gabinete CIBERCRIME

# GABINETE CIBECRIME

# RELATÓRIO DA ACTIVIDADE

# 2013

PROCURADORIA-GERAL DA REPÚBLICA – GABINETE CIBERCRIME, Rua do Vale de Pereiro, nº 2, 2º, 1269-113 LISBOA
cibercrime@pgr.pt

# I. O Gabinete Cibercrime

O Gabinete Cibercrime foi criado por despacho de 7 de Dezembro de 2011, do Procurador-Geral da República, sendo-lhe dado o carácter de estrutura de coordenação da atividade do Ministério Público na área da cibercriminalidade. Pelo mesmo despacho foi designado como coordenador do projeto Pedro Verdelho e como coadjutora de coordenação Patrícia Agostinho, aos quais se juntou mais tarde, como colaborador permanente, por despacho da Sra. Vice-Procuradora Geral, o ponto de contacto distrital de Lisboa, Rui Batista.

# II. Escopo do Gabinete

O Gabinete Cibercrime tem como objetivos primordiais a coordenação interna do Ministério Público nesta área da criminalidade, o desenvolvimento de ações de formação específica nesta matéria e ainda a criação de canais de comunicação, em particular com órgãos de polícia criminal e com fornecedores de serviço de acesso às redes de comunicação, que permitam a respetiva colaboração na investigação criminal.

Quanto à coordenação do Ministério Público, foi estabelecido como objetivo específico desta estrutura coordenar uma rede de pontos focais que propiciem a troca de informação e experiências entre os magistrados do Ministério Público. No que respeita à formação, foi estabelecido que deveriam ser desenvolvidas ações de carácter abrangente, dirigidas a todos os magistrados em funções em tribunais ou departamentos criminais.

# III. Atividade desenvolvida

No cumprimento da missão e dos objetivos definidos, foram desenvolvidas, no ano de 2013, as atividades que de seguida se descrevem.

# 1. Coordenação no seio do Ministério Público

## 1.1. Reuniões com a rede de pontos de contacto

No decurso de 2013 foi dada continuidade a anterior estratégia de coordenação da atuação do Ministério Público na área do cibercrime e da obtenção de prova digital. Nesse sentido, foram realizadas reuniões com os pontos de contacto nos Distritos Judiciais de Évora, Coimbra e Porto. Não se tornou necessária a realização, durante 2013, de nenhuma específica reunião dos pontos de contacto do Distrito Judicial de Lisboa, uma vez que os mesmos participaram em reuniões diversas, realizadas em Lisboa, ao longo do ano, no decurso das quais se atingiram os objetivos propostos para estas reuniões.

Recorda-se que existe um magistrado ponto de contacto do Gabinete Cibercrime em cada círculo judicial, com a função de, por um lado, junto dos colegas, detetar dificuldades na investigação da cibercriminalidade e na obtenção da prova digital, tendo em vista a respetiva discussão com a rede de pontos de contacto e, por outro lado, ser apoio dos colegas das circunscrições, quando houver dúvidas nas investigações criminais relacionadas com estas temáticas.

Estas reuniões com os pontos de contacto distritais, em 2013, tiveram como finalidade, antes de mais, atualizar os magistrados quanto às diversas iniciativas do Gabinete Cibercrime, sobretudo no que respeita a novos protocolos celebrados, tendo em vista a obtenção de prova em processos concretos. Também se destinaram a discutir questões práticas, suscitadas nos processos, bem como boas práticas na obtenção de prova digital.

Neste âmbito, realizaram-se as seguintes reuniões:

- a 1 de Julho de 2013, no DIAP de Évora, com os pontos de contacto no Distrito Judicial de Évora, com a presença de 10 magistrados;
- a 9 de Outubro de 2013, no DIAP de Coimbra, com os pontos de contacto no Distrito Judicial de Coimbra, com a presença de 9 magistrados e
- a 13 de Dezembro de 2013, no Tribunal da Relação do Porto, com os pontos de contacto no Distrito Judicial do Porto, com a presença de 22 magistrados.

