estruturas, sistemas e interesses jurídicos críticos, incluindo a perda de vida
- Disseminação de conteúdos ilegais, incluindo ameaças de ataques terroristas, incitamento ou promoção do terrorismo, recrutamento ou formação
- Utilização das TIC por terroristas para efeitos logísticos, tais como comunicação interna, recolha de inteligência e análises de alvos

14

II. International standards: the Convention on Cybercrime

Alexander Seger
Economic Crime Division, Council of Europe
Strasbourg, France
alexander.seger@coe.int

15

II. Normas internacionais: a Convenção sobre o Cibercrime

www.coe.int/cybercrime

15

Cybercrime: the criminal law response

- Criminalise certain conduct ► substantive criminal law
- Give law enforcement/criminal justice the means to investigate, prosecute and adjudicate cybercrimes (immediate actions, electronic evidence) ► criminal procedure law
- Allow for efficient international cooperation ► harmonise legislation, make provisions and establish institutions for police and judicial cooperation, conclude or join agreements

16

Cibercrime: a resposta do direito penal

- Incriminar certas condutas ► direito penal substantivo
- Atribuir às autoridades responsáveis pela aplicação da lei/justiça criminal os meios para investigar, processar judicialmente e julgar os cibercrimes (ações imediatas, provas electrónicas) ► processo penal
- Permitir uma cooperação internacional eficaz ► harmonizar a legislação, introduzir disposições e estabelecer instituições para a cooperação policial e judiciária, concluir ou aderir a acordos

16

Criminalising conduct

Legislation to deal with – as a minimum:

- Illegal access to a computer system
- Illegal interception
- Data interference
- System interference
- Misuse of devices
- Computer-related forgery
- Computer-related fraud
- Child pornography
- Infringement of copyright and related rights

17

Penalização conduta

Legislação para lidar com - como um mínimo:

- Acesso ilegítimo
- Intercepção ilegítima
- Interferência em dados
- Interferência em sistemas
- Uso abusivo de dispositivos
- Uso abusivo de dispositivos
- Burla informática
- Infracções relacionadas com pornografia infantil
- Infracções relacionadas com a violação do direito de autor e dos direitos conexos

17

Legal conditions for efficient investigations

Procedural law to provide for – as a minimum:

- Expedited preservation of stored computer data
- Expedited preservation and partial disclosure of traffic data
- Production order
- Search and seizure of stored computer data
- Real-time collection of traffic data
- Interception of content data
- Procedural safeguards

18

Condições legais eficientes para investigações

Direito Processual – como um mínimo:

- Conservação expedita de dados informáticos armazenados
- Conservação expedita e divulgação parcial de dados de tráfego
- Injunção
- Busca e Apreensão de dados informáticos armazenados
- Recolha em tempo real de dados informáticos
- Intercepção de dados relativos ao conteúdo
- Garantias processuais

18

Council of Europe	II. International standards: the Convention on Cybercrime	II. Normas internacionais: a Convenção sobre o Cibercrime
<p>Legal conditions for efficient investigations</p> <p>Issues:</p> <ul style="list-style-type: none"> ➤ Need for efficient investigations ➤ Probably 99.99% legitimate users ➤ Security versus privacy, freedom of expression and other civil rights ➤ Efficient investigations versus due process 	<p>Condições legais eficientes para investigações</p> <p>Questões:</p> <ul style="list-style-type: none"> ➤ Necessidade de investigações eficazes ➤ Provavelmente 99,99% de utilizadores legítimos ➤ Segurança versus privacidade, liberdade de expressão e outros direitos civis ➤ Investigações eficazes versus o devido processo 	

19

Council of Europe	II. International standards: the Convention on Cybercrime	II. Normas internacionais: a Convenção sobre o Cibercrime
<p>Conditions for efficient international cooperation</p> <ul style="list-style-type: none"> ➤ Harmonise legislation between countries ➤ Create legal basis for judicial cooperation ➤ Direct, immediate police cooperation ➤ Immediate measures based on requests from other countries ➤ Join international agreements 	<p>Condições para uma cooperação internacional eficaz</p> <ul style="list-style-type: none"> ➤ Harmonizar a legislação entre os países ➤ Criar uma base legal para a cooperação judiciária ➤ Cooperação directa e imediata com a polícia ➤ Medidas imediatas baseadas em pedidos de outros países ➤ Aderir a acordos internacionais 	

