

# Projecto sobre a Cibercriminalidade [www.coe.int/cybercrime](http://www.coe.int/cybercrime)



COUNCIL OF EUROPE    CONSEIL DE L'EUROPE

et le

e a

## Rede de Lisboa

[www.coe.int/lisbon-network](http://www.coe.int/lisbon-network)

Serviço da Sociedade da  
Informação e do Combate  
contra a Criminalidade  
Direcção-Geral dos  
Direitos Humanos e dos s  
Assuntos Jurídicos  
Estrasburgo, França

8 de Outubro de 2009

# **Formação dos juízes e dos procuradores em matéria de cibercriminalidade: um conceito**

Este documento foi elaborado por um grupo de trabalho multilateral no quadro do Projecto sobre o Cibercriminalidade e da Rede de Lisboa de Instituições de Formação do Conselho da Europa.

**Contacto:**

Para mais informações, por favor contactar:

Serviço da Sociedade da Informação e do Combate  
contra a Criminalidade  
Direcção-Geral dos Direitos Humanos e dos Assuntos  
Jurídicos  
Conselho da Europa  
Estrasburgo, França

Tel.: +33-3-9021-4506

Fax: +33-3-9021-5650

E-mail: [alexander.seger@coe.int](mailto:alexander.seger@coe.int)

**Termo de responsabilidade:**

Este relatório técnico não reflecte necessariamente as posições oficiais do Conselho da Europa nem das entidades financiadoras deste projecto, nem das Partes dos instrumentos referidos no presente documento.

# Índice

<b>1</b>	<b>Resumo executivo</b>	<b>4</b>
<b>2</b>	<b>Introdução</b>	<b>7</b>
<b>3</b>	<b>Instituições e sistemas de formação</b>	<b>9</b>
<b>4</b>	<b>Competências e conhecimentos necessários para juízes e procuradores</b>	<b>12</b>
4.1	Conhecimentos elementares	12
4.2	Conhecimentos aprofundados	15
4.3	Conhecimentos especializados	18
<b>5</b>	<b>Formação actual em matéria de cibercriminalidade e provas electrónicas</b>	<b>20</b>
5.1	Formação inicial	20
5.2	Formação em exercício	21
<b>6</b>	<b>Abordagem proposta</b>	<b>25</b>
6.1	Objectivo	25
6.2	Institucionalização da formação inicial	25
6.3	Institucionalização da formação em exercício	25
6.4	Formações e módulos normalizados e replicáveis	26
6.5	Acesso aos materiais de formação/autoformação	26
6.6	Centros piloto de formação básica e avançada	27
6.7	Enriquecimento dos conhecimentos através do trabalho em rede	27
6.8	Cooperação público-privado	28
<b>7</b>	<b>Apoio à implementação deste conceito</b>	<b>30</b>
<b>8</b>	<b>Anexo</b>	<b>31</b>
8.1	Rede de Lisboa: Ligações com as instituições de formação judiciária	31
8.2	Exemplos de formações de nível elementar: estrutura e temas abordados	32
8.2.1	Exemplo da formação dada nos Países Baixos	32
8.2.2	Exemplo da formação dada na Alemanha (Academia da Magistratura alemã)	32
8.2.3	Exemplos de formações do Conselho da Europa	33
8.3	Exemplos de formações de nível avançado: estrutura e temas abordados	36
8.3.1	Exemplo da formação dada nos Países Baixos	36
8.3.2	Proposta de formação de nível superior dos Países Baixos	37

# 1 Resumo executivo

Tendo em conta a dependência das sociedades do mundo inteiro relativamente às tecnologias da informação e da comunicação, os juizes e os procuradores devem estar preparados para lidar com a questão da cibercriminalidade e das provas electrónicas. Apesar de, em inúmeros países, as forças da ordem já terem conseguido reforçar as suas capacidades de investigação da cibercriminalidade e de recolha de provas electrónicas, o mesmo não parece ser o caso relativamente aos juizes e procuradores. A experiência sugere que, na maioria dos casos, os juizes e os procuradores deparam com dificuldades na adaptação às novas realidades do mundo virtual. Assim sendo, há que envidar esforços especiais para conferir aos juizes e aos procuradores a capacidade para instaurarem processos penais e se pronunciarem em matéria de cibercriminalidade, bem como para utilizarem provas electrónicas, através da formação, da ligação em rede e da especialização.

O presente conceito visa apoiar esses esforços. Foi elaborado no decurso de 2009 pelo Projecto sobre a Cibercriminalidade e pela Rede de Lisboa de instituições de formação judiciária do Conselho da Europa, em colaboração com um grupo de trabalho multilateral.

O objectivo do conceito é ajudar as instituições de formação judiciária a criarem programas de formação sobre cibercriminalidade e provas electrónicas para juizes e procuradores, e integrar essa formação na formação inicial e na formação em exercício (isto é, institucionalizá-la). Irá, além disso, facilitar o trabalho em rede dos juizes e procuradores, a fim de favorecer o desenvolvimento dos seus conhecimentos, bem como providenciar um apoio sistemático, e não pontual, às iniciativas de formação das partes interessadas.

O conceito abrange os seguintes elementos:

## **Objectivos**

De modo geral, a formação inicial e em exercício que é dada actualmente não dota os juizes e os procuradores do nível de conhecimentos exigido para lidarem com a cibercriminalidade e as provas electrónicas.

Assim, os objectivos de um conceito de formação para juizes e procuradores devem ser:

- Permitir às instituições de formação a prestação de formação inicial e em serviço em matéria de cibercriminalidade com base nas normas internacionais
- Dotar o maior número possível de juizes e procuradores em exercício e de candidatos a juizes e procuradores dos conhecimentos elementares em matéria de cibercriminalidade e de provas informáticas
- Providenciar formação avançada a um número consequente de juizes e procuradores;
- Apoiar a especialização e a formação técnica contínuas de juizes e procuradores
- Contribuir para um enriquecimento dos conhecimentos através do trabalho em rede entre juizes e procuradores
- Facilitar o acesso a diferentes redes e iniciativas de formação.

As seguintes medidas devem contribuir para a realização destes objectivos:

### **1. Institucionalização da formação inicial**

- Nos países onde a formação inicial consiste numa formação prática no local de trabalho, recomenda-se que, pelo menos parte dessa formação seja consagrada à cibercriminalidade e às provas electrónicas.
- Nos países onde a formação inicial é dada por instituições de formação judiciária, os programas devem conter no mínimo um módulo de nível elementar que incida na

cibercriminalidade e nas provas electrónicas. Estas questões devem, além disso, ser abordadas no quadro de módulos obrigatórios que incidam sobre o direito material e o direito processual. Devem ser ainda oferecidos módulos opcionais de nível avançado sobre cibercriminalidade e provas electrónicas.

- Os módulos de formação específicos devem ser normalizados de forma a serem replicáveis e a permitirem uma progressão dos candidatos entre o nível elementar e avançado.

## **2. Institucionalização da formação em exercício**

- As instituições de formação em exercício devem oferecer pelo menos um módulo de nível básico sobre cibercriminalidade e provas electrónicas de modo a dotar os juízes e procuradores em exercício dos conhecimentos de base que não adquiriram aquando da sua formação inicial
- Além disso, devem oferecer formação de nível avançado.

## **3. Formações e módulos normalizados e replicáveis**

- Devem ser criados módulos ou formações normalizados que possam ser replicados em grande escala e de forma rentável, e que permitam aos candidatos a juízes e procuradores, bem como aos juízes e procuradores em exercício uma progressão entre o nível elementar e o nível avançado.
- As formações de nível elementar existentes passíveis de ser integradas nos programas de formação inicial ou em exercício devem ser avaliadas. Poderia subsequentemente ser recomendada uma formação padrão às instituições de formação inicial e em exercício
- Poderia ser efectuada uma avaliação semelhante para as formações de nível avançado e, posteriormente, ser recomendada uma formação padrão de nível avançado
- Os formadores necessitariam de receber formação sobre o modo de dar essas formações de modo a permitir a realização dessa formação por formadores locais na língua local, limitando assim o recurso a formadores internacionais.

## **4. Acesso aos materiais de formação/autoformação**

- Devem ser criados materiais de formação que reflectam as normas internacionais e as boas práticas internacionais comuns. Devem ser disponibilizados às instituições de formação de acordo com critérios de rentabilidade tendo em vista a sua utilização ao nível local
- Se é verdade que os juízes e procuradores têm de receber formação sobretudo na aplicação da sua legislação nacional, é contudo possível criar materiais de formação normalizados que permitam integrar os sistemas e legislação nacionais
- Devem ser criados e disponibilizados cursos de formação online.

## **5. Centros piloto de formação básica e avançada**

- Devem ser criados vários centros piloto de formação básica e avançada para juízes e procuradores no domínio da cibercriminalidade e das provas electrónicas com o objectivo de testar e melhorar as formações e os materiais normalizados, divulgar as boas práticas, fazer investigação sobre a formação, manter um registo dos formadores, oferecer formação de formadores, providenciar formação a outros países com sistemas e línguas semelhantes
- Os centros piloto devem coordenar o seu trabalho entre si com o apoio do Conselho da Europa.
- Os juízes e procuradores que pretendam especializar-se devem considerar participar nas formações propostas pelos centros de excelência destinados às forças da ordem e ao sector privado.

## **6. Enriquecimento dos conhecimentos através do trabalho em rede**

- Para além da formação, a cooperação entre pares e o trabalho em rede entre juízes e procuradores, mas também entre as outras partes interessadas serão extremamente importantes
- Os juízes e procuradores devem utilizar as redes existentes para juízes ou procuradores (como a GPEN)
- A possibilidade da criação de uma rede internacional de juízes especializados em cibercriminalidade ou em criminalidade electrónica (semelhante à GPEN para os procuradores) deve ser analisada pelo Conselho da Europa.
- O Conselho da Europa e a Rede Europeia de Formação Judiciária devem apoiar o trabalho em rede entre as instituições europeias que oferecem formações em matéria de cibercriminalidade e provas electrónicas.
- Com vista a facilitar o acesso dos juízes e dos procuradores a estas redes de juízes e procuradores, assim como às inúmeras redes relacionadas com a cibercriminalidade, o Conselho da Europa deve fazer um recenseamento das iniciativas e das redes e criar um portal com os links, informação resumida e pormenores de contacto para cada rede. Esta medida deverá também facilitar a coordenação entre redes. Deve, além disso, facilitar o acesso aos materiais e iniciativas de formação existentes.

## **7. Cooperação público-privado**

- O apoio do sector privado à formação de juízes e procuradores seria benéfico, uma vez que o sector privado dispõe de conhecimentos altamente especializados sobre esta matéria. Ao mesmo tempo, os juízes e os procuradores têm de permanecer independentes e imparciais.
- As instituições de formação judiciária podem utilizar os conhecimentos especializados do sector privado na concepção dos programas de formação, na criação de materiais de formação e na realização das formações propriamente ditas.
- O apoio do sector às instituições de formação não pode ser visto como um meio potencial de assegurar decisões favoráveis dos tribunais ou de gerar negócios, mas sim de garantir que seja dada informação adequada aos juízes e procuradores que lhes permita tomar decisões informadas.
- O sector privado poderá apoiar com toda a transparência as organizações internacionais ou nacionais, as universidades, as iniciativas de formação ou outras entidades terceiras que, por sua vez, poderão dar apoio a instituições de formação independentes.
- Se os juízes e procuradores devem adquirir uma visão global sobre a internet e a cibercriminalidade, também é importante disponibilizar-lhes informações específicas relativas a determinadas plataformas informáticas. O sector poderá fornecer materiais para módulos específicos (em vez de cursos completos) sobre o funcionamento das plataformas principais.

A Rede de Lisboa do Conselho da Europa aprovou este conceito em Setembro de 2009 e recomendou que o mesmo fosse amplamente divulgado e implementado por parte das instituições de formação judiciária. Decidiu levá-lo à atenção do Conselho Consultivo dos Juízes Europeus e do Conselho Consultivo dos Procuradores Europeus, bem como da Comissão Europeia para a Eficiência da Justiça (CEPEJ) de modo a assegurar o maior apoio possível ao conceito.