## 1.2. Reuniões com outros magistrados

Além das reuniões com os magistrados pontos de contacto, foram realizadas sessões em vários outros círculos, nos quais foi manifestado o interesse na realização das mesmas. Todas elas

resultaram de iniciativa e solicitação local. Por isso, procuraram ir ao encontro das questões suscitadas pelos magistrados – tiveram sempre uma estrutura informal, privilegiando a análise de casos reais e a discussão de concretas questões suscitadas nos processos.

Neste âmbito, realizaram-se as seguintes reuniões:

- a 5 de Março de 2013, no DIAP do Porto, com a presença dos 6 magistrados da 9ª Secção daquele DIAP. A esta sessão foi dada grande importância, uma vez que, em consequência da reestruturação/alteração da competência das secções do DIAP do Porto, a 1 de Fevereiro de 2013, a 9ª Secção passou a ter, em exclusivo, a competência para a investigação dos crimes previstos na Lei do Cibercrime (Lei 109/2009, de 15/09), na área do Círculo Judicial do Porto. Tal como já antes acontecia, desde 1994, com a 9ª Secção do DIAP de Lisboa, esta 9ª Secção do DIAP do Porto passou assim a ser especializada na área da criminalidade informática.
- a 19 de Novembro de 2013, no Palácio de Justiça de Aveiro, com magistrados em funções na Comarca do Baixo Vouga, contando com 38 participantes. Esta sessão teve a particularidade de permitir uma rica discussão multidisciplinar, uma vez que contou com a presença de inspetores da Polícia Judiciária e dos dois Juízes de Instrução em funções na Comarca.
- a 22 de Novembro, no Tribunal Judicial de Loures, com magistrados em funções no Círculo de Loures, com a presença de 7 magistrados.
- a 9 de Dezembro de 2013, no Tribunal Judicial de Portimão, com magistrados em funções no respetivo Círculo Judicial, com a presença de 17 magistrados.

### 1.3. Notas das reuniões

De todas essas reuniões com magistrados foram recolhidas importantes notas referentes à situação da investigação da cibercriminalidade e, sobretudo, referentes às investigações criminais, em geral, quando se torna necessária a recolha de prova em suporte digital.

#### 1.3.1. Questões referentes a métodos e procedimentos

a) Não tem sido claro o resultado da delegação de competência, nos termos da lei processual penal, para a investigação de inquéritos na área da cibercriminalidade ou que suponham o uso de meios informáticos ou de redes de comunicações. Em regra, os magistrados têm delegado a competência na Polícia Judiciária, dada a sofisticação técnica e as exigências específicas da investigação. Porém,

por vezes, a Policia Judiciária não tem desenvolvido as diligências de inquérito, devolvendo os processos sem investigação, por não se achar competente quanto a ela. Assim tem acontecido, por exemplo, com casos de injúrias ou difamações por meios tecnológicos. Neste tipo de situações, frequentemente, os magistrados acabam assumir diretamente a direção da investigação, uma vez que nem sempre se afigura viável a delegação de competência na PSP ou na GNR.

Na origem desta questão estão diferentes interpretações da Lei n.º 49/2008, de 27 de Agosto (Lei de Organização da Investigação Criminal). No Artigo 7º deste diploma descreve-se a competência da Polícia Judiciária em matéria de investigação criminal, dizendo-se, no nº 3, alínea l), que é da competência reservada da Polícia Judiciária a investigação dos crimes "informáticos e praticados com recurso a tecnologia informática". Esta disposição não tem interpretações unívocas, desde logo porque deixou de existir, após a entrada em vigor da Lei nº 109/2009, de 15 de Setembro, conteúdo legal para a expressão "crimes informáticos", que foi substituída na lei pela expressão "cibercrime".

b) Ainda no campo metodológico, foi manifestado por magistrados que haveria conveniência e vantagem na exigência de um guião de "diligências possíveis em casos específicos", sobretudo em relação aos casos mais frequentes: utilizações de dados de cartões de crédito por terceiros em compras *online,* criação de perfis falsos no Facebook e colocação em blogs de conteúdos com teor difamatório ou com fotografias cuja utilização não foi autorizada.