20

Council of Europe	II. International standards: the Convention on Cybercrime	II. Normas internacionais: a Convenção sobre o Cibercrime
<p>A response to this challenge:</p> <p>The Convention on Cybercrime</p> <ul style="list-style-type: none"> ➤ Elaborated by the Council of Europe with the participation of Canada, Japan, South Africa and the USA ➤ Opened for signature in Budapest in November 2001 ➤ In force since July 2004 <p>The Protocol on Xenophobia and Racism Committed through Computer Systems</p> <ul style="list-style-type: none"> ➤ Opened for signature in January 2003 ➤ In force since March 2006 	<p>Uma resposta a este desafio:</p> <p>A Convenção sobre o Cibercrime</p> <ul style="list-style-type: none"> ➤ Elaborada pelo Conselho da Europa com a participação do Canadá, Japão, África do Sul e EUA ➤ Aberta a assinatura em Budapeste, em Novembro de 2001 ➤ Em vigor desde Julho de 2004 <p>O Protocolo relativo à Incriminação de Actos de Natureza Racista ou Xenófoba Cometidos através de Sistemas Informáticos</p> <ul style="list-style-type: none"> ➤ Aberto a assinatura em Janeiro de 2003 ➤ Em vigor desde Março de 2006 	

21

Council of Europe	II. International standards: the Convention on Cybercrime	II. Normas internacionais: a Convenção sobre o Cibercrime
<p>Structure and content of the Convention</p> <p>Chapter I: Definitions</p> <p>Chapter II: Measures at national level Section 1 - Substantive criminal law Section 2 - Procedural law Section 3 - Jurisdiction</p> <p>Chapter III: International cooperation Section 1 - General principles Section 2 - Specific provisions</p> <p>Chapter IV: Final provisions</p>	<p>Estrutura e conteúdo da convenção</p> <p>Capítulo I – Terminologia</p> <p>Capítulo II: Medidas a tomar a nível nacional Secção 1 - Direito penal material Secção 2 – Direito Processual Secção 3 - Competência</p> <p>Capítulo III – Cooperação Internacional Secção 1 – Princípios gerais Secção 2 – Disposições específicas</p> <p>Capítulo IV – Disposições Finais</p>	

22

Criminalising conduct

Chapter II – Measures at national level

Section 1 – Substantive criminal law

- Title 1 - Offences against the confidentiality, integrity and availability of computer data and systems (illegal access, illegal interception, data interference, system interference, misuse of devices)
- Title 2 – Computer-related offences (forgery, fraud)
- Title 3 – Content-related offences (child pornography)
- Title 4 – Infringements of copyright and related rights
- Title 5 – Ancillary liability and sanctions (attempt, aiding, abetting, corporate liability, sanctions and measures)

Penalização conduta

Capítulo II – Medidas a tomar a nível nacional

Secção 1 – Direito penal material

- Título 1 – Infracções contra a confidencialidade, integridade e disponibilidade de sistemas informáticos e dados informáticos (Acesso ilegítimo , Intercepção ilegítima , Interferência em dados , Interferência em sistemas , Uso abusivo de dispositivos)
- Título 2 – Infracções relacionada com computadores (Falsidade informática, Burla informática)
- Título 3 – Infracções relacionadas com o conteúdo (Infracções relacionadas com pornografia infantil)
- Título 4 – Infracções relacionadas com a violação do direito de autor e direitos conexos
- Título 5 – Outras formas de Responsabilidade e Sanções (Tentativa e cumplicidade , responsabilidade de pessoas colectivas , sanções e medidas)

23

23

Procedural tools

Section 2 – Procedural law

- Title 1 – Common provisions (scope of procedural provisions, conditions and safeguards)
- Title 2 – Expedited preservation of stored computer data (and traffic data and partial disclosure)
- Title 3 – Production order
- Title 4 – Search and seizure of stored computer data
- Title 5 – Real-time collection of computer data (traffic data, interception of content data)

These apply to all criminal offences involving a computer system!

Instrumentos processuais

Secção 2 – Direito Processual

- *Título 1 – Disposições comuns (Âmbito das disposições processuais , Condições e salvaguardas)*
- *Título 2 – Conservação expedita de dados informáticos armazenados (Conservação expedita de dados informáticos armazenados e divulgação parcial de dados de tráfego)*
- *Título 3 – Injunção*
- *Título 4 – Busca e Apreensão de dados informáticos armazenados*
- *Título 5 – Recolha em tempo real de dados informáticos (Recolha em tempo real de dados relativos ao tráfego, intercepção de dados relativos ao conteúdo)*

Estes se aplicam a todos os crimes que envolvem um sistema de computador!