## 2 Introdução

Nos últimos anos, as sociedades do mundo inteiro conseguiram avanços espectaculares no sentido da sua transformação em sociedades da informação. As tecnologias da informação e da comunicação (TIC) estão agora presentes em quase todos os aspectos da vida das pessoas. O recurso e, conseqüentemente, a dependência crescente relativamente às TIC torna as sociedades vulneráveis a ameaças como a cibercriminalidade, isto é, infracções cometidas contra ou através de dados e sistemas informáticos.

Para além do elevado número de infracções cometidas contra ou através das TIC, um número crescente de outros casos que acabam no tribunal estão relacionados com provas electrónicas armazenadas em sistemas informáticos ou outros dispositivos.

Por conseguinte, os juízes e procuradores têm de estar preparados para fazer face à cibercriminalidade e lidar com as provas electrónicas. Conforme afirmado pelo Conselho Consultivo dos Juízes Europeus<sup>1</sup>, "é essencial que os juízes, após terem completado estudos jurídicos completos, recebam uma formação elaborada, aprofundada e diversificada que lhes permita exercer as suas funções de forma satisfatória" (3.º parágrafo), "Essa formação é também uma garantia da sua independência e da sua imparcialidade" (4.º parágrafo) e "deve também ter em consideração a necessidade de uma sensibilidade social e de uma compreensão alargada das diferentes disciplinas que reflectem a complexidade da vida em sociedade" (27.º parágrafo). A importância das TIC é tal nas sociedades actuais que os juízes e os procuradores têm de ter, no mínimo, um conhecimento de nível elementar sobre essas tecnologias e problemas afins.

Se bem que em muitos Estados-Membros as forças da ordem conseguiram reforçar as suas capacidades para investigarem a cibercriminalidade e obter provas electrónicas, o mesmo não parece ter sucedido relativamente aos juízes e procuradores que, contudo, desempenham um papel crucial no processo penal. A experiência sugere que, na maioria dos casos, os juízes e os procuradores deparam com dificuldades na adaptação às novas realidades do mundo virtual.

Assim sendo, há que envidar esforços especiais para conferir aos juízes e aos procuradores a capacidade para instaurarem processos penais e para se pronunciarem em matéria de cibercriminalidade, bem como para utilizarem provas electrónicas através da formação, da ligação em rede e da especialização.

Os conhecimentos especializados do sector privado relativamente às novas tecnologias foram essenciais para a formação das forças da ordem. Serão igualmente úteis para a formação judiciária<sup>2</sup>, se bem que este potencial tenha, até à data, sido sub-aproveitado. Ao mesmo tempo, a independência e a imparcialidade dos juízes e procuradores têm de ser mantidas. Assim, são necessárias abordagens inovadoras que assegurem a independência dos juízes e procuradores, e que lhes permitam ao mesmo tempo ter acesso aos conhecimentos especializados do sector privado e compreender o funcionamento do sector e das tecnologias. O conceito aqui apresentado mostra de que modo as instituições de formação podem beneficiar do apoio do sector e das universidades através de programas de formação normalizados, bem como através de outros meios.

O objectivo do conceito apresentado neste relatório é ajudar as instituições de formação judiciária a criar programas de formação em matéria de cibercriminalidade e provas electrónicas para juízes

---

<sup>1</sup> Parecer nº 4 sobre a formação inicial e contínua para juízes, a nível nacional e europeu (CCJE (2003) Op. nº 4).

<sup>2</sup> Ver o estudo publicado em Março de 2009: "[Co-operation between LE, Industry and Academia to deliver long term sustainable training to key cybercrime personnel](#)."

e procuradores, e integrar essa formação na formação inicial e no exercício regular, isto é, institucionalizá-la).

O conceito fundamenta-se igualmente nas informações recebidas de instituições de formação da Alemanha, Bélgica, Croácia, Espanha, França, Geórgia, Países Baixos, Polónia, Portugal, Reino Unido, Roménia, e antiga República Jugoslava da Macedónia (respostas a um questionário recebidas em Junho de 2009), de um ateliê realizado em Portugal em Julho de 2009 com representantes da Bélgica, Irlanda, Itália, Portugal, Países Baixos e Reino Unido, bem como do sector privado, e de um ateliê realizado em Estrasburgo em 3 e 4 de Setembro de 2009 que contou com a participação de representantes das instituições de formação, juízes e procuradores dos países acima referidos, do sector privado e ainda da Rede Europeia de Formação Judiciária e da Rede de Lisboa do Conselho da Europa<sup>3</sup>.

Este processo multilateral conduziu à elaboração, pela primeira vez, de um conceito para a formação de juízes e procuradores em matéria de cibercriminalidade e provas electrónicas. O carácter participativo deste processo facilitará, sem dúvida, a cooperação de diferentes partes interessadas e a convergência dos conhecimentos e da especialização na aplicação do conceito.

A Rede de Lisboa do Conselho da Europa aprovou este conceito em Setembro de 2009 e recomendou que o mesmo fosse amplamente divulgado e implementado por parte das instituições de formação judiciária. Decidiu levá-lo à atenção do Conselho Consultivo dos Juízes Europeus e do Conselho Consultivo dos Procuradores Europeus, bem como da Comissão Europeia para a Eficiência da Justiça (CEPEJ) de modo a assegurar o maior apoio possível ao conceito.

---

<sup>3</sup> Rede de Lisboa para o Intercâmbio de Informação entre Pessoas e Entidades Responsáveis pela Formação de Juízes



### 3 Instituições<sup>4</sup> e sistemas de formação

Na Europa – como noutras regiões – os sistemas de formação dos juízes e dos procuradores divergem consideravelmente entre si<sup>5</sup>.

No que diz respeito à formação inicial, os sistemas correspondem geralmente a um ou uma combinação dos seguintes modelos<sup>6</sup>:

- Sistema A: Depois de terem concluído estudos superiores em Direito e, frequentes vezes, após terem passado um exame de admissão, os candidatos recebem formação específica num centro de formação judiciária para poderem exercer como juízes e/ou procuradores. Por vezes, os futuros juízes e procuradores recebem formação em conjunto, por vezes em instituições diferentes.
- Sistema B: Depois de terem concluído estudos superiores em Direito, os candidatos adquirem experiência prática no local de trabalho (por vezes no quadro de uma aprendizagem formal) em serviços do Ministério Público, em tribunais, em escritórios de advogados ou noutras instituições, antes de serem submetidos a um exame que os habilita a trabalhar como advogados, procuradores e juízes. Não passam por nenhuma instituição de formação centralizada específica<sup>7</sup>.

A formação em exercício, isto é, a formação profissional contínua dos juízes e dos procuradores em exercício, é oferecida quer por instituições públicas de formação judiciária que também são responsáveis pela formação inicial (p. ex., França, Geórgia, Países Baixos, Polónia, Portugal, Roménia, Espanha, “a antiga República Jugoslava da Macedónia”, Croácia), quer por instituições de formação que foram especificamente criadas para darem formação em exercício (por exemplo, [Alemanha](#)), quer ainda por outras instituições públicas, organizações não governamentais, organizações internacionais, quer ainda pelo sector privado. Em alguns casos, a formação em exercício está prevista através de planos de formação anuais, ou pode ser dada pontualmente. Na

---

<sup>4</sup> Para efeitos do presente documento, o termo “instituição de formação” deve ser entendido como qualquer entidade que dê formação.

<sup>5</sup> Conforme indicado pelo [Conselho Consultivo dos Juízes Europeus](#) do Conselho da Europa em 2003: “Existem grandes diferenças entre os países europeus no que diz respeito à formação inicial e em exercício dos juízes. Estas diferenças podem estar em parte relacionadas com características específicas dos diferentes sistemas judiciais, mas em alguns aspectos não parecem ser inevitáveis ou necessárias. Alguns países oferecem uma formação institucionalizada de longa duração num estabelecimento especializado, seguida de formação contínua intensiva. Outros prevêem um tipo de aprendizagem sob a supervisão de um juiz com experiência, que ministra conhecimentos e aconselhamento profissional com base em exemplos concretos, mostrando qual a abordagem a seguir e evitando qualquer tipo de didactismo. Os países de *common law* recorrem frequentemente a profissionais com uma longa experiência, normalmente na qualidade de advogados. Entre estas possibilidades, há toda uma série de países nos quais a formação está mais ou menos organizada e tem um carácter mais ou menos obrigatório”.

Parecer nº 4 do Conselho Consultivo dos Juízes Europeus (CCJE) à atenção do Comité de Ministros do Conselho da Europa sobre formação inicial e contínua adequada para juízes a nível nacional e europeu (CCJE (2003) Op. Nº 4, Novembro de 2003).

<sup>6</sup> Para mais informações, consultar o Anexo.

<sup>7</sup> Cabe aqui referir as especificidades dos sistemas de “common law”. No Reino Unido, por exemplo, os juízes são nomeados de entre profissionais experientes. Há também a possibilidade de os profissionais que não exercerem como juízes a tempo inteiro exercerem como juízes a tempo parcial pelo menos um mês por ano, após o que, na sua maioria, são nomeados como juízes a tempo inteiro. Além disso, inúmeros juízes não profissionais podem integrar os tribunais de primeira instância (“Tribunals” em matéria cível e « Magistrates Courts » sobretudo em matéria penal). Estão previstos programas de formação distintos antes de qualquer nomeação e ao longo do mandato.

maioria dos casos, a formação em exercício é facultativa, salvo nos casos em que os juízes ou procuradores desempenhem as suas funções em tribunais especializados (p. ex., Roménia).

Os programas de formação inicial e em exercício exigem, na maioria dos casos, um processo de avaliação e de aprovação formal, apesar de haver uma maior flexibilidade relativamente à formação em exercício facultativa. Por exemplo:

- Em França, os programas são definidos na sequência de consultas entre profissionais de direito e da justiça e os departamentos do Ministério da Justiça. O programa de formação é então apresentado ao Conselho de Administração da instituição para aprovação.
- Na Alemanha, a Conferência dos Programas da Academia alemã da Magistratura, que reúne representantes das diferentes administrações judiciais e das associações profissionais de juízes e procuradores, é responsável pela elaboração dos programas de formação em exercício da Academia.
- Na Polónia, até 30 de Abril de cada ano, são apresentadas propostas pelos departamentos do Ministério da Justiça, presidentes dos tribunais e serviços do Ministério Público. Com base nestas propostas, o Director da Escola Nacional apresenta o programa de actividades de formação para o ano seguinte ao Conselho dos Programas, para ser aprovado até 30 de Julho. Uma vez aprovado pelo Ministro da Justiça, o programa de formação é enviado aos respectivos departamentos do Ministério da Justiça, aos presidentes e aos procuradores gerais dos tribunais de apelação.
- Na Roménia, a estratégia para a formação inicial e em exercício é aprovada pelo Conselho Científico do Instituto Nacional da Magistratura e pelo Conselho Superior da Magistratura.
- Em Espanha, os currículos e programas de formação são elaborados por uma comissão pedagógica constituída por peritos em assuntos jurídicos, em consulta com associações de juízes ou com juízes individualmente. Por último, os programas de formação inicial e em exercício para juízes são aprovados pelo Conselho Geral da Magistratura.
- Em Portugal, é elaborado anualmente um programa de formação pelo Centro de Estudos Judiciários. Apesar de o programa de formação inicial estar previsto na lei, a formação em exercício muda todos os anos consoante as necessidades identificadas na prática. O programa de formação é definido após consultas com o Conselho Superior de Magistratura, o Tribunal Fiscal e Administrativo e o Ministério Público.
- Na Bélgica, são elaborados anualmente programas de formação mais específicos pelo Instituto de Formação Judiciária, ou sob supervisão do mesmo. Este instituto foi recentemente criado através de uma lei (31/01/07), tendo iniciado as suas actividades no início de 2009. A cibercriminalidade pode ser abordada no quadro da formação em exercício (que frequentemente é facultativa).
- Nos Países Baixos, o Conselho dos Juízes e o Conselho dos Procuradores-Gerais (que, em conjunto, dão instruções ao Centro de Formação Judiciária dos Países Baixos – o SSR) são as entidades que decidem se existe ou não verba para a formação proposta. Por exemplo, podem ser apresentadas propostas pelos procuradores ou juízes, ou por docentes do SSR, e se houver verba disponível e se esta for atribuída, a formação será então elaborada por peritos competentes do SSR, por representantes do Ministério Público, juízes e, se for caso disso, por entidades terceiras, incluindo do sector privado.
- Na Croácia, os programas de formação inicial e os planos relativos à formação em exercício são definidos em cooperação com o Conselho Consultivo e com o Conselho dos Programas da Escola da Magistratura. O Conselho dos Programas identifica as prioridades em matéria de formação e apresenta a proposta para o projecto de programa anual de formação profissional. O Conselho Consultivo adopta o documento e estabelece orientações para a definição da estratégia de formação profissional. Os membros de ambos os Conselhos são peritos jurídicos eminentes e representantes de todos os grupos visados pela Escola de Magistratura.