Um tal tipo de guião teria a virtualidade de permitir aos magistrados conduzir diretamente algumas das investigações, sem ter recorrer sistematicamente à delegação de competência na Polícia Judiciária, tanto mais que existe a perceção de que, no presente momento, aquela polícia não tem meios humanos capazes de dar resposta às inúmeras diligências de investigação.

### 1.3.2. Questões referentes a fenómenos criminógenos

Não existem estatísticas englobantes da cibercriminalidade em Portugal, mas as reuniões com magistrados permitiram aperceber que existem algumas grandes tendências nas queixas que têm dado entrada nos serviços do Ministério Público.

a) Uma das realidades criminais mais denunciadas é a da criação de falsos perfis em redes sociais (em particular no Facebook), com o nome de outra pessoa – é crescente o número de queixas relatando situações em que alguém cria um perfil com o nome de outra pessoa, tendo em vista

injuriá-la, difamá-la ou relatar factos da sua vida privada ou denegridores da sua imagem. Em regra, tais situações têm sido enquadradas como injúrias/difamações ou, em alternativa, como devassa da vida privada (Artigo 193º do Código Penal) ou, ainda como divulgação de fotografias (crime previsto no Artigo 199º, nº 2, alínea b) do Código Penal).

b) Em paralelo, têm sido crescentes as denúncias contra autores de blogs com conteúdos difamatórios – a que normalmente se associam comentários, de terceiros, igualmente difamatórios. Tal como nas redes sociais, também nos blogs tem sido denunciada a publicação não autorizada de fotografias.

c) Outra das grandes causas de denúncia tem sido a das burlas em compras na Internet. Têm sido registadas muitas queixas de cidadãos que compram objetos *online*, os quais depois não lhes são entregues. Estas queixas surgem normalmente isoladas e espalhadas pelas várias comarcas, mas correspondem frequentemente a ações de um mesmo indivíduo, que usa o mesmo método e os mesmos meios, de forma repetida, em relação a várias vítimas. Não existem mecanismos que permitam saber das várias investigações contra um só suspeito, de forma a poder vir a articulá-las – o que traria com certeza vantagens e sinergia às investigações.

d) O mesmo sucede com burlas referentes a emprego (na Internet), uso não autorizado de cartões de crédito para compras na Internet e *phishing*. Todas estas situações foram referidas como emergentes.

e) Ainda nesta área, embora com menor frequência, foram relatadas burlas em reservas de hotéis, com a criação de falsas páginas de hotéis, que aceitam reservas e pagamentos (em regra por preços muito mais baratos que noutros sites). O cliente do hotel apenas dá conta da burla quando chega ao hotel e a sua reserva não existe. Este tipo de queixas tem surgido mais em zonas turísticas (no Algarve).

f) Embora fora do conceito de cibercriminalidade, mas requerendo o recurso a meios digitais de prova, foram mencionadas como muito relevantes, as queixas por furto de telemóveis. Este segmento de criminalidade encerra grande relevância "digital", quer pelo conteúdo dos telefones (mensagens,

registo ou fotografias pessoais e íntimas, por exemplo), quer pela forma de chegar ao autor do furto e de demostrar essa mesma autoria, com uso das redes de comunicações.

Foi referido que, numa comarca da zona metropolitana do Porto, se estima que 25 a 30 % dos furtos denunciados são furtos de telemóveis. Não obstante, não há uma estratégia estabelecida para contrariar este tipo de furtos, nem para os investigar de forma eficaz. Por exemplo, não há rotina de bloqueio desses telefones furtados (que assim podem continuar a ser utilizados). O bloqueio é facilmente efetuado pelas operadoras, que o podem fazer a pedido do seu cliente e dono do telefone, mas não a pedido do Ministério Público.

Por outro lado, e ainda como exemplo, não tem havido o hábito de localizar telefones furtados usando *software* de geolocalização. Não obstante, foram descritos casos concretos em que telefones foram recuperados – e descobertos os autores do furto -, com recurso a este tipo de tecnologia.

Este tipo de procedimentos, além de conferir eficácia às investigações, seria também, com certeza, dissuasor da prática deste tipo de furtos.