24

24

Art 15 Common provisions

Scope of procedural provisions

- Apply to all offences involving a computer system

Conditions and safeguards

- powers and procedures to be subject to conditions and safeguards provided for under domestic law, which shall provide for the adequate protection of human rights and liberties
- principle of proportionality
- judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure

Art 15 *Disposições comuns*

Âmbito das disposições processuais

- Aplicável a todos os crimes que envolvem um sistema de computador

Condições e salvaguardas

- dos poderes e procedimentos previstos e sujeitos às condições e salvaguardas estabelecidas pela legislação nacional, que deve assegurar uma protecção adequada dos direitos do Homem e das liberdades
- princípio da proporcionalidade
- um controlo judicial ou outras formas de controlo independente, os fundamentos que justificam a sua aplicação, bem como a limitação do âmbito de aplicação e a duração do poder ou procedimento

25

25

Art 16 Expedited preservation of stored computer data

- enable the competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification
- oblige a person to preserve and maintain the integrity of that computer data for a period of time as long as necessary to enable the competent authorities to seek its disclosure

Art 16 Conservação expedita de dados informáticos armazenados

- permitir às suas autoridades competentes exigir ou obter de uma outra forma a conservação expedita de dados informáticos específicos, incluindo dados relativos ao tráfego, armazenados por meio de um sistema informático, nomeadamente nos casos em que existem motivos para pensar que os mesmos são susceptíveis de perda ou alteração
- para obrigar essa pessoa a conservar e proteger a integridade dos referidos dados durante um período de tempo tão longo quanto necessário.

26

26

Chapter III - International cooperation

Section 1 – General principles

Section 2 – Specific provisions

- Art 29 - Expedited preservation of stored computer data
- Art 30 - Expedited disclosure of preserved computer data
- Art 31 - Mutual assistance re accessing stored computer data
- Art 32 - Trans-border access to stored computer data (public/with consent)
- Art 33 - Mutual assistance in real-time collection of traffic data
- Art 34 - Mutual assistance re interception of content data
- Art 35 - 24/7 network

27

Capítulo III – Cooperação Internacional

Secção 1 – Princípios gerais

Secção 2 – Disposições específicas

- Artigo 29º - Conservação expedita de dados informáticos armazenados
- Artigo 30º - Divulgação expedita dos dados de tráfego conservados
- Artigo 31º - Auxílio mútuo relativamente ao acesso a dados informáticos armazenados
- Artigo 32º - Acesso transfronteiriço a dados informáticos armazenados, com consentimento ou quando são acessíveis ao público
- Artigo 33º - Auxílio mútuo relativamente à recolha de dados de tráfego em tempo real
- Artigo 34º - Auxílio mútuo em matéria de intercepção de dados de conteúdo
- Artigo 35º - Rede 24/7

27

Article 35 – 24/7 Network

Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance ... Such assistance shall include facilitating, or ... directly carrying out the following measures:

- the provision of technical advice;
- the preservation of data pursuant to Articles 29 and 30;
- the collection of evidence, the provision of legal
- information, and locating of suspects.

Based on the G8 experience

28

Artigo 35º - Rede 24/7

Cada Parte designará um ponto de contacto disponível 24 horas sobre 24 horas, 7 dias por semana, a fim de assegurar a prestação de assistência imediata ... O auxílio incluirá a facilitação, ou ... a aplicação directa das seguintes medidas:

- A prestação de aconselhamento técnico
- A conservação de dados em conformidade com os artigos 29º e 30º; e
- A recolha de provas, informações de carácter jurídico
- Localização de suspeitos.