As instituições de formação podem recorrer a peritos externos, nomeadamente quando os temas abordados são de natureza específica e técnica, como sucede no caso da cibercriminalidade e das provas informáticas. Por exemplo:

- Na Alemanha, a Academia da Magistratura alemã recorre frequentemente a docentes externos que são, na sua maioria, juristas ou investigadores, mas por vezes também peritos do sector.
- Nos Países Baixos, consultores e peritos do sector participam na elaboração dos programas de formação, bem como na leccionação das formações propriamente ditas.
- Na Roménia, o Instituto Nacional da Magistratura recorre a formadores e docentes externos especializados em domínios como a cibercriminalidade (por exemplo, peritos do Conselho da Europa, do Ministério da Justiça dos EUA, do FBI, dos Serviços Secretos americanos e do sector privado (eBay, Visa, American Express, Amazon, PayPal, Microsoft), nomeadamente no quadro da formação de formadores.
- Em Espanha, o Conselho Geral da Magistratura concluiu acordos com empresas do sector privado (CYBEX, Logality) para dar formação em matéria de cibercriminalidade e criminalística. Além disso, peritos do sector privado participam na formação judiciária.
- Em Portugal, a maioria dos formadores do Centro de Estudos Judiciários é constituída por juízes ou procuradores. Para a formação em exercício (por exemplo, seminários ou formações de curta duração) podem ser solicitados formadores do sector privado e outros peritos.
- Na Croácia, peritos das unidades da polícia especializadas no combate à criminalidade organizada e económica participam na concepção e na ministração da formação.
- Na Bélgica, uma parte importante do orçamento afectada à formação de juízes e procuradores tem de ser organizada pelas universidades. Contudo, é possível fazer participar peritos do sector privado em alguns programas de formação.

As implicações para a formação de juízes e procuradores em matéria de cibercriminalidade/provas electrónicas são as seguintes:

- Os juízes e os procuradores começam a sua formação, em regra, com estudos superiores de direito. Pode assim supor-se que, quanto mais as questões relacionadas com a cibercriminalidade e as provas electrónicas forem regulamentadas pela legislação, mais estas questões serão reflectidas nos manuais e nos programas de estudos de direito. Contudo, poderá ser útil apresentar sugestões relativamente a esta matéria aos responsáveis pela concepção dos materiais para os cursos de nível universitário.
- Nos países onde a formação inicial é assegurada por instituições de formação judiciária, deverá ser possível integrar uma formação em matéria de cibercriminalidade e provas electrónicas nos programas.
- Quando a formação inicial decorre no local de trabalho, essa hipótese torna-se mais difícil.
- Na maior parte dos países, existem instituições de formação judiciária que oferecem formação em exercício, pelo que deve ser possível integrar nos programas as questões relacionadas com a cibercriminalidade e as provas electrónicas.
- Se é possível ministrar a formação em exercício caso a caso, é necessário um procedimento formal e uma aprovação oficial para integrar uma formação em matéria de cibercriminalidade/provas electrónicas nos programas oficiais, ou seja, para institucionalizar essa formação.
- A formação em exercício tem, normalmente, um carácter facultativo. O desafio está em convencer os juízes e os procuradores a submeterem-se a formação num domínio técnico, como o da cibercriminalidade e das provas electrónicas<sup>8</sup>.
- Os conhecimentos especializados externos dos sectores público e privado são necessários, podendo ser utilizados no quadro da elaboração de cursos de formação, da formação de formadores e da ministração desses cursos de formação.

---

<sup>8</sup> Em Portugal, a formação em exercício é obrigatória (isto é, cada juiz e procurador tem de participar, no mínimo, em dois estágios de formação por ano). Na Roménia, a formação em exercício pode ser obrigatória em alguns casos.

## 4 Competências e conhecimentos necessários para juízes e procuradores

É evidente que, a partir de agora, um número crescente dos casos levados a tribunal, quer de índole penal, quer cível, quer também de índole administrativa, estejam de alguma forma relacionados com as tecnologias da informação e da comunicação, e que a maioria dos juízes e procuradores penais se vejam confrontados, se não com a cibercriminalidade, pelo menos com a questão das provas electrónicas. Assim, não basta dar formação apenas a juízes e procuradores especializados.

Torna-se necessária uma difusão ampla dos conhecimentos em matéria de cibercriminalidade e provas electrónicas: todos ou o maior número possível de juízes e procuradores necessitam, deste modo, de obter pelo menos uma formação elementar no domínio da cibercriminalidade e das provas electrónicas. Esses conhecimentos elementares devem ser transmitidos através de formação inicial para futuros juízes e procuradores, e através da formação em exercício para juízes e procuradores em exercício activo de funções.

Ao mesmo tempo, trata-se de questões de cariz altamente técnico e em constante evolução, pelo que não se pode esperar que os juízes e procuradores em geral consigam acompanhar em permanência o desenvolvimento tecnológico. Assim, é necessário providenciar conhecimentos aprofundados a um número suficiente de juízes e procuradores que se especializem no domínio da cibercriminalidade e das provas electrónicas.

### 4.1 Conhecimentos elementares

Na maioria dos sistemas judiciais, não é possível prever qual o juiz que irá ter a seu cargo determinado processo (princípio do juiz natural). É por esse motivo que, todos os juízes, juízes de instrução e procuradores devem dispor de conhecimentos de nível elementar em matéria de cibercriminalidade e provas electrónicas. Através desses “conhecimentos elementares” devem ficar aptos a compreender o seguinte:

- Computadores e redes: como funcionam, noções elementares sobre o funcionamento da internet, papel dos fornecedores de serviços, dificuldades particulares que se colocam aos juízes e procuradores
- Cibercriminalidade: como são utilizadas as tecnologias da informação e da comunicação na prática de crimes
- Legislação em matéria de cibercriminalidade: legislação interna (incluindo jurisprudência) e normas internacionais
- Jurisdição e competências territoriais
- Provas electrónicas: procedimentos técnicos e aspectos jurídicos.

Terminada essa formação elementar, os juízes e procuradores deverão estar aptos a:

- Relacionar a conduta criminosa com as disposições correspondentes da legislação interna
- Aprovar técnicas de investigação
- Ordenar a busca e a apreensão de sistemas informáticos e a produção de provas electrónicas
- Agilizar a cooperação internacional
- Interrogar testemunhas e peritos
- Apresentar/validar provas electrónicas.

Apresenta-se de seguida um exemplo de um curso de formação elementar típico para juízes e procuradores:

**Exemplo: Formação em matéria de cibercriminalidade e provas electrónicas – módulo-tipo de formação elementar**

Objectivo da formação	No final da formação, os juizes e procuradores devem dispor de conhecimentos elementares sobre cibercriminalidade e provas electrónicas, a forma de as abordarem, o direito material e processual que pode ser aplicado e as tecnologias que podem ser utilizadas, e sobre como adoptar medidas urgentes e eficazes em matéria de cooperação internacional
1ª Sessão	Sobre a cibercriminalidade <ul style="list-style-type: none"> <li>➢ Porquê preocupar-se com a cibercriminalidade?</li> <li>➢ O que é cibercriminalidade?</li> <li>➢ Problemas que se colocam aos juizes e procuradores</li> <li>➢ Legislação nacional e normas internacionais</li> </ul>
2ª Sessão	Tecnologia <ul style="list-style-type: none"> <li>➢ Funcionamento da internet (noções elementares)</li> <li>➢ Glossário</li> <li>➢ Protocolos</li> </ul>
3ª Sessão	A cibercriminalidade enquanto infracção penal na legislação interna <ul style="list-style-type: none"> <li>➢ Infracções contra dados e sistemas informáticos</li> <li>➢ Fraude e falsificação informáticas</li> <li>➢ Infracções relacionadas com conteúdos (pornografia infantil, xenofobia, racismo)</li> <li>➢ Infracções relacionadas com a propriedade intelectual</li> <li>➢ Decisões judiciais/jurisprudência</li> </ul>
4ª Sessão	Provas electrónicas <ul style="list-style-type: none"> <li>➢ Sobre as provas electrónicas: definições e características</li> <li>➢ Condições a respeitar em matéria de provas electrónicas</li> <li>➢ Informática judiciária</li> </ul>
5ª Sessão	Direito processual/medidas de investigação <ul style="list-style-type: none"> <li>➢ Jurisdição e competências territoriais</li> <li>➢ Preservação expedita de dados informáticos</li> <li>➢ Injunções/ordens de produção de prova</li> <li>➢ Busca e apreensão de dados informáticos</li> <li>➢ Intercepção de dados relativos a tráfego e conteúdo</li> <li>➢ Salvaguardas</li> </ul>
6ª Sessão	Interacção com o sector privado
7ª Sessão	Cooperação internacional <ul style="list-style-type: none"> <li>➢ Convenção sobre a Cibercriminalidade enquanto quadro de cooperação internacional</li> <li>➢ Princípios gerais</li> <li>➢ Medidas provisórias e o papel dos pontos de contacto 24/7</li> <li>➢ Assistência jurídica mútua e o papel das autoridades competentes</li> </ul>
8ª Sessão	Avaliação e conclusão
Logística e materiais	A formação pode ser dada online ou numa sala de formação. Se for dada numa sala: <ul style="list-style-type: none"> <li>➢ É suficiente uma sala de formação equipada com um computador e um projector para as apresentações (uma vez que esta formação não inclui exercícios práticos, como a demonstração de software de criminalística ou técnicas de investigação, não é necessário um laboratório informático).</li> <li>➢ Extractos pertinentes do direito material e do direito processual nacional</li> <li>➢ Convenção de Budapeste sobre a Cibercriminalidade, incluindo o relatório explicativo</li> </ul>

- Manual com glossário e outras informações de natureza geral
- Se as aulas forem dadas numa língua estrangeira, deverá ser previsto um serviço de interpretação e os materiais deverão ser traduzidos.

## 4.2 Conhecimentos aprofundados

Por vezes, os conhecimentos elementares não são suficientes para instruir um processo judicial envolvendo cibercriminalidade. Para fazer face a este tipo de situações, seria necessário que um número considerável de juízes, juízes de instrução e procuradores dispusesse de conhecimentos aprofundados que lhes permitissem investigar/instaurar processos/julgar processos complexos relacionados com a cibercriminalidade e as provas electrónicas, ou dar apoio a outros procuradores e juízes.

Em alguns países, foram criadas unidades ou serviços especializados no seio do Ministério Público (por exemplo, na Roménia e na Sérvia); noutros países, os serviços do Ministério Público com maior dimensão dispõem de um determinado número de procuradores especializados. Nos Países Baixos, foi instituído o programa «intensiveringsprogramma» com o objectivo de assegurar, entre outras coisas, que existe pelo menos um procurador especializado em cibercriminalidade em cada um dos onze principais serviços. Em Itália, e ao abrigo da nova legislação sobre cibercriminalidade, 29 serviços do Ministério Público têm agora jurisdição nesta matéria. Em Portugal, o Ministério Público da Comarca de Lisboa tem uma secção especializada em cibercriminalidade, à qual são distribuídas as investigações nesta matéria.

Em alguns países, procuradores específicos podem supervisionar as actividades das unidades de polícia especializadas em crimes associados à alta tecnologia. Na maioria dos países, os serviços do Ministério Público estão hierarquicamente organizados de modo a que um procurador principal possa distribuir um processo a um procurador especializado. Assim, é possível identificar os procuradores que devem dispor de um conhecimento aprofundado sobre questões de cibercriminalidade.