Além disso, colateralmente, iria porventura reduzir casos de burla: foram relatados casos de queixas de furtos de telemóveis e *tablets* para fazer acionar o respetivo seguro, sem que o furto tivesse efetivamente ocorrido.

g) Ainda na área dos furtos, foram noticiados casos de furto de consolas de videojogos e de caixas descodificadoras de televisão por cabo, havendo alguns de entre eles em que é solicitado pelo queixoso que se averigue se as mesmas estão, ou não, a ser utilizadas *online* pelo seu possuidor. Esta diligência não se tem verificado viável, no caso das consolas, por a informação em causa apenas estar disponível em servidores no estrangeiro.

h) Os casos de crimes previstos na Lei do Cibercrime, embora referenciados, são em número pouco expressivo fora de Lisboa.

### 1.3.3. Questões referentes a dificuldades na investigação

Apercebeu-se dos magistrados dificuldade na compreensão dos conceitos e das regras referentes à obtenção de prova digital, apesar de, em geral, se assumir a sua crescente relevância, num número cada vez maior de processos.

a) Nalguns casos, estas dificuldades resultam de incoerências ou inconsistências do sistema legislativo. Assim acontece, por exemplo, pela dificuldade de conciliação entre a Lei nº 32/2008, referente à retenção de dados, e a Lei do Cibercrime (Lei nº 109/2009). Ou, também por exemplo, pela dificuldade prática de, no articulado da Lei nº 32/2008, distinguir entre dados de assinante e dados de tráfego. As discussões a este propósito culminam, em regra, na conclusão da necessidade de ajustamento legislativo.

b) Noutros casos, as dificuldades resultam da natureza das investigações e do ecossistema em que se desenrolam. Foi referida a impossibilidade de ter sucesso na identificação de suspeitos, se estes utilizarem servidores *proxy*, que em termos práticos tornam as suas comunicações quase anónimas. O mesmo se diga de suspeitos que utilizem pontos de acesso públicos à Internet (Juntas de Freguesia, bibliotecas públicas ou hotéis, por exemplo). Quanto a estes, não há nenhum mecanismo legal que permita ultrapassar o completo anonimato daqueles que acedem à Internet a partir deles.

c) Outro dos motivos que contribuem para o insucesso das investigações é a dificuldade de obter resultados positivos pelas vias da cooperação judiciária tradicional. Nem sempre é possível obter resposta às cartas rogatórias, sendo as razões e critérios para a não-resposta ou para a resposta negativa, por parte de autoridades estrangeiras, pouco claros. Ainda a este propósito tem sido notado que as traduções das cartas rogatórias são muito difíceis de conseguir e são muito demoradas.

d) O mesmo foi possível concluir quanto às perícias informáticas: na falta de alternativas, mesmo para casos simples, tem sido solicitada a Polícia Judiciária para este efeito. Porém, a realização das perícias tem sido demoradíssima, chegando a haver casos de demora superior a dois anos.

### 1.3.4. Questões referentes aos pedidos a operadores de comunicações

Uma das questões recorrentemente abordada nas reuniões foi a do pedido de informações a operadores de telecomunicações. Estes pedidos foram, durante muitos anos, muito problemáticos. A nota atual, porém, é de otimismo.

Em geral, os magistrados aderiram à utilização dos formulários criados pelo protocolo com os operadores e veiculados pela circular nº 12/2012 da Procuradoria-Geral da República. Foi frequentemente referido haver atualmente uma excelente resposta a esta prática: os operadores

respondem muito mais depressa (há casos de 10 dias, contra os vários meses de antes). Pelo contrário, quanto aos Magistrados que não usam os formulários (e fazer os pedidos por ofício, seguindo a prática tradicional), as respostas são muito mais demoradas.

O sentimento geral detetado foi o de que, em termos práticos, o protocolo firmado com os operadores de comunicações, em Julho de 2012, e os formulários vieram encurtar em muito a duração dos inquéritos.

### 1.4.
### Notas práticas

Uma das mais importantes notas recolhidas nas reuniões com magistrados foi a da falta de orientação no momento de interpretar a lei, sobretudo a respeito das regras respeitantes à obtenção de prova digital. Foi recorrentemente manifestada dificuldade em aplicar a lei ao caso concreto, sobretudo quanto a leis novas, que incidam sobre realidades técnicas sofisticadas, das quais há pouco conhecimento, sem que haja referenciais anteriores.