Com base na experiência do G8

28

Chapter III - International cooperation

Art 37 Convention is open for accession by third countries

➤ Global scope of the Convention

Capítulo III – Cooperação Internacional

Art. 37º Convenção está aberta à adesão por países terceiros

➤ Âmbito global da Convenção

29

29

Supervision of the treaty

Art 46 Consultation of the Parties (Cybercrime Convention Committee, T-CY)

- Facilitate effective implementation of the treaty and identify problems
- Facilitate information exchange
- Consider possible amendments or supplements to the treaty

Supervisão do tratado

Art. 46º Consulta entre as Partes (Comité da Convenção sobre o Cibercrime, T-CY)

- Facilitar a eficaz implementação do tratado e identificar problemas
- Facilitar o intercâmbio de informação
- Considerar possíveis alterações ou suplementos ao tratado

30

30

Implementation – current status

- The Convention entered into force in July 2004
- 23 ratifications + 22 signatures
- Signed by Canada, Japan, South Africa, ratified by USA
- Costa Rica, Mexico, Philippines have been invited to accede
- Legislative amendments adopted or underway in many other countries and accession to the Convention under consideration
- = Major global trend towards better cybercrime legislation
- = Convention provides a global standard

Implementação – situação actual

- A Convenção entrou em vigor em Julho de 2004
- 23 ratificações + 22 assinaturas
- Assinada pelo Canadá, Japão, África do Sul, ratificada pelos EUA
- Costa Rica, México e Filipinas foram convidados a aderir
- Alterações legislativas adoptadas ou em curso em muitos outros países e adesão à Convenção a ser considerada
- = Importante tendência global para uma melhor legislação sobre o cibercrime
- = A Convenção proporciona um padrão global

31

31

Harmonising legislation:

- Use Convention on Cybercrime as a guideline or model law

Legal basis for judicial cooperation:

- As many countries as possible to become a party to the Convention

Harmonização da legislação:

- Utilizar a Convenção sobre o Cibercrime como directriz ou lei modelo

Base legal para a cooperação judiciária:

- Tantos países quantos possível deverão tornar-se parte da Convenção

32

32

International cooperation:

- **Need maximum number of parties**
- **Need efficient, immediate measures**
- **Need to back up immediate police cooperation with efficient judicial cooperation**

Cooperação internacional:

- **Necessário número máximo de partes**
- **Necessárias medidas eficazes e imediatas**
- **É necessário reforçar a cooperação imediata com a polícia com uma cooperação judiciária eficaz**

33

33

Law enforcement authorities (LEA) / Internet service provider (ISP) cooperation**Issues:**

- **LEA and ISP play crucial role in a secure Internet**
- **Need for LEA / ISP cooperation in the investigation of cybercrime**
- **Ensure efficient work of LEA**
- **Protect ability of ISP to provide services**
- **Ensure due process**
- **Protect rights of users**
- **How to enhance, how to structure cooperation?**

Cooperação entre as autoridades responsáveis pela aplicação da lei (ARAL) e o fornecedor de serviços de Internet (FSI)**Questões:**

- **ARAL e FSI desempenham papel crucial numa Internet segura**
- **Necessária cooperação entre as ARAL e o FSI na investigação do cibercrime**
- **Assegurar um trabalho eficaz das ARAL**
- **Proteger a capacidade do FSI de fornecer serviços**
- **Assegurar o devido processo**
- **Proteger os direitos dos utilizadores**
- **Como melhorar e como estruturar a cooperação?**

34

34

Guidelines for the cooperation between law enforcement and internet service providers against cybercrime

Adopted at the global Conference on Cooperation against Cybercrime (Council of Europe, Strasbourg, 1-2 April 2008):

- Common measures (including protection of rights and freedoms)
- Measures to be taken by law enforcement
- Measures to be taken by service providers

Directrizes para a cooperação entre as autoridades responsáveis pela aplicação da lei e os fornecedores de serviços de Internet no combate ao cibercrime

Adoptadas na Conferência Global sobre a Cooperação no Combate ao Cibercrime (Conselho da Europa, Estrasburgo, 1-2 de Abril de 2008):

- Medidas comuns (incluindo protecção dos direitos e liberdades)
- Medidas a serem tomadas pelas autoridades responsáveis pela aplicação da lei
- Medidas a serem tomadas pelos fornecedores de serviços

35

35

III. Procedural tools and international cooperation

III. Ferramentas procedimentais e cooperação internacional

Alexander Seger
Economic Crime Division, Council of Europe
Strasbourg, France
alexander.seger@coe.int

www.coe.int/cybercrime

36

36

Procedural tools

Issues:

- Need for efficient investigations
- Probably 99.99% legitimate users
- Security versus privacy, freedom of expression and other civil rights
- Efficient investigations versus due process

Ferramentas procedimentais

Questões:

- Necessidade de investigações eficazes
- Provavelmente 99,99% de utilizadores legítimos
- Segurança versus privacidade, liberdade de expressão e outros direitos civis
- Investigações eficazes versus o devido processo

37

37

Procedural tools

Convention on Cybercrime

Section 2 – Procedural law

- Title 1 – Common provisions (scope of procedural provisions, conditions and safeguards)
- Title 2 – Expedited preservation of stored computer data (and traffic data and partial disclosure)
- Title 3 – Production order
- Title 4 – Search and seizure of stored computer data
- Title 5 – Real-time collection of computer data (traffic data, interception of content data)

Instrumentos processuais

Convenção sobre o cibercrime Secção 2 – Direito Processual

- Título 1 – *Disposições comuns* (Âmbito das disposições processuais, Condições e salvaguardas)
- Título 2 – *Conservação expedita de dados informáticos armazenados* (Conservação expedita de dados informáticos armazenados e divulgação parcial de dados de tráfego)
- Título 3 – *Injunção*
- Título 4 – *Busca e Apreensão de dados informáticos armazenados*
- Título 5 – *Recolha em tempo real de dados informáticos* (Recolha em tempo real de dados relativos ao tráfego, interceptação de dados relativos ao conteúdo)

38

38

Art 15 Common provisions

Scope of procedural provisions

- Apply to all offences involving a computer system

Conditions and safeguards

- powers and procedures to be subject to conditions and safeguards provided for under domestic law, which shall provide for the adequate protection of human rights and liberties
- principle of proportionality
- judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure

Art 15 *Disposições comuns*

Âmbito das disposições processuais

- Aplicável a todos os crimes que envolvem um sistema de computador

Condições e salvaguardas

- dos poderes e procedimentos previstos e sujeitos às condições e salvaguardas estabelecidas pela legislação nacional, que deve assegurar uma protecção adequada dos direitos do Homem e das liberdades
- princípio da proporcionalidade
- um controlo judicial ou outras formas de controlo independente, os fundamentos que justificam a sua aplicação, bem como a limitação do âmbito de aplicação e a duração do poder ou procedimento

39

39

Art 16 Expedited preservation of stored computer data

- enable the competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification
- oblige a person to preserve and maintain the integrity of that computer data for a period of time as long as necessary to enable the competent authorities to seek its disclosure

Art 16 Conservação expedita de dados informáticos armazenados

- permitir às suas autoridades competentes exigir ou obter de uma outra forma a conservação expedita de dados informáticos específicos, incluindo dados relativos ao tráfego, armazenados por meio de um sistema informático, nomeadamente nos casos em que existem motivos para pensar que os mesmos são susceptíveis de perda ou alteração
- para obrigar essa pessoa a conservar e proteger a integridade dos referidos dados durante um período de tempo tão longo quanto necessário.

40

40

Art 17 Expedited preservation and partial disclosure of traffic data

- ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication
- ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted

Expedited preservation versus data retention

41

Art 17 Conservação expedita e divulgação parcial de dados de tráfego

- A fim de assegurar a conservação de dados relativos ao tráfego, cada Parte adoptará as medidas legislativas e outras que se revelem necessárias assegurar a conservação rápida desses dados de tráfego, quer tenham participado na transmissão dessa comunicação um ou vários fornecedores de serviços
- Assegurar a divulgação rápida à autoridade competente da Parte ou a uma pessoa designada por essa autoridade, de uma quantidade de dados de tráfego, suficiente para permitir a identificação dos fornecedores de serviços e da via através do qual a comunicação foi efectuada

Acelerada preservação versus a conservação de dados

41

Art 18 Production order

Empower competent authorities to order:

- a person in its territory to submit specified computer data
- a service provider to submit subscriber information

“Subscriber information” means any information relating to subscribers of its services other than traffic or content data and by which can be established:

- the type of communication service used, the technical provisions taken thereto and the period of service;
- the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement

42

Art 18 Injunção

Habilitar as autoridades competentes a fim:

- A uma pessoa que comunique os dados informáticos específicos,
- A um fornecedor de serviços, relativos aos assinantes e respeitantes a esses serviços

“Dados relativos aos assinantes” designa qualquer informação, diferentes dos dados relativos ao tráfego ou ao conteúdo e que permitam determinar:

- O tipo de serviço de comunicação utilizado, as medidas técnicas tomadas a esse respeito e o período de serviço;
- A identidade, a morada postal ou geográfica e o número de telefone do assinante, e qualquer outro número de acesso, os dados respeitantes à facturação e ao pagamento, disponíveis com base num contrato ou acordo de serviços

42

Art 19 Search and seizure of stored computer data

Empower competent authorities to search or similarly access:

- a computer system or part of it and computer data stored therein
- a computer-data storage

Ensure that authorities are able to expeditiously extend the search or similar accessing to another system.