No que diz respeito aos juízes, em alguns países, é possível que os processos de cibercriminalidade sejam confiados a um juiz especializado num tribunal que lide com tipos de infracções particulares, como a criminalidade organizada. Um exemplo (possivelmente o único na Europa) é a Sérvia, onde um serviço especial do tribunal distrital de Belgrado trata dos processos relacionados com a cibercriminalidade. Contudo, uma vez que a maioria dos sistemas judiciais assenta no princípio do juiz natural, é necessária uma abordagem diferente. Os Países Baixos têm um sistema que é provavelmente único na Europa: cinco centros com juízes especializados aos quais os outros juízes podem recorrer em caso de necessidade. Em Espanha, o Conselho Geral da Magistratura está a discutir uma proposta semelhante, ao abrigo da qual um grupo de juízes especializados em cibercriminalidade e provas electrónicas prestaria apoio e aconselharia os outros juízes. Na Bélgica, a lei não exige qualquer tipo de especialização, mas a maioria dos tribunais tem a possibilidade de solicitar a um ou mais dos seus membros que se especializem. Contudo, a atribuição desses processos a esses juízes especializados depende apenas da organização interna do tribunal. Por vezes, a lei dá competência a determinadas jurisdições (Bruxelas) do país para julgar determinados processos. Contudo, na maioria dos casos, a competência é determinada pelo local onde a infracção foi cometida e nem sempre existe um juiz ou um procurador especializado nesse local. Em muitos países, pode haver tribunais que lidem mais vezes com processos de cibercriminalidade do que outros, precisando assim de um grau de especialização superior ao dos outros tribunais.

Por “conhecimentos aprofundados” entende-se que os juízes e procuradores devem ter um entendimento prático e estar aptos a aplicar os seus conhecimentos nos seguintes domínios:

- Computadores e redes:
  - Glossário de termos relativos à informática e à cibercriminalidade
  - Funcionamento da internet
  - Protocolos e tecnologia
  - Papel dos fornecedores de serviços

- Cibercriminalidade:
  - Evolução da cibercriminalidade
  - Tipologias: Tipos e técnicas especiais de cibercriminalidade (p. ex., cibercisagem (phishing), redes zombies (botnets) e outros programas malévolos (malware), pornografia infantil)
  - Exemplos concretos e simulações
  
- Legislação em matéria de cibercriminalidade:
  - Legislação e jurisprudência internas
  - Cooperação internacional: acordos internacionais e bilaterais, canais de cooperação judiciária e meios concretos de cooperação expedita
  
- Investigação e provas electrónicas:
  - Jurisdição e competências territoriais
  - Disposições do direito processual e sua aplicação concreta
  - Busca, apreensão e preservação de provas electrónicas
  - Características dos softwares de criminalística
  - Identificação dos suspeitos
  - Seguimento do dinheiro sujo
  - Salvaguardas e condições
  - Apresentação das provas electrónicas em tribunal.

**Exemplo: Formação em matéria de cibercriminalidade e de provas electrónicas – módulo-tipo de formação avançada<sup>9</sup>**

Objectivo da formação	Terminada a formação, os juizes e procuradores devem dispor de conhecimentos aprofundados que podem ser aplicados na prática aos seguintes domínios: funcionamento dos sistemas informáticos e das redes, o que é a cibercriminalidade, legislação em matéria de cibercriminalidade, jurisdições competentes, meios de investigação e provas electrónicas, e cooperação internacional.
1ª Sessão	<p>Sistemas informáticos e redes</p> <ul style="list-style-type: none"> <li>➤ Glossário de termos relativos à informática e à cibercriminalidade</li> <li>➤ Funcionamento das TIC/infra-estrutura de internet                             <ul style="list-style-type: none"> <li>- Protocolos e tecnologia</li> <li>- Como comunicam os computadores entre si</li> <li>- Investigação de endereços IP e provas electrónicas – número e códigos de identificação dos computadores</li> <li>- Papel dos fornecedores de serviços</li> </ul> </li> <li>➤ Informação na internet                             <ul style="list-style-type: none"> <li>- Recolha de informação</li> <li>- Utilização de bases de dados (escondidas) da internet</li> </ul> </li> <li>➤ Perfis dos grupos sociais                             <ul style="list-style-type: none"> <li>- Formas de comunicar</li> <li>- Formas de preservação do anonimato</li> </ul> </li> <li>➤ Detecção/determinação da localização e da identidade dos computadores, das empresas e das pessoas na internet</li> </ul>
2ª Sessão	<p>Cibercriminalidade e riscos para a segurança</p> <ul style="list-style-type: none"> <li>➤ Evolução da cibercriminalidade</li> <li>➤ Tipologias: Tipos e técnicas especiais de cibercriminalidade (p. ex., cibercisagem (phishing), redes zombies (botnets) e outros programas malévolos (malware), pornografia infantil)</li> <li>➤ De que modo os criminosos utilizam as tecnologias da informação e da comunicação</li> </ul>

<sup>9</sup> Com base nas respostas ao questionário e no exemplo fornecido pelos Países Baixos.



	<ul style="list-style-type: none"> <li>➤ Autores das infracções</li> <li>➤ Impacto da cibercriminalidade</li> <li>➤ Como melhorar a segurança das TIC</li> <li>➤ Exemplos concretos e simulações</li> </ul>
3ª Sessão	<b>Legislação em matéria de cibercriminalidade: Direito penal material</b>
	<ul style="list-style-type: none"> <li>➤ Infracções contra dados e sistemas informáticos</li> <li>➤ Fraude e falsificação informáticas</li> <li>➤ Infracções relacionadas com conteúdos (pornografia infantil, infracções motivadas pelo ódio)</li> <li>➤ Infracções relacionadas com a propriedade intelectual</li> <li>➤ Decisões judiciais/jurisprudência</li> </ul>
4ª Sessão	<b>Investigação e provas electrónicas</b>
	<ul style="list-style-type: none"> <li>➤ Provas electrónicas <ul style="list-style-type: none"> <li>- Vestígios/impressões deixados(as) em computadores, na internet, na comunicação digital</li> <li>- Busca, apreensão e preservação de provas electrónicas</li> <li>- Características dos softwares de criminalística</li> <li>- Identificação dos suspeitos</li> <li>- Seguimento do dinheiro sujo</li> <li>- Salvaguardas e condições</li> <li>- Gestão/preparação dos processos</li> <li>- Apresentação de provas electrónicas em tribunal</li> </ul> </li> <li>➤ Organização do sistema repressivo relativamente à cibercriminalidade/provas electrónicas</li> <li>➤ Estudos de casos</li> </ul>
5ª Sessão	<b>Legislação em matéria de cibercriminalidade: direito processual</b>
	<ul style="list-style-type: none"> <li>➤ Preservação expedita de dados informáticos</li> <li>➤ Ordens de produção de prova</li> <li>➤ Busca e apreensão de dados informáticos</li> <li>➤ Intercepção de dados relativos a tráfego e conteúdo</li> <li>➤ Salvaguardas</li> <li>➤ Cooperação com fornecedores de serviços de internet/sector privado</li> <li>➤ Estudos de casos</li> </ul>
6ª Sessão	<b>Jurisdição e competências territoriais</b>
	<ul style="list-style-type: none"> <li>➤ Princípios gerais</li> <li>➤ Competência em matéria de cibercriminalidade - desafios</li> <li>➤ Disposições relativas à competência jurisdicional na Convenção sobre a Cibercriminalidade</li> <li>➤ Estudos de casos</li> </ul>
7ª Sessão	<b>Cooperação internacional</b>
	<ul style="list-style-type: none"> <li>➤ Convenção sobre a Cibercriminalidade enquanto quadro de cooperação internacional</li> <li>➤ Princípios gerais</li> <li>➤ Medidas provisórias, papel dos pontos de contacto 24/7 e cooperação policial</li> <li>➤ Assistência jurídica mútua e o papel das autoridades competentes</li> <li>➤ Estudos de casos</li> </ul>
8ª Sessão	<b>Avaliação e conclusões</b>
Logística e materiais	<p>A formação pode ser dada online ou numa sala de formação. Se for dada numa sala:</p> <ul style="list-style-type: none"> <li>➤ Sala de formação com um PC e projector para as apresentações</li> <li>➤ Seria desejável que os formandos dispusessem de um computador com acesso à internet (mas esta não é uma condição indispensável)</li> <li>➤ Extractos pertinentes do direito material e do direito processual nacional</li> </ul>

- Convenção de Budapeste sobre a Cibercriminalidade, incluindo o relatório explicativo
- Manual com glossário e outras informações de natureza geral
- Se as aulas forem dadas numa língua estrangeira, deverá ser previsto um serviço de interpretação e os materiais deverão ser traduzidos.

Os juizes e os procuradores não necessitam normalmente do tipo de competências e conhecimentos técnicos necessários aos investigadores nos domínios da cibercriminalidade e da criminalística. Contudo, poderá ser útil recordar os esforços desenvolvidos com vista a conseguir a elaboração de um programa de formação sistemática para os representantes das forças da ordem.

Com base num financiamento da Comissão Europeia (Programa Falcone 2002), um projecto liderado pela polícia (Garda Síochana) da Irlanda que contou com a participação de peritos de dez Estados-Membros da UE conduziu à elaboração de um programa de formação em matéria de cibercriminalidade ("Nível 1") destinado aos representantes das forças da ordem. Desde 2004, está disponível um curso de duas semanas que já foi seguido em inúmeros países europeus e não europeus. O curso recebeu acreditação do [University College Dublin](#) (UCD) em 2006.

No quadro de outros projectos levados a cabo pela polícia irlandesa em parceria com o UCD, foram elaborados módulos suplementares de nível intermédio e avançado, com o objectivo global de criar um programa de mestrado com a devida acreditação em informática judiciária e investigação da cibercriminalidade e destinado à globalidade dos representantes das forças da ordem. Os módulos de nível intermédio existentes incidem nos seguintes domínios:

- Investigações sobre a internet
- Investigações sobre redes
- Especialização técnico-jurídica nos sistemas de ficheiros NT
- Especialização técnico-jurídica nos sistemas LINUX
- Especialização técnico-jurídica em telemóveis
- Redes locais (LAN) sem fios e VOIP
- Linguagem de scripting – nível avançado
- Especialização técnico-jurídica em dados reais
- Especialização técnico-jurídica em Microsoft Vista

Estes módulos são constantemente actualizados, estando em preparação módulos adicionais<sup>10</sup>.

Em Julho de 2007, a Europol criou o Cybercrime Investigation Training Harmonisation Group (Grupo de harmonização das formações em matéria de investigação sobre a cibercriminalidade) que tem como objectivo principal a coordenação das iniciativas de formação em matéria de criminalidade tecnológica no âmbito da UE. Pretende-se deste modo criar um programa de formação certificado para os investigadores das forças da ordem na Europa e divulgá-lo para além da UE de modo a dar apoio a outros serviços policiais e judiciários interessados. De entre os parceiros do projecto incluem-se a Comissão Europeia, o OLAF, a Eurojust, a CEPOL, a Interpol, o Conselho da Europa, a ONU, o Centro de Investigação sobre a Cibercriminalidade do UCD, a Universidade de Troyes, Canterbury Christchurch University, a Universidade de Bolonha, bem como o sector das TIC.

### 4.3 Conhecimentos especializados

Alguns juizes e procuradores podem adquirir conhecimentos especializados através de estudos de pós-graduação, autoformação, ligação em rede ou através da experiência profissional. Esses conhecimentos não seriam leccionados no âmbito dos programas de formação ordinários. Os

<sup>10</sup> Refiram-se igualmente outros exemplos de programas de criminalidade tecnológica criados pela [UK National Policing Improvement Agency](#) (agência responsável pelo melhoramento dos serviços da polícia do Reino Unido).

juízes e procuradores com conhecimentos especializados desse tipo constituem um recurso inestimável para os seus colegas e para os formadores.

## **5 Formação actual em matéria de cibercriminalidade e provas electrónicas**

### **5.1 Formação inicial**

Por “formação inicial” entende-se a formação que os candidatos recebem, após terem concluído estudos superiores de direito, a fim de poderem exercer como juizes e/ou procuradores. Em inúmeros sistemas, a formação inicial é dada por instituições de formação judiciária ao longo de um período de um a três anos. Noutros sistemas, a formação inicial consiste numa formação prática no local de trabalho, mais ou menos formalizada e sem programa específico.