Tendo em vista superar esta dificuldade, em 2013, o Gabinete Cibercrime passou a coligir notas práticas, resultantes do debate nas reuniões de pontos de contacto. Estas notas práticas constituem regras de boas práticas sobre aspetos concretos da investigação.

Durante 2013 foram disponibilizadas duas notas práticas: uma delas sobre entendimentos doutrinários respeitantes ao endereço IP e à identificação do seu utilizador; a outra, respeitante à jurisprudência concernente à obtenção do endereço IP em inquérito. Juntam-se em anexo (Anexos 7 e 8).

## 2. Relacionamento com os fornecedores de serviço de comunicações

### 2.1.Operadores portugueses

No decurso de 2012 foram estabelecidos contactos com os maiores operadores portugueses de comunicações. Em sequência, foi assinado um protocolo com cinco desses operadores, procurando apontar para a diminuição das divergências de entendimento jurídico no relacionamento processual (em particular na obtenção de elementos de prova em posse dos operadores), tendo em vista um entendimento harmonizado quanto a questões controvertidas. Em termos concretos, em

consequência deste protocolo, a PGR e os operadores comprometeram-se a desenvolver contactos permanentes, tendo em vista melhor a cooperação. Além disso, previu-se que, quando o Ministério Público solicitasse aos operadores de comunicações elementos de prova, em concretos processos de inquérito, esses pedidos se fizessem com recurso a formulários pré-elaborados.

Este protocolo deu origem à Circular 12/2012 da PGR.

Durante 2013, a experiência veio a revelar que a adoção destes formulários tornou os pedidos mais simples, eficazes e expeditos, facilitando a respetiva satisfação pelos operadores. Ficou já acima relatada essa experiência (ponto 1.3.4).

## 2.2.Operadores globais

Foi prioridade para 2013 abordar os operadores globais, tendo em vista vir a estabelecer o mesmo tipo de entendimento que fora possível obter com os operadores portugueses.

Foram assim abordadas a Google Inc., a Microsoft Co. e a Facebook. Estas três operadoras globais foram selecionadas, desde logo, porque é muito significativo o número de pedidos de informação que se torna necessário fazer-lhes, em concretos inquéritos. Por outro lado, porque a respetiva política de relacionamento com operadores judiciários e policiais é amigável e permite o pedido de informações independentemente de solicitações formais, por via de pedidos de cooperação judiciária internacional. O mesmo não acontece, por exemplo, com a Twitter ou com a Yahoo!, cujas políticas a este propósito são muito mais formais, requerendo que toda a prestação de informação a entidades policiais ou judiciárias estrangeiras se faça no âmbito da cooperação judiciária internacional.

A 9 de Abril de 2013 realizou-se uma primeira reunião com a Google e a 23 de Abril o mesmo sucedeu com a Microsoft. Com a Facebook, a aproximação apenas foi possível durante o mês de Julho de 2013.

Com todas elas foi possível chegar a um entendimento de cooperação, de acordo com o qual os magistrados do Ministério Público de Portugal passaram a poder solicitar, diretamente, sem necessidade de recorrer a cartas rogatórias ou a outros mecanismos ou canais da cooperação internacional, alguns tipos de informações (correspondentes às informações que podem pedir, a nível doméstico, aos operadores nacionais, nos termos gerais do processo penal).

Assim, a partir de 18 de Setembro de 2013, passou a ser possível efetuar pedidos diretos à Google (incluindo o YouTube e o Blogger) e a partir de 28 de Novembro de 2013 o mesmo se passou com a

Facebook e a Microsoft. Os pedidos são possíveis por via de formulários que foram disponibilizados no SIMP.