Art 19 Busca e apreensão de dados informáticos armazenados

Habilitar as suas autoridades competentes para proceder a buscas ou aceder de modo semelhante :

- A um sistema informático ou a uma parte do mesmo, bem como a dados informáticos que nele se encontrem armazenados
- A um suporte que permita armazenar dados informáticos.

assegurar que suas autoridades procedam de estender de forma expedita a busca, ou o acesso de forma semelhante ao outro sistema.

43

43

Art 19 Search and seizure of stored computer data

Empower competent authorities to:

- seize or similarly secure a computer system or part of it or a computer-data storage medium;
- make and retain a copy of those computer data;
- maintain the integrity of the relevant stored computer data;
- render inaccessible or remove those computer data in the accessed computer system.
- order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide the necessary information to permit a search or seizure

Art 19 Busca e apreensão de dados informáticos armazenados

Habilitar as autoridades competentes a:

- Apreender ou obter de forma semelhante um sistema informático ou uma parte deste ou um suporte de armazenamento informático ;
- Realizar e conservar uma cópia desses dados informáticos ;
- Preservar a integridade dos dados informáticos pertinentes armazenados ;
- Tornar inacessíveis ou eliminar esses dados do sistema informático acedido .
- Ordenar a qualquer pessoa que conheça o funcionamento do sistema informático ou as medidas utilizadas para proteger os dados informáticos nele contidos, que forneça na medida do razoável as informações razoavelmente necessárias

44

44

Art 20 Real-time collection of traffic data

Empower competent authorities to:

- collect or record through the application of technical means on the territory of that Party,
- compel a service provider, within its existing technical capability:
 - to collect or record; or
 - to co-operate and assist the competent authorities in the collection or recording of,

traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.

Art 20 Recolha em tempo real de dados relativos ao tráfego

Habilitar as autoridades competentes a:

- Recolher ou registar, através da aplicação de meios técnicos existentes no seu território,
- Obrigar um fornecedor de serviços, no âmbito da sua capacidade técnica existente:

- Recolher ou registar por meio da aplicação de meios técnicos no seu território, ou
- Prestar às autoridades competentes o seu apoio e assistência para recolher ou registar,

em tempo real, dados de tráfego relativos a comunicações específicas no seu território transmitidas através de um sistema informático .

45

45

Art 21 Interception of content data

Empower competent authorities to:

- collect or record, and
- compel a service provider, within its existing technical capability:
 - to collect or record; or
 - to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications

The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Art 21 Intercepção de dados relativos ao conteúdo

Habilitar as autoridades competentes a :

- Recolher ou registar
- Obrigar um fornecedor de serviços, no âmbito da sua capacidade técnica existente, a:
 - Recolher ou registar, ou
 - Prestar às autoridades competentes o seu apoio e a sua assistência para recolher ou registar, em tempo real, dados relativos ao conteúdo de comunicações específicas

Os poderes e procedimentos referidos no presente artigo devem estar sujeitos aos artigos 14º e 15º.

46

46

International cooperation

Conditions for efficient international cooperation:

- Harmonise legislation between countries
- Create legal basis for judicial cooperation
- Direct, immediate police cooperation
- Immediate measures based on requests from other countries
- Join international agreements

Problem: scattering and layering of crime, damage and proceeds

47

Cooperação internacional

Condições para uma eficiente cooperação internacional:

- Harmonizar a legislação entre os países
- Criar uma base legal para a cooperação judiciária
- Cooperação directa e imediata com a polícia
- Medidas imediatas baseadas em pedidos de outros países
- Aderir a acordos internacionais

Problema: distribuição e estratificação do crime, danos e produto dos crimes

47

Harmonising legislation:

- Use Convention on Cybercrime as a guideline or model law

Legal basis for judicial cooperation:

- As many countries as possible to become a party to the Convention

48

Harmonização da legislação:

- Utilizar a Convenção sobre o Cibercrime como directriz ou lei modelo

Base legal para a cooperação judiciária:

- Tantos países quantos possível deverão tornar-se parte da Convenção

48

Council of Europe	III. Procedural tools and international cooperation	III. Ferramentas procedimentais e cooperação internacional
<p>Convention on Cybercrime Chapter III - International cooperation</p> <p>Parties to the Convention agree to cooperate with each other to the widest extent possible</p> <p>Section 1 – General principles</p> <ul style="list-style-type: none"> • Art 23 General principles on international cooperation • Art 24 Principles related to extradition • Art 25 Principles related to mutual legal assistance • Art 26 Spontaneous information • Art 27 MLA in the absence of applicable international instruments • Art 28 Confidentiality and limitation on use 	<p>Convenção sobre o Cibercrime Capítulo III – Cooperação Internacional</p> <p>As Partes cooperarão entre si na medida mais ampla possível</p> <p>Secção 1 – Princípios gerais</p> <p>Artigo 23º - Princípios gerais relativos à cooperação internacional Artigo 24º - Extradicação Artigo 25º - Princípios gerais relativos ao auxílio mútuo. Artigo 26º - Informação espontânea Artigo 27º - Procedimentos relativos aos pedidos de auxílio mútuo na ausência de acordos internacionais aplicáveis Artigo 28º - Confidencialidade e restrição de utilização</p>	

49

Council of Europe	III. Procedural tools and international cooperation	III. Ferramentas procedimentais e cooperação internacional
<p>Chapter III - International cooperation</p> <p>Section 2 – Specific provisions</p> <ul style="list-style-type: none"> • Art 29 - Expedited preservation of stored computer data • Art 30 - Expedited disclosure of preserved computer data • Art 31 - Mutual assistance re accessing stored computer data • Art 32 - Trans-border access to stored computer data (public/with consent) • Art 33 - Mutual assistance in real-time collection of traffic data • Art 34 - Mutual assistance re interception of content data • Art 35 - 24/7 network 	<p>Capítulo III – Cooperação Internacional</p> <p>Secção 2 – Disposições específicas</p> <ul style="list-style-type: none"> • Art 29º - Conservação expedita de dados informáticos armazenados • Art 30º - Divulgação expedita dos dados de tráfego conservados • Art 31º - Auxílio mútuo relativamente ao acesso a dados informáticos armazenados • Art 32º - Acesso transfronteiriço a dados informáticos armazenados, com consentimento ou quando são acessíveis ao público • Art 33º - Auxílio mútuo relativamente à recolha de dados de tráfego em tempo real • Art 34º - Auxílio mútuo em matéria de intercepção de dados de conteúdo • Art 35º - Rede 24/7 	

50

Article 35 – 24/7 Network

Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance ... Such assistance shall include facilitating, or ... directly carrying out the following measures:

- the provision of technical advice;
- the preservation of data pursuant to Articles 29 and 30;
- the collection of evidence, the provision of legal
- information, and locating of suspects.

Based on the G8 experience

Artigo 35º - Rede 24/7

Cada Parte designará um ponto de contacto disponível 24 horas sobre 24 horas, 7 dias por semana, a fim de assegurar a prestação de assistência imediata ... O auxílio incluirá a facilitação, ou ... a aplicação directa das seguintes medidas:

- A prestação de aconselhamento técnico
- A conservação de dados em conformidade com os artigos 29º e 30º; e
- A recolha de provas, informações de carácter jurídico
- Localização de suspeitos.

Com base na experiência do G8

51

51

International cooperation:

- Need maximum number of parties
- Need efficient, immediate measures
- Need to back up immediate police cooperation with efficient judicial cooperation

Cooperação internacional:

- Necessário número máximo de partes
- Necessárias medidas eficazes e imediatas
- É necessário reforçar a cooperação imediata com a polícia com uma cooperação judiciária eficaz

52

52

IV. Law enforcement/ service provider cooperation

Alexander Seger
Economic Crime Division, Council of Europe
Strasbourg, France
alexander.seger@coe.int

53

IV. Cooperação entre as autoridades responsáveis pela aplicação da lei e o fornecedor de serviços

www.coe.int/cybercrime

53

Law enforcement authorities (LEA) / Internet service provider (ISP) cooperation

Issues:

- LEA and ISP play crucial role in a secure Internet
- Need for LEA / ISP cooperation in the investigation of cybercrime
- Ensure efficient work of LEA
- Protect ability of ISP to provide services
- Ensure due process
- Protect rights of users
- How to enhance, how to structure cooperation?