Na maioria dos países, a cibercriminalidade e as provas electrónicas não estão previstas na formação inicial, ou são abordadas apenas de forma muito limitada. Por exemplo:

- Em França, a formação em direito processual ministrada na Escola Nacional da Magistratura (ENM) compreende uma aula com a duração de três horas dada por um perito de informática sobre a investigação de provas electrónicas e sobre as tecnologias. Não são abordadas as questões relacionadas com a cibercriminalidade.
- Na Geórgia, a cibercriminalidade não é abordada no quadro da formação inicial dos procuradores, mas faz parte da dos juizes e do pessoal dos serviços judiciários sob a forma de uma conferência com a duração de meio dia.
- Na Alemanha, o estudo destas questões não é obrigatório no quadro da formação prática no local de trabalho.
- Na Croácia, na Polónia e na Roménia, estes tópicos não fazem parte da formação inicial.

Contudo, em alguns países, a cibercriminalidade e as provas electrónicas fazem parte da formação inicial. Por exemplo:

- Nos Países Baixos, a formação inicial contém um curso de nível elementar sobre a cibercriminalidade que é ministrado pelo Instituto de Formação de Procuradores e Juizes (SSR) em Utrecht ou Zutphen, que inclui um manual e outras informações de natureza geral. O curso é constituído por seminários interactivos e estudos de casos. Para além desta formação elementar de um dia e de uma formação aprofundada de quatro dias, é oferecida uma formação superior com a duração de dois dias.
- A Escola Judiciária espanhola ministra uma formação inicial em matéria de cibercriminalidade e de provas electrónicas aos juizes recentemente nomeados, abordando igualmente as questões de natureza processual e as questões de fundo. Inscreve-se no quadro da formação obrigatória em direito processual e de instrução. A cibercriminalidade e as provas electrónicas são abordadas no âmbito de seminários que decorrem durante quatro tardes e que abrangem os seguintes temas: direito interno, instrumentos de cooperação internacional, demonstração de software de criminalística e de técnicas de investigação, apreensão de provas electrónicas e estudos de casos. Além disso, uma vez por ano é organizado um seminário especial sobre provas electrónicas e outro seminário sobre direito material (crimes cometidos através de meios electrónicos). Estes seminários são ministrados por juristas e por peritos em tecnologias da informação. Além disso, os juizes têm acesso a uma biblioteca virtual sobre criminalidade electrónica. O objectivo desta formação inicial é fornecer conhecimentos elementares aos interessados.
- Na “antiga República Jugoslava da Macedónia”, a Escola de Formação de Juizes e Procuradores prevê uma formação inicial em matéria de cibercriminalidade e de provas electrónicas no quadro da formação em matéria de direito penal, TI e buscas. São assim consagradas dez horas à cibercriminalidade e às provas electrónicas.

- Em Portugal, a cibercriminalidade não constitui uma matéria específica e autónoma do currículo. Contudo, no quadro da formação em matéria de investigação penal, há um seminário específico consagrado à cibercriminalidade e às provas digitais (uma hora e meia). No quadro da formação em matéria de direito penal e de direito penal processual, são dedicadas 9 horas à criminalidade informática e aos procedimentos de obtenção de provas digitais, e 9 horas às TIC.

As formações são dadas por formadores permanentes, juizes, procuradores ou juristas com experiência na matéria, funcionários da polícia especializados, peritos de informática ou especialistas de empresas do sector privado.

As informações disponíveis levam-nos às seguintes conclusões:

- Uma vez que o objectivo é dotar todos os juizes e procuradores de um nível elementar de conhecimentos sobre cibercriminalidade e provas electrónicas, a oferta existente no domínio da formação é demasiadamente limitada.
- Com raras excepções, a formação inicial abrange apenas níveis elementares, não estando prevista nenhuma formação aprofundada.
- De modo geral, não estão disponíveis materiais de formação normalizados que permitam a replicação das formações.

## **5.2 Formação em exercício**

A formação em exercício, isto é, a formação profissional contínua de juizes e procuradores em exercício, é assegurada por instituições públicas de formação judiciária, podendo ser igualmente assegurada por diversas outras organizações. Por exemplo:

- Em França, a Escola Nacional de Magistratura organiza um seminário de nível avançado com a duração de cinco dias, oferecendo além disso estágios com a duração de dois dias no Serviço Central de Combate à Criminalidade Associada às TIC (OCLCTIC). O custo (cerca de 5 000 € por estágio) é suportado pela escola. Os formadores são juizes, procuradores, funcionários da polícia, peritos de informática ou peritos seleccionados do sector privado.
- Na Geórgia, a Escola Superior de Justiça é a única instituição responsável pela formação em exercício dos juizes. Levou a cabo uma formação elementar sobre cibercriminalidade com a duração de dois dias, financiada a partir do orçamento de Estado. Os formadores são membros do corpo docente e juizes do Supremo Tribunal e dos tribunais de apelação. Os procuradores recebem formação da unidade de formação do Ministério da Justiça, mas até à data não foram organizados cursos sobre cibercriminalidade e provas electrónicas.
- Na Alemanha, a formação em exercício para juizes e procuradores é dada pela Academia da Magistratura alemã, que organiza cerca de 150 eventos por ano. Em 2009, dois desses seminários incidiram na cibercriminalidade e tiveram uma duração de quatro dias cada. Os formadores são geralmente procuradores e juizes com experiência no domínio da cibercriminalidade, mas podem também pertencer à polícia, alfândegas, autoridades fiscais ou outros sectores. O custo é partilhado entre as autoridades federais e estatais. Estes cursos dão conhecimentos de nível elementar e avançado.
- Nos Países Baixos, apesar de a formação em exercício ser facultativa, os juizes têm obrigatoriamente de dedicar um determinado número de horas à formação. Cada juiz pode decidir qual(is) o(s) domínio(s) que pretende aprofundar. O Instituto de Formação dos Juizes e Procuradores (SSR), mas também várias outras instituições e organismos de formação ao nível de pós-graduação, oferecem formações em exercício no domínio da cibercriminalidade e das provas electrónicas de nível elementar e avançado. O SSR oferece anualmente três formações de nível elementar, três formações de nível aprofundado e uma formação de nível

superior. Os formadores são magistrados do Ministério Público especializados na cibercriminalidade e peritos de empresas privadas e do sector. Contudo, o SSR também oferece uma vasta gama de outros cursos de formação que incidem em domínios quer jurídicos, quer de natureza prática (num total de aproximadamente 400 formações). Assim, a formação em matéria de cibercriminalidade tem de competir com todos os outros temas propostos.

- Na Polónia, a Escola Nacional dos Juizes e dos Procuradores propõe formações de nível elementar e de nível avançado sob a forma de conferências com uma duração de quatro a cinco dias. Em 2009, foram organizados dois eventos desse tipo, a saber, "Metodologia das infracções cometidas com o auxílio dos sistemas informáticos" e "Provas electrónicas nos procedimentos judiciais".
- Na Roménia, o Instituto Nacional da Magistratura oferece formações em serviço, mas apenas de nível elementar. Por exemplo, de 2006 a 2009, foram organizados anualmente dois seminários de dois dias, cada um para aproximadamente 25 juizes ou procuradores, na sua maioria a partir do orçamento do INM, alguns com financiamento da Comissão Europeia (PHARE), e alguns, em 2006, com o apoio da eBay. Os formadores são magistrados romenos, especialistas de TI, bem como peritos estrangeiros financiados por organizações como o Conselho da Europa. Além disso, a cibercriminalidade é uma disciplina obrigatória nas formações descentralizadas dadas ao nível dos serviços do Ministério Público afectos aos tribunais de apelação. Esta formação é igualmente coordenada pelo INM.
- Em Espanha, a Escola Judiciária sob a direcção do Conselho Geral da Magistratura assegura a formação em exercício para juizes em matéria de cibercriminalidade e provas electrónicas. Para os procuradores, essa formação é assegurada pelo Centro de Estudos Jurídicos, sob direcção do Ministério da Justiça. Em ambos os casos, a formação é organizada em cooperação com a CYBEX, uma empresa privada especializada neste domínio. A Escola Judiciária dispõe de um orçamento de cerca de 42 000 € para a formação em matéria de cibercriminalidade. É igualmente possível obter financiamento e apoio por parte do sector privado. A formação em exercício é de nível elementar, e as formações têm uma duração de três a quatro dias e incluem palestras e análises de casos práticos. Os materiais são publicados e colocados normalmente à disposição de cada juiz. Em 2008 e 2009, foram realizados anualmente dois seminários desse tipo. Apesar de algumas matérias serem abordadas com algum grau de profundidade, não existe uma formação sistemática de nível avançado.
- Em Portugal, a formação em exercício em matéria de cibercriminalidade é dada pelo Centro de Estudos Judiciários, que organiza cerca de 30 seminários por ano. Dois desses seminários são normalmente dedicados a questões elementares no domínio da cibercriminalidade. Por vezes, são também organizados outros seminários sobre temas afins, como direitos de autor online ou as tecnologias e os tribunais. Os formadores são juizes, procuradores, juristas, funcionários da polícia e peritos dos sectores público e privado. Os seminários têm um bom acolhimento e atraem um elevado número de participantes (na sua maioria procuradores, mas também juristas e juizes penais).
- Na Bélgica, o programa de formação em exercício está ainda em fase de elaboração uma vez que o Instituto de Formação Judiciária só foi criado recentemente. O objectivo é, obviamente, a organização dessa formação tomando em consideração os resultados e as recomendações de vários grupos de reflexão e, nomeadamente, as observações do Conselho da Europa. A participação de magistrados belgas na formação no estrangeiro pode ser financiada pelo Instituto a pedido do magistrado (p. ex., um juiz e um procurador seguiram o seminário de formação ECCE (Certificado europeu sobre a luta contra a cibercriminalidade e a utilização de provas electrónicas) organizado em Paris em Fevereiro de 2009).

- Na Croácia, não existe actualmente qualquer formação em exercício no domínio da cibercriminalidade e/ou das provas electrónicas. Estas questões só foram abordadas no quadro do programa CARDS no qual a Croácia participou.
- Na “antiga República Jugoslava da Macedónia”, não existe organizada nenhuma formação em exercício.
- Formações oferecidas pela Academia de Direito Europeu (ERA). A ERA, criada oficialmente por iniciativa do Parlamento Europeu em 1992, visa providenciar uma análise e um conhecimento aprofundados do direito europeu e comunitário, através da organização de seminários e cursos de índole prática destinados a profissionais de direito. A Academia é igualmente um fórum de troca de experiências e opiniões sobre as políticas e o direito europeus. A ERA organiza regularmente acontecimentos abertos ao público sobre o tema da cibercriminalidade que atraem participantes oriundos de toda a UE. Para o período 2009 e 2010, a ERA também vai colaborar com a TAIEX na implementação de uma série de seminários na Roménia, Bulgária, países candidatos e potenciais países candidatos tendo em vista a apresentação dos principais instrumentos europeus e internacionais de combate à cibercriminalidade. Todos os seminários visam servir de plataforma para o debate e avaliação do modo como a legislação europeia no domínio da cibercriminalidade é aplicada nos diferentes Estados-Membros e países candidatos, bem como da possibilidade de uma campanha europeia contra a utilização ilícita da internet. São discutidos os instrumentos e textos jurídicos europeus mais recentes, como a Convenção do Conselho da Europa sobre a Cibercriminalidade (2001), a Decisão-Quadro 2005/222/JAI do Conselho, relativa a ataques contra os sistemas de informação, e a Decisão-Quadro 2004/68/JAI do Conselho, relativa à luta contra a exploração sexual de crianças e a pornografia infantil. A questão da cooperação com os fornecedores de serviços e as empresas ligadas à internet, como a Google, a Microsoft e a Yahoo é igualmente discutida. Cada seminário utiliza uma variedade de métodos de formação, que vão desde cursos de introdução, cursos mais aprofundados, estudos de casos e outros tipos de aprendizagem interactiva. É dedicada atenção especial à discussão em pequenos grupos de trabalho. As palestras e as sessões dos ateliês são apresentadas por peritos da UE e por peritos nacionais.
- Numa série de países, as sessões de formação são apoiadas pelo sector. Por exemplo:

Na Alemanha, a eBay apoiou a formação “Os novos meios de comunicação e o direito penal» organizada pela Academia da Magistratura alemã destinada a juízes e procuradores, enviando um orador para apresentar o site comercial eBay, as actividades delituosas que o mesmo suscita, as contra-medidas instituídas e a forma como a eBay colabora com as forças da ordem. A eBay também participou em várias formações pontuais organizadas pelo Ministério da Justiça de Berlim, tendo cada sessão contado com a participação de cerca de 100 procuradores.