Esta possibilidade operacional veio a revelar-se de grande eficácia prática, uma vez que veio a facilitar a obtenção de informação essencial à investigação criminal em situações em que anteriormente tal informação não era, na prática, de todo, possível de obter. Além disso, veio a permitir obter informação de operadores globais de forma muitíssimo expedita, sem necessidade das complexidades burocráticas dos mecanismos da cooperação judiciária internacional. A título exemplificativo, registou-se um caso (num inquérito do DCIAP, em que se investigavam pornografia de menores e abuso sexual de crianças) em que foi formulado um pedido de informação à Google Inc num determinado dia, às 16:51, sendo a respetiva resposta recebida, pelo DCIAP, nesse mesmo dia às 21:06. As experiências a este propósito recolhidas nas reuniões com magistrados em todo o país, embora ainda muito recentes, confirmam que, em geral, os pedidos a estas entidades foram satisfeitos com grande eficácia, num espaço muito curto de tempo.

## 3. Plataforma comunicacional

Em cumprimento de um dos objetivos do Gabinete Cibercrime, foi disponibilizada, no decurso de 2012, e tem vindo a ser regularmente atualizada, a área temática do SIMP dedicada ao Cibercrime.

Além disso, desde essa altura, passou a estar disponível *online* o espaço do Gabinete Cibercrime (http://cibercrime.pgr.pt) na página web da Procuradoria-Geral da República (www.pgr.pt).

Também nesta mesma ocasião passou a estar disponível o endereço eletrónico do Gabinete (cibercrime@pgr.pt).

Este último assumiu, em 2013, uma grande importância, por ser uma via de grande comunicação da comunidade com o Gabinete Cibercrime. Nesta caixa de correio foram recebidas, durante 2013, várias centenas de menagens, sobretudo a relatar crimes, métodos criminais e incidentes informáticos. A todas elas, com exceção das mensagens de *spam*, foi dada resposta. Por erro técnico, apenas foi possível contabilizar as mensagens recebidas depois de 30 de Julho de 2013. Entre essa data e o fim do ano, foram movimentadas nesta conta de correio eletrónico 106 mensagens.

O correio eletrónico foi, durante 2013, igualmente, uma importantíssima forma de comunicar com magistrados de todo o país. Por esta via foram colocadas ao Gabinete Cibercrime muitas questões

técnicas, sobretudo processuais. A todas as mensagens foi dada resposta. Por esta via, foram movimentadas, ao longo de 2013, 328 mensagens.

## 4. Intervenções noutras atividades da PGR

O Gabinete Cibercrime foi solicitado a intervir e participar em ações e reuniões promovidas pela Procuradoria-Geral da República. Assim aconteceu com os eventos que de seguida se descrevem.

### 4.1. Colóquio sobre «A Partilha de Ficheiros na Internet e o Direito de Autor»

Decorreu a 18 de Janeiro de 2013, na Procuradoria-Geral da República, contando com 70 participantes. Tratou-se de uma sessão de estrito carácter jurídico, que teve em vista a discussão de temáticas respeitantes à valoração jurídica da partilha de ficheiros na Internet, quando essa partilha significar violação de direito de autor (em particular na vertente penal). Esta temática surge, cada vez mais, em processos investigados pelo Ministério Público.

No decurso do colóquio, foram apresentadas comunicações por magistrados do Ministério Público, por representantes da Fundação para a Computação Científica Nacional e da Polícia Judiciária e ainda por advogados. Uma vez que existiam intenções legislativas governamentais neste domínio, foi ainda feita uma comunicação por representante da Secretaria de Estado da Cultura. Após as comunicações, decorreu um debate entre os oradores e os restantes participantes.

O evento contou com a presença da Senhora Procuradora-Geral da República e do Senhor Secretário de Estado da Cultura.

Do colóquio foram extraídas conclusões, que se juntam em anexo (Anexo 1)

### 4.2. Colóquio "Informação e Liberdade de Expressão na Internet e a Violação de Direitos Fundamentais - comentários em meios de comunicação *online*".

Realizou-se, na Procuradoria-Geral da República, a 17 de Junho de 2013 e foi repetido, na íntegra, a 13 de Dezembro de 2013, no Tribunal da Relação do Porto. Na sessão de Lisboa compareceram 45 pessoas e na do Porto 120. Ambas foram promovidas pela Procuradoria-Geral da República, com a colaboração da ERC – Entidade Reguladora para a Comunicação Social, dirigindo-se a magistrados e jornalistas, mas também a toda a comunidade jurídica.