Cooperação entre as autoridades responsáveis pela aplicação da lei (ARAL) e o fornecedor de serviços de Internet (FSI)

Questões:

- ARAL e FSI desempenham papel crucial numa Internet segura
- Necessária cooperação entre as ARAL e o FSI na investigação do cibercrime
- Assegurar um trabalho eficaz das ARAL
- Proteger a capacidade do FSI de fornecer serviços
- Assegurar o devido processo
- Proteger os direitos dos utilizadores
- Como melhorar e como estruturar a cooperação?

54

54

Guidelines for the cooperation between law enforcement and internet service providers against cybercrime

Adopted at the global Conference on Cooperation against Cybercrime (Council of Europe, Strasbourg, 1-2 April 2008):

- Common measures (including protection of rights and freedoms)
- Measures to be taken by law enforcement
- Measures to be taken by service providers

Directrizes para a cooperação entre as autoridades responsáveis pela aplicação da lei e os fornecedores de serviços de Internet no combate ao cibercrime

Adoptadas na Conferência Global sobre a Cooperação no Combate ao Cibercrime (Conselho da Europa, Estrasburgo, 1-2 de Abril de 2008):

- Medidas comuns (incluindo protecção dos direitos e liberdades)
- Medidas a serem tomadas pelas autoridades responsáveis pela aplicação da lei
- Medidas a serem tomadas pelos fornecedores de serviços

55

55

Common guidelines for LEA and ISP:

- Develop a culture of cooperation
- Develop written procedures for cooperation with each other
- Cooperate for the protection of rights and freedoms of individuals
- Respect each others roles, rights and limitations
- Mindful of cost of cooperation
- Etc

Directrizes comuns para as ARAL e os FSI:

- Desenvolver uma cultura de cooperação
- Desenvolver procedimentos escritos para a cooperação mútua
- Cooperar para a protecção dos direitos e liberdades dos indivíduos
- Respeitar os papéis, direitos e limitações uns dos outros
- Ter em atenção o custo da cooperação
- Etc.

56

56

Measures to be taken by law enforcement

- Broad and strategic cooperation with ISP
- Procedures for legally binding requests
- Designated and trained personnel for cooperation
- Verification of source of requests
- Standard request format
- Specificity and accuracy of requests
- Follow preservation orders with production/disclosure orders
- Criminal compliance programme
- International requests: 24/7 network and formal mutual legal assistance

Medidas a serem tomadas pelas autoridades responsáveis pela aplicação da lei

- Cooperação ampla e estratégica com os FSI
- Procedimentos para pedidos legalmente vinculativos
- Pessoal nomeado e formado para a cooperação
- Verificação da fonte dos pedidos
- Formato padrão do pedido
- Especificidade e exactidão dos pedidos
- Ordens de conservação seguidas por injunção/divulgação
- Programa de cumprimento na área criminal
- Pedidos internacionais: rede 24/7 e assistência jurídica mútua formal

57

57

Measures to be taken by ISP

- Report criminal incidents
- Assist LEA with training and other support
- Procedures for responding to requests
- Designated and trained personnel for cooperation
- Emergency assistance outside business hours
- Criminal compliance programme
- Verification of source of requests
- Standard response format
- Explanation for information not provided
- Coordination among ISP

Medidas a serem tomadas pelos FSI

- Participar incidentes criminais
- Auxiliar as ARAL com a formação e outro apoio
- Procedimentos para responder a pedidos
- Pessoal nomeado e formado para a cooperação
- Auxílio de emergência fora das horas de expediente
- Programas de cumprimento na área criminal
- Verificação da fonte de pedidos
- Formato padrão da resposta
- Explicação para a informação não fornecida
- Coordenação entre os FSI

58

58

Important:

- **Guidelines, not binding**
- **Not substitute for procedural law and other formal regulations**
- **Based on good practices already available**
- **Help LEA and ISP in any country to structure their cooperation**

Importante:

- **Directrizes, não vinculativas**
- **Não são um substituto para o direito processual e outros regulamentos formais**
- **Baseadas nas boas práticas já disponíveis**
- **Ajudam as ARAL e os FSI em qualquer país a estruturar a sua cooperação**

59

Obrigado.**Alexander.seger@coe.int**

60

60