Na Roménia, a eBay dinamizou inúmeras formações para juízes, procuradores e representantes das forças da ordem. A eBay colaborou nomeadamente com os Serviços Secretos dos Estados Unidos e com a Embaixada americana com vista à formação de 25 procuradores de diferentes serviços da DIICOT (Direcção de Investigação da Criminalidade Organizada e do Terrorismo), 15 juízes e 20 funcionários da polícia em Silbiu. Além disso, a eBay participou em sessões de formação complementar para juízes em Targu Jiu e 60 juízes de diferentes jurisdições do tribunal de apelação de Craiova.

Conforme acima referido, em quase todos os casos, quaisquer alterações ou aditamentos aos programas de formação judiciária institucional necessitam de ser aprovados e validados pelas instâncias oficiais<sup>11</sup>.

Apesar de ser evidente que existem inúmeras iniciativas que visam dar resposta à necessidade de disponibilizar formação adequada em matéria de cibercriminalidade a juízes e procuradores, existe uma falta evidente de coerência entre as abordagens acima descritas.

Apesar de ser necessário tomar em consideração as especificidades das legislações nacionais e a grande diversidade de sistemas de ensino, a cibercriminalidade é, por natureza, um problema internacional que exige um mínimo de coordenação e coerência entre os países. Um entendimento idêntico dos vários países relativamente ao que é a cibercriminalidade irá, certamente, melhorar a coerência das decisões judiciais e impedir a criação de zonas onde os criminosos estejam em segurança, para além de dotar as instituições de formação de conteúdos de formação de qualidade a preços reduzidos.

A informação disponível sugere o seguinte:

- A maioria das formações em exercício oferecidas é de nível elementar.
- O número de formações disponibilizadas é muito limitado e apenas beneficia um número reduzido de juízes e procuradores.
- Na maioria dos casos, as formações elementares não parecem ser normalizadas. Por esse motivo, não são replicáveis e não permitem a um juiz ou procurador uma progressão sistemática dos níveis elementares para os níveis avançados. Os Países Baixos parecem constituir a excepção.
- Os materiais de formação parecem ser dispersos e elaborados caso a caso.
- Se considerarmos que todos os juízes e procuradores acabarão eventualmente por necessitar de dispor de conhecimentos de nível elementar sobre cibercriminalidade e provas electrónicas, a formação proposta é, em larga medida, insuficiente, designadamente quando se considera que a actual geração de juízes e procuradores em actividade não terá, muito provavelmente, recebido qualquer formação inicial nem abordou estas questões durante os seus estudos universitários.
- Salvo raras excepções, não existe formação de nível avançado para juízes e procuradores.
- Dado o cariz internacional da cibercriminalidade, seria necessário um nível mínimo de coordenação e coerência entre os países.

---

<sup>11</sup> Neste contexto, o projecto relativo ao [Certificado europeu sobre a cibercriminalidade e as provas electrónicas](#) posto em prática pela CYBEX e financiado pela Comissão Europeia (JPEN) é interessante. Prevê uma formação elementar normalizada de quatro dias destinada a juízes, procuradores e juristas. Entre o início de 2009 e o fim de 2010, a formação vai ser testada em catorze países piloto na Europa e na América Latina. Os participantes receberão um certificado que atesta a aquisição de conhecimentos teóricos, práticos, jurídicos e técnicos de nível elementar em matéria de provas electrónicas e cibercriminalidade.

O Conselho da Europa – no quadro do Projecto sobre a Cibercriminalidade – iniciou igualmente a elaboração de um manual de formação para juízes e procuradores que será utilizado no quadro de uma formação de nível elementar com a duração de dois dias incidindo na legislação relativa à cibercriminalidade.



## **6 Abordagem proposta**

### **6.1 Objectivo**

Conforme indicado na secção anterior, em geral, as formações iniciais e em exercício existentes não conferem aos juízes o nível de conhecimentos necessário para abordar a questão da cibercriminalidade e das provas electrónicas.

Assim, os objectivos de um conceito de formação para juízes e procuradores devem ser:

- Permitir às instituições de formação a prestação de formação inicial e em exercício em matéria de cibercriminalidade com base nas normas internacionais
- Dotar o maior número possível de juízes e procuradores futuros e em exercício de conhecimentos elementares em matéria de cibercriminalidade e de provas electrónicas
- Providenciar formação avançada a um número conseqüente de juízes e procuradores;
- Apoiar a especialização e a formação técnica contínuas de juízes e procuradores
- Contribuir para um enriquecimento dos conhecimentos através do trabalho em rede entre juízes e procuradores
- Facilitar o acesso a diferentes redes e iniciativas de formação.

As medidas a seguir enunciadas devem contribuir para a realização destes objectivos.

### **6.2 Institucionalização da formação inicial**

- Nos países onde a formação inicial consiste numa formação prática no local de trabalho (um tipo de aprendizagem ou série de estágios) sem programa oficial, recomenda-se que, pelo menos, parte dessa formação (por exemplo, um estágio ou uma actividade idêntica) seja consagrada à cibercriminalidade e às provas electrónicas.
- Nos países onde a formação inicial é assegurada por instituições de formação judiciária:
  - os programas deveriam conter pelo menos um módulo de nível elementar sobre cibercriminalidade e provas electrónicas
  - além disso, estas questões devem ser abrangidas no quadro dos módulos obrigatórios sobre direito material e direito processual
  - devem ser disponibilizados módulos facultativos de nível avançado que incidam na cibercriminalidade e nas provas electrónicas.

Os módulos de formação específicos devem ser normalizados de forma a serem replicáveis e a permitirem aos candidatos uma progressão entre o nível elementar e o nível avançado. Por "replicáveis" entende-se que os módulos devem ser passíveis de ser repetidos pelo menos no mesmo país para diferentes pessoas, para que os participantes em diferentes eventos de formação tenham um nível de conhecimentos idêntico. Isto supõe igualmente que os métodos de formação sejam normalizados. Para assegurar à formação uma qualidade elevada constante, deve ser feita uma avaliação no fim de cada curso.

### **6.3 Institucionalização da formação em exercício**

- As instituições de formação em exercício devem disponibilizar pelo menos um módulo de nível elementar em matéria de cibercriminalidade e provas electrónicas de modo a dotar os juízes e os procuradores em exercício de conhecimentos elementares que não tenham podido adquirir na sua formação inicial.
- Além disso, devem oferecer formação de nível avançado.

- Também aqui: os módulos de formação específicos devem ser normalizados de modo a serem replicáveis e a permitirem aos candidatos uma progressão entre o nível elementar e o nível avançado. Por conseguinte, poderá ser necessário proceder, na medida do possível, a uma harmonização entre os módulos de formação em exercício e os módulos de formação inicial. Os métodos de ministração da formação também devem ser harmonizados, desde os controlos de qualidade às avaliações no final da formação.
- Para dar formação a juizes e procuradores especializados, deve ser incentivada a realização de estágios em unidades especializadas em crimes associados à alta tecnologia ou formações/estudos de nível pós-graduação<sup>12</sup>.

#### **6.4 Formações e módulos normalizados e replicáveis**

- Devem ser criados módulos e formações normalizados que possam ser replicados em grande escala de forma rentável, e que permitam quer aos candidatos a juiz e procurador, quer aos juizes e procuradores em exercício uma progressão do nível elementar para o nível avançado.
- As formações de nível elementar existentes<sup>13</sup> que podem ser integradas nos programas de formação inicial ou em exercício devem ser avaliadas. Posteriormente, poderia ser recomendada uma formação normalizada às instituições de formação inicial e em exercício.
- Uma avaliação semelhante deve ser efectuada para as formações de nível avançado, e uma formação normalizada de nível avançado poderia subseqüentemente ser recomendada.
- Por último, os formadores devem receber formação sobre a forma de ministrar esses cursos na língua local de modo a limitar o recurso a formadores internacionais<sup>14</sup>.

#### **6.5 Acesso aos materiais de formação/autoformação**

- Devem ser criados materiais de formação que reflectam as normas internacionais e as boas práticas internacionais comuns. Devem ser disponibilizados às instituições de formação de forma rentável tendo em vista a sua utilização ao nível local. Obviamente que se, para as forças da ordem, é possível uma formação que incida nas tecnologias e na criminalística com um elevado nível de normalização, tal afigura-se menos fácil no que diz respeito à formação de juizes e procuradores que necessitam de receber formação sobretudo em matéria de aplicação da legislação interna. Contudo, é possível criar materiais de formação normalizados que possibilitem a integração dos sistemas e legislação internas.
- Em alguns países, são disponibilizados online materiais para juizes e procuradores<sup>15</sup>. Esta prática deve ser seguida por outros países.
- Devem ser criados e disponibilizados cursos online.<sup>16</sup>

---

<sup>12</sup> A título de exemplo, a formação de nível elementar de duas semanas criada pela polícia irlandesa e pelo University College Dublin poderia igualmente ser de interesse para os juizes e os procuradores.

<sup>13</sup> Por exemplo, a formação ECCE criada e actualmente em fase de experimentação pela CYBEX.

<sup>14</sup> Um programa de "formação de formadores" que foi elaborado pelo UCD e pela Interpol pode ser disponibilizado. Incide nas técnicas de formação, na elaboração das formações, etc. NÃO é um curso reservado às forças da ordem e pode ser ministrado a qualquer pessoa.

<sup>15</sup> É o caso dos Países Baixos e da biblioteca de provas electrónicas da CYBEX. No quadro do projecto 2CENTRE, o UCD prevê criar um serviço de recursos online para disponibilização de alguns materiais de formação AGIS/ISEC.

<sup>16</sup> Por exemplo, o UCD oferece neste momento dois programas de mestrado em ciências, uma parte dos quais é ministrada inteiramente online. O Centro de Estudos Judiciários de Portugal tenciona organizar um curso online sobre "Os tribunais e as tecnologias da informação e da comunicação", que inclui módulos sobre a

- O acesso às formações (nacionais e internacionais) deve ser facilitado, na medida do possível, através de uma simplificação dos procedimentos de aprovação.

## 6.6 Centros piloto de formação básica e avançada

- Devem ser criados vários centros piloto de formação de nível elementar e avançado para juízes e procuradores em matéria de cibercriminalidade e provas electrónicas. Esses centros poderão:
  - Testar e melhorar as formações e os materiais normalizados
  - Difundir as boas práticas
  - Levar a cabo investigação sobre a formação
  - Manter um registo dos formadores
  - Fazer formação de formadores
  - Propor formação a outros países com sistemas e línguas semelhantes.
- Seria desejável que os centros piloto coordenassem o seu trabalho entre si com o apoio do Conselho da Europa.
- Os juízes e os procuradores que pretendam especializar-se devem considerar a participação nas formações propostas pelos centros de excelência e destinadas às forças da ordem e ao sector privado<sup>17</sup>.

## 6.7 Enriquecimento dos conhecimentos através do trabalho em rede

Apesar de a formação inicial e em exercício permitir aos juízes e aos procuradores a aquisição de conhecimentos de base, a cooperação entre pares, o trabalho em rede entre juízes e procuradores, mas também com diversas partes interessadas serão extremamente importantes.

Assim sendo:

- Os juízes e os procuradores devem utilizar as redes de juízes<sup>18</sup> e de procuradores existentes (como a GPEN)<sup>19</sup>.

---

cibercriminalidade e as provas electrónicas. A formação será em português e está prevista a possibilidade de alargar a formação a outros países de língua portuguesa (p. ex., Brasil, Cabo Verde, Angola, Moçambique, Guiné-Bissau, São Tomé ou Timor).

<sup>17</sup> A iniciativa 2Centre ([Cybercrime Centres of Excellence Network for Training Research and Education](#)) (Rede de centros de excelência para a formação e a investigação em matéria de cibercriminalidade) foi lançada em Março de 2009, no decurso da Conferência Octopus do Conselho da Europa. O projecto 2Centre “analisa os métodos actuais de formação das forças da ordem e do sector no domínio da informática judiciária e das investigações sobre a cibercriminalidade. Analisa as actividades levadas a cabo por elementos das forças da ordem e pelo pessoal das empresas interessadas do sector com o objectivo de obterem conhecimentos e competências num domínio onde coexistem actualmente vários níveis de formação profissional, formação interna, formação polivalente e de formação no local de trabalho”. O University College Dublin é o primeiro centro de excelência, e a Universidade de Troyes tornar-se-á no segundo em 2010.