Este colóquio pretendeu suscitar a reflexão sobre as consequências, ao nível da lesão de direitos fundamentais, dos comentários em meios de comunicação *online*, bem como sobre a viabilidade, à luz dos princípios e da técnica, da triagem de conteúdo *online* desta natureza, por parte dos órgãos de comunicação social. Pretendeu ainda clarificar a respetiva valoração jurídica criminal, tendo em vista propiciar aos magistrados do Ministério Público (e à comunidade jurídica) que possam consolidar opinião sobre esta problemática, quando a mesma se suscitar em sede judiciária.

Do colóquio foram extraídas conclusões, que se juntam em anexo (Anexo 2).

Quanto à versão realizada no Porto, foi realizada avaliação do mesmo, juntando-se em anexo o respetivo relatório (Anexo 3). Entre outras conclusões, esse relatório permitiu apurar que, de entre os 44 participantes que responderam à avaliação, 25 acharam que a organização dos conteúdos foi boa e 8 que foi muito boa. Ainda, 9 acharam esta organização satisfatória e apenas 2 fraca. Por outro lado, quanto à qualidade das comunicações, 22 dos 44 participantes acharam que foi boa e 10 muito boa. 10 dos respondentes acharam que as comunicações foram satisfatórias e apenas 4 que foram fracas.

### 4.3. Visitas de Procuradores-Gerais de outros Estados

O Gabinete Cibercrime participou nas sessões de receção aos Procuradores-Gerais da República de São Tomé e Príncipe, de Moçambique e da Finlândia, os quais realizaram visitas de trabalho à Procuradoria-Geral da República durante o ano de 2013.

#### 4.3.1. São Tomé e Príncipe

Aquando da visita do Senhor Procurador-Geral da República de São Tomé, a 15 de Maio de 2013, o Gabinete Cibercrime teve oportunidade de, numa reunião de trabalho, apresentar ao Senhor Procurador-Geral as suas atividades. Na altura, suscitou muito interesse do Senhor Procurador-Geral o plano de formação de magistrados nesta área específica.

Por aquele representante do Ministério Público de São Tomé foi também manifestado interesse no regime legal em vigor em Portugal, quanto à cibercriminalidade e à obtenção de prova em formato digital. Foi igualmente manifestado interesse em que viesse a ser dado apoio à PGR de São Tomé, no trabalho de elaboração de um eventual anteprojeto legislativo nesta área.

No presente momento, São Tomé e Príncipe não dispõe de legislação a este propósito, quer substantiva, quer processual, quer ainda quando a cooperação judiciária internacional (aliás, quanto

a esta última, a lacuna é integral, uma vez que o país não dispõe de quadro normativo geral enquadrador da cooperação judiciária internacional).

Quanto a todas estas matérias, foi manifestada disponibilidade para ulteriormente se desenvolverem contactos e cooperação com a Procuradoria-Geral de São Tomé e Príncipe.

### 4.3.2. Moçambique

A 17 de Junho de 2013, decorreu uma reunião do Gabinete Cibercrime, com o Senhor Procurador-Geral da República de Moçambique e outros magistrados Moçambicanos, integrada na agenda da respetiva visita à Procuradoria-Geral da Republica, em Lisboa.

No decurso dessa reunião, foi apresentado ao Senhor Procurador-Geral da República de Moçambique o Gabinete Cibercrime e foram descritas as respetivas atividades.

Tal como acontecera com o Procurador-Geral de São Tomé, também agora suscitou interesse a formação de magistrados na área do cibercrime e da obtenção de prova em formato digital. Da mesma forma, também houve visível interesse manifestado no quadro normativo português a propósito da cibercriminalidade e da prova digital. Foi igualmente manifestado interesse em que viesse a ser dado apoio à PGR de Moçambique, no estudo de um eventual anteprojeto legislativo nesta área, tanto mais que está em curso o processo de revisão dos códigos Penal e de Processo Penal de Moçambique, os quais se encontram em sede de análise parlamentar, esperando-se, para breve, a respetiva aprovação.

No presente momento, Moçambique não dispõe de qualquer diploma legislativo a propósito de cibercrime ou prova digital, quer no campo do direito substantivo, quer no campo processual.

Quanto a todas