<sup>18</sup> Não parece existir ainda qualquer rede internacional para juízes vocacionada para os temas relacionados com a cibercriminalidade e as provas electrónicas. Um exemplo de uma iniciativa nacional é aquela que foi posta em funcionamento nos Países Baixos onde foi criado um recurso intranet do tipo wiki.

<sup>19</sup> A GPEN (Global Prosecutor’s E-Crime Network (Rede internacional de procuradores especializados no crime electrónico) foi criada em 2008 sob a égide da Associação Internacional dos Procuradores Penais (IAP). Tem por objectivo facilitar as trocas de informação e a cooperação entre os procuradores em processos relacionados com a criminalidade electrónica e a cibercriminalidade apoiando-se na Convenção sobre a Cibercriminalidade, criar e ministrar programas de formação, e disponibilizar recursos online aos procuradores. A GPEN é uma rede

- A possibilidade da criação de uma rede internacional de juízes especializados em cibercriminalidade e criminalidade electrónica (semelhante à GPEN) deve ser discutida pelo Conselho da Europa.
- A ligação em rede entre as instituições europeias que disponibilizam formação em matéria de cibercriminalidade e provas electrónicas deve ser apoiada pelo Conselho da Europa e pela Rede Europeia de Formação Judiciária.
- Com vista a facilitar o acesso por parte de juízes e procuradores a estas e às inúmeras redes relacionadas com a cibercriminalidade, o Conselho da Europa – no seu sítio web [www.coe.int/cybercrime](http://www.coe.int/cybercrime) – deve criar um portal que apresente os links, informações resumidas e os dados de contacto relativamente às diferentes redes. Isto deverá também facilitar a coordenação entre redes. Deve além disso facilitar o acesso aos materiais e iniciativas de formação existentes.

## 6.8 Cooperação público-privado

Com o objectivo de facilitar as investigações em matéria de cibercriminalidade e de recolher provas electrónicas, é absolutamente indispensável<sup>20</sup> uma cooperação estruturada e regulamentada entre as forças da ordem e o sector privado (sector das TIC, nomeadamente fornecedores de serviços de internet), sendo que o sector privado contribui com conhecimentos especializados e outros apoios às iniciativas de formação para as forças da ordem.

O apoio do sector privado à formação de juízes e procuradores seria benéfico, uma vez que o sector privado dispõe de conhecimentos altamente especializados sobre esta matéria. Ao mesmo tempo, os juízes e procuradores têm de manter a sua independência e imparcialidade.

Assim sendo:

- As instituições de formação judiciária podem utilizar os conhecimentos especializados do sector privado no quadro da concepção de programas de formação, da elaboração dos materiais de formação e da ministração das formações propriamente ditas.
- O apoio do sector às instituições de formação não pode ser visto como um meio potencial de assegurar decisões favoráveis dos tribunais ou de gerar negócios, mas sim de garantir que seja dada informação adequada aos juízes e procuradores que lhes permita tomar decisões informadas.
- O sector privado poderá apoiar com toda a transparência as organizações internacionais ou nacionais, as universidades, as iniciativas de formação ou outras entidades terceiras que, por sua vez, poderão dar apoio a instituições de formação independentes.
- Se os juízes e procuradores devem adquirir uma visão global sobre a internet e a cibercriminalidade, também é importante disponibilizar-lhes informações específicas relativamente a plataformas informáticas. O sector poderá fornecer materiais para módulos específicos (em vez de cursos completos) sobre o funcionamento das plataformas principais.

---

de procuradores especializados na criminalidade electrónica e cada organização membro da IAP foi convidada a designar pelo menos um procurador como ponto de contacto nacional da GPEN. A rede é gerida pelo Conselho de Desenvolvimento da GPEN que é constituído por membros da IAP.

<sup>20</sup> Ver, por exemplo, as orientações relativamente à cooperação entre as forças da ordem e os fornecedores de serviços de internet Guidelines for law enforcement – ISP cooperation adoptadas pela Conferência Octopus do Conselho da Europa em Abril de 2008.



## **7 Apoio à implementação deste conceito**

A implementação deste conceito compete, antes de mais, às instituições de formação judiciária, mas deve ser apoiada pelas instituições e parceiros do sector público e privado, nomeadamente as organizações internacionais. Tendo em conta a importância que as tecnologias da informação e da comunicação têm para a sociedade, o financiamento dessas medidas de formação representa um investimento inestimável, e devem ser envidados todos os esforços no sentido de providenciar recursos suficientes para as instituições de formação.

O Conselho da Europa e a Rede Europeia de Formação Judiciária (REFJ), bem como outros organismos, devem promover a execução do conceito em toda a Europa e no resto do mundo.

Além disso, a REFJ e o Conselho da Europa poderiam organizar uma conferência conjunta sobre este conceito no futuro próximo.

Por último, seria útil que o Conselho da Europa e a REFJ pudessem avaliar regularmente os progressos conseguidos.

Na prática, a implementação deste conceito também deveria ser apoiada por doadores. As organizações e os dados interessados poderiam participar no desenvolvimento conjunto de projectos de apoio às instituições de formação e às outras partes interessadas que estejam dispostas a assumir a responsabilidade pelas medidas propostas neste conceito.

No intuito de reduzir o risco de conflitos de interesse ou de comprometer a imparcialidade dos juízes e procuradores, os dados – em vez de oferecerem apoio directo – poderiam disponibilizar recursos a entidades terceiras neutras – como organizações internacionais que, por sua vez, cooperariam com as instituições de formação.

## 8 Anexo

### 8.1 Rede de Lisboa: Ligações com as instituições de formação judiciária

Quarenta e quatro dos quarenta e sete países membros do Conselho da Europa estão representados no seio da Rede de Lisboa. Os membros da Rede de Lisboa são instituições nacionais competentes, responsáveis pela formação inicial e contínua dos juízes e procuradores. Consoante o caso, poderão ser Escolas de Magistratura, Centros de Formação Judiciária ou serviços de formação de magistrados integrados nos Ministérios da Justiça.

Para consultar a informação disponível relativamente a cada um dos países membros da Rede (incluindo, em determinados casos, os programas de formação associados), ver:

- |                                    |                               |                                                           |
|------------------------------------|-------------------------------|-----------------------------------------------------------|
| <a href="#">Albânia</a>            | <a href="#">Alemanha</a>      | <a href="#">Portugal</a>                                  |
| <a href="#">Andorra</a>            | <a href="#">Grécia</a>        | <a href="#">Roménia</a>                                   |
| <a href="#">Arménia</a>            | <a href="#">Hungria</a>       | <a href="#">Federação Russa</a>                           |
| <a href="#">Áustria</a>            | <a href="#">Islândia</a>      | <a href="#">Sérvia</a>                                    |
| <a href="#">Azerbaijão</a>         | <a href="#">Irlanda</a>       | <a href="#">Eslováquia</a>                                |
| <a href="#">Bélgica</a>            | <a href="#">Itália</a>        | <a href="#">Eslovénia</a>                                 |
| <a href="#">Bósnia Herzegovina</a> | <a href="#">Letónia</a>       | <a href="#">Espanha</a>                                   |
| <a href="#">Bulgária</a>           | <a href="#">Lituânia</a>      | <a href="#">Suécia</a>                                    |
| <a href="#">Croácia</a>            | <a href="#">Luxemburgo</a>    | <a href="#">Suíça</a>                                     |
| <a href="#">Chipre</a>             | <a href="#">Malta</a>         | <a href="#">"antiga República Jugoslava da Macedónia"</a> |
| <a href="#">República Checa</a>    | <a href="#">Moldávia</a>      | <a href="#">Turquia</a>                                   |
| <a href="#">Dinamarca</a>          | <a href="#">Montenegro</a>    | <a href="#">Ucrânia</a>                                   |
| <a href="#">Estónia</a>            | <a href="#">Países Baixos</a> | Reino Unido                                               |
| <a href="#">Finlândia</a>          | <a href="#">Noruega</a>       | - <a href="#">Inglaterra e País de Gales</a>              |
| <a href="#">França</a>             | <a href="#">Polónia</a>       | - <a href="#">Escócia</a>                                 |
| <a href="#">Geórgia</a>            |                               |                                                           |

#### Observador

- [UNMIK](#)

## 8.2 Exemplos de formações de nível elementar: estrutura e temas abordados

### 8.2.1 Exemplo da formação dada nos Países Baixos

#### **Formação de nível elementar – 1 dia**

Programa:

- 1 Aspectos gerais:
  - O que é a cibercriminalidade?
  - Manifestações da cibercriminalidade
  - Quadro jurídico que rege a repressão das infracções e os processos penais
- 2 Repressão das infracções:
  - Aplicação do direito digital enquanto prática quotidiana
  - Métodos de repressão das infracções
- 3 Repressão das infracções (2ª parte):
  - A internet e a repressão das infracções no quadro da lei sobre os privilégios especiais em matéria de repressão das infracções

Conclusões + avaliação

### 8.2.2 Exemplo da formação dada na Alemanha (Academia da Magistratura alemã)

#### **Formação inicial: “Diferentes manifestações e estratégia de combate contra a cibercriminalidade” – 4 dias**

Programa:

##### **1º dia:**

- Código Penal alemão
- Utilização do Código Penal alemão no contexto da criminalidade informática e da cibercriminalidade
- Problemas encontrados na prática quotidiana dos serviços do Ministério Público e dos tribunais

O orador é juiz do Tribunal de Munique e especializado em criminalidade financeira e económica. Trabalhou há alguns anos atrás como procurador em processos envolvendo a cibercriminalidade, espionagem de dados, falsificação de datas, etc.

- Problemas constatados na prática quotidiana dos serviços do Ministério Público e dos tribunais dos Países Baixos
- Evolução da cibercriminalidade e combate contra este fenómeno na Europa
- Problemas constatados com fornecedores nos Países Baixos e noutros países europeus
- Convenção sobre a Cibercriminalidade do Conselho da Europa
- Importância e interesse da Convenção sobre a Cibercriminalidade para a Europa e para o resto do mundo (China, EUA, Rússia)

O orador é o Prof. Henrik Kaspersen, Países Baixos.

##### **2º Dia:**

- Sabotagem de sistemas informáticos
- Piratagem na internet (hacking)
- Riscos associados às compras feitas através da internet
- Espionagem de dados
- Fraude informática com cartões de crédito
- Ataques contra dados bancários
- Cibercriminalidade (phishing) e novos tipos de infracções na internet
- Redes zombies (botnets)
- Fraude através do eBay ou de outros sites de venda

O orador é funcionário da polícia na Sede da Polícia alemã (BKA, Wiesbaden).



- Pesquisa preventiva na internet como forma de combater a criminalidade organizada, o terrorismo, as infracções graves, o branqueamento de capitais, etc.
- Pesquisa na internet de avisos de pessoas atingidas de fúria assassina (escolas, etc.)
- Pesquisa na internet sobre pornografia infantil
- Cooperação internacional em matéria de pesquisa na internet
- Pesquisa online (problemas constitucionais)

O orador é chefe de um serviço especial da Sede da Polícia da Baviera (LKA, Munique).

**3º dia:**

- Salvaguarda e avaliação de dados na Alemanha ou noutros países
- Pesquisa de dados na internet e rastreabilidade dos dados na internet
- Possibilidades criadas através da informática judiciária e os limites de análise dos dados
- Sistemas de anonimização de dados na internet
- Utilização de criptogramas por parte dos criminosos

O orador é um perito da Sede da Polícia de Munique.

- Os novos problemas jurídicos suscitados pela salvaguarda e avaliação dos dados da internet
- Competência para o conjunto das medidas jurídicas que as buscas envolvem
- Competência em matéria de recolha de provas para as investigações e os tribunais
- Evoluções recentes em matéria de repressão das infracções

O orador é juiz no Tribunal Penal Superior de Bamberg, na Baviera.

**4º dia:**

- Rede de negócios russa
- Intercage
- Protecção contra a sabotagem de computadores ou dados
- "Piratagem" positiva
- Viciação e falsificação de máquinas de voto
- Influência política nas novas leis
- A população sentada numa casa de vidro

O orador é membro do famoso Chaos Computer Club (CCC) de Hamburgo, cujos membros têm por objectivo penetrar nos computadores do governo, da Casa Branca, da CIA. O clube demonstra, por exemplo, como é possível manipular o sistema de distribuição de água de uma cidade, etc.

**8.2.3 Exemplos de formações do Conselho da Europa**

**1. Ateliê de formação sobre a cibercriminalidade para procuradores, 26 de Agosto de 2008** (organizado pelo Ministério Público Estadual de Minas Gerais, em cooperação com o Conselho da Europa)

**Formação de nível elementar – 1 dia**

Programa:

- 1 Sessão de abertura
  - Nota de abertura
  - As reformas legislativas actuais
- 2 A cibercriminalidade: as suas manifestações
  - Visão geral das ameaças actuais
  - Ameaças específicas e processos investigados no Brasil

- 3 Direito material: que infracções?
  - Normas internacionais
    - Tipologia, conceitos jurídicos
    - Convenção sobre a Cibercriminalidade
  - Disposições na legislação brasileira
    - Disposições actuais
    - Reformas jurídicas em curso
- 4 Investigações e cooperação internacional
  - Papel dos procuradores nas investigações sobre a cibercriminalidade
  - Direito processual nacional
  - Medidas processuais e cooperação internacional previstas pela Convenção sobre a Cibercriminalidade
- 5 Parcerias público-privado
  - Exemplos de parcerias público-privado no Brasil
  - Repressão das infracções – cooperação dos fornecedores de serviços de internet na investigação da cibercriminalidade: orientações
  - Discussão: Cooperação entre as forças da ordem e os fornecedores de serviços de internet: a experiência no Brasil

## **2. Cibercriminalidade: formação para juizes, Cairo, Egipto, 9 e 10 de Junho de 2008**

(organizada pela Microsoft com a participação do Conselho da Europa).

*Esta formação foi dada por duas vezes a diferentes grupos de juizes de tribunais comerciais (também responsáveis pelas questões de cibercriminalidade)*

### **Formação de nível elementar – 1 dia**

Programa:

- 1 Sessão de abertura
- 2 A cibercriminalidade: as suas manifestações
  - Visão geral das ameaças actuais
  - Ameaças específicas
    - Utilização fraudulenta de identidades e de informações online: exemplos
    - Fraude com cartões de crédito e outros tipos de fraude
- 3 Direito material: que infracções?
  - Normas internacionais (perito do Conselho da Europa)
    - Tipologia, conceitos jurídicos
    - Convenção sobre a Cibercriminalidade
    - Criminalização do roubo de identidade
  - Disposições contidas na legislação nacional
    - Disposições actuais
    - Reformas jurídicas em curso

### **2ª Parte - A prova nos processos em matéria de cibercriminalidade**

- 4 Investigações e processos penais
  - Medidas processuais previstas na Convenção sobre a Cibercriminalidade
  - Papel da polícia, dos procuradores, dos juizes, dos serviços especializados
  - Direito processual nacional
- 5 Cooperação internacional
  - Convenção sobre a Cibercriminalidade
  - Disposições do direito nacional e acordos bilaterais
  - Pontos de contacto 24/7

- Papel dos juízes

6 Obtenção, preservação e utilização das provas electrónicas

- Provas no computador do arguido: Presença de ficheiros digitais utilizados no cometimento do crime cibernético
- Provas que identificam a localização de uma rede: endereços IP
- Provas obtidas a partir de fornecedores de serviços de internet

7 Processos judiciais e jurisprudência: exemplos

## **8.3 Exemplos de formações de nível avançado: estrutura e temas abordados**

### **8.3.1 Exemplo da formação dada nos Países Baixos**

#### **Formação aprofundada – 4 dias**

Programa:

#### **1º e 2º Dia**

##### *A infra-estrutura da internet*

- Compreender como funciona a internet
- Como comunicam os computadores entre si?
- O que é o endereço IP e o código de identificação do computador?

##### *Informação na internet*

- Como recolher informações na internet
- Pesquisa em bases de dados (escondidas) na internet

##### *Caracterização das Redes Sociais*

- comunicação
- anonimato
- determinação da localização e da identidade dos computadores, empresas e pessoas na internet

##### *Trilhos digitais*

- o que são os “trilhos”?
- que trilhos são deixados num computador?
- que trilhos são deixados na internet?
- que trilhos podem ser encontrados na comunicação digital?

##### *Segurança*

- os riscos da internet
- a importância de uma forte segurança digital
- armazenamento seguro de informações
- segurança em matéria de correio electrónico

Durante estes dois dias, cada participante tem acesso a um computador ligado à internet e pode fazer exercícios concretos relacionados com os temas abordados. Por exemplo, é dado aos participantes o nome de determinada pessoa e é-lhes pedido que reúnam o máximo de informação possível sobre essa pessoa em fontes de acesso livre na internet. Também lhes é solicitado que identifiquem a origem de um correio electrónico (a partir dos cabeçalhos da mensagem) ou de procurar trilhos de comunicação digital.

#### **3º e 4º Dia**

##### *O quadro jurídico*

- Quais as competências da polícia e dos procuradores nas investigações em matéria de cibercriminalidade
- Estudo de caso apresentado pela equipa de Criminalidade Tecnológica

*A Organização de investigação e de instauração de processos em matéria de cibercriminalidade nos Países Baixos;*

*Intercepção (este ponto não constará da nova formação e será integrado no programa elementar).*

##### *Contra-alegações digitais*

- quais as contra-alegações que se conhecem?

- jurisprudência relativamente a estas contra-alegações
- que contra-alegações devemos esperar no futuro, e como reagir a elas?
- estudos de casos

Cada participante recebe materiais de formação, um manual sobre todos os temas abordados durante a formação e que podem ser utilizados como obra de referência, uma versão impressa das apresentações dos formadores e a obra *Handboek Digitale Criminaliteit* de Arjan Dasselaar.

### **8.3.2 Proposta de formação de nível superior dos Países Baixos**

#### **Elaboração de uma nova formação em matéria de cibercriminalidade**

O "Intensiveringsprogramma Cybercrime", o Procurador nacional responsável pela Cibercriminalidade e o SSR (Centro de Formação Judiciária dos Países Baixos estão a elaborar uma nova formação em matéria de cibercriminalidade que abrange tópicos que vão desde a 'intercepção' a cursos especializados sobre temas específicos em cibercriminalidade (botnets).

O programa ainda não está concluído, mas o primeiro dia incidirá nos princípios essenciais da intercepção (escutas telefónicas e escutas na internet), o segundo dia será constituído por um curso elementar sobre cibercriminalidade. Ambos os cursos serão obrigatórios para *todos* os procuradores dos Países Baixos no quadro da sua formação permanente. A segunda parte da formação será reservada aos peritos em cibercriminalidade (as condições de admissão serão extremamente restritas) e consiste num curso de nível aprofundado (de 2 a 4 dias) e num curso superior de dois dias (anualmente). Estes cursos serão dados em cooperação com parceiros externos, como a Fox-IT, Digital Intelligence Training e Hoffman Bedrijfsrecherche.

A razão que motivou a criação deste programa não é o descontentamento com a formação existente, mas a vontade de estruturar e ajustar melhor os diferentes elementos de formar a evitar qualquer duplicação. A reestruturação da formação foi também fortemente motivada pela nomeação, no quadro do "Intensiveringsprogramma", de procuradores especializados em matéria de cibercriminalidade no seio dos onze principais serviços do Ministério Público neerlandês. É igualmente essencial que haja uma progressão na nova formação: cada participante deverá assim seguir os dois cursos elementares antes de ser admitido na formação aprofundada e cursos superiores.

Uma das novidades previstas para a nova formação será a realização de ilustrações infográficas que descrevam o funcionamento e os riscos da internet. Essas ilustrações estão nas fases finais da sua criação e podem ser igualmente utilizadas em apresentações experimentais. A seguir são dados alguns exemplos do aspecto das ilustrações infográficas.



## Seguimento

Para assegurar que os procuradores que lidam com a cibercriminalidade na sua prática quotidiana se mantêm actualizados com os desenvolvimentos no mundo dinâmico da cibercriminalidade, estão já a ser criados dois programas adicionais.

O primeiro diz respeito ao estabelecimento de um Centro de Conhecimentos Especializados no Serviço Nacional do Ministério Público em Roterdão. Este Centro dará resposta a questões de natureza técnica e judiciária, acompanhará a evolução da jurisprudência e divulgará esta, bem como toda a outra informação pertinente ao conjunto dos profissionais da cibercriminalidade, quer

da polícia, quer do Ministério Público (o centro é uma iniciativa conjunta de ambas as organizações).

Em segundo lugar, e na sequência deste projecto, está em fase de criação um "espaço de cooperação digital", comparável a uma aplicação SharePoint. Neste espaço virtual, os profissionais de cibernética poderão debater questões ligadas ao seu trabalho e encontrar todo o tipo de informações com interesse para o seu trabalho. Será feito um inventário dos conteúdos e das possibilidades (técnicas) desse espaço digital em Outubro deste ano. Eis um exemplo daquilo que poderia ser a página inicial desse espaço:

**OPENBAAR MINISTERIE**

OM Portal | Samenwerkingsruimte

Welkom Reinier van Loon | Mijn Site | Mijn Links

zoek....

Voorpagina | Agenda | Mensen | Documenten | Discussie

OM Portal > Samenwerkingsruimte > Cybercrime

**CRIME SCENE**

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Vivamus malesuada erat consectetur diam tincidunt faucibus. Nam facilisis justo ac risus dignissim a ornare lectus pretium. Aliquam id pretium quam. Ut at tortor arcu. Nulla sit amet velit dolor. Sed eu eros ac quam sagittis laoreet. Aliquam euismod faucibus malesuada. Pellentesque porttitor, nisi et accumsan porta, nisi arcu aliquet leo, nec euismod.

**Deelnemers samenwerkingsruimte**

Naam:	Functie:
Jan Hoekman	
Reinier van Loon	
Danielle Laheij	

[Deelnemers toevoegen](#)

**Laatste discussies / reacties**

Discussie	Aantal reacties:
Cybercrime of niet? <i>Nieuw</i>	0
Is downloaden strafbaar?	10

[Deelnemers toevoegen](#)

**RSS feed**

**Nu.nl (internet)**

- Liever zonder televisie dan zonder internet. *Nieuw*
- China blokkeert Google om porno. *Nieuw*
- Reparatie site Brein duurt zeker etmaal
- Thuiskopie wil schadevergoeding uitblijven mp3-heffing

[RSS feeds toevoegen](#)

**Laatste documenten**

Titel document:	Laatst bewerkt door:	Datum:
Samenvatting Plan van Aanpak Cybercrime <i>Nieuw</i>	Jan Hoekman	26 juni 2009 - 15:23
Plan van Aanpak Cybercrime	Reinier van Loon	19 mei 2009 - 08:42

[Document toevoegen](#)

**Agenda**

Agendat punten:	Datum:
Brainstorm Cybercrime Samenwerkingomgeving	29 juni 2009 - 15:00
Kickoff Cybercrime officieren	06 september 2009 - 14:00

[Agenda item toevoegen](#)

### Criar um sentimento de urgência: formação dos responsáveis

Dadas as capacidades relativamente limitadas das forças policiais neerlandesas, há que escolher quais os crimes que são investigados ou não (nota: o sistema jurídico neerlandês autoriza o Ministério Público a não investigar nem instaurar processos relativamente a determinadas infracções, é o chamado princípio do "opportuïteitsbeginsel"). Em geral, estas decisões são tomadas ao nível dos responsáveis.

Quer a polícia, quer o Ministério Público consideram que, a este nível, há uma falta de conhecimentos relativamente ao impacto da cibercriminalidade e à importância de a combater, pelo que há o risco de processos importantes não serem tratados porque outros crimes (convencionais) são considerados prioritários. É por esse motivo que está neste momento a ser criada uma formação destinada aos responsáveis da polícia e do Ministério Público. De acordo com o calendário, será dada uma formação piloto no final deste ano. Esta formação terá como objectivo a criação de um sentimento de urgência e irá sobretudo confrontar os responsáveis com a realidade da cibercriminalidade na sociedade actual. Assim, a formação não vai abordar os tópicos no plano dos conteúdos (que é o que faz a formação aprofundada), mas de um ponto de vista estratégico e administrativo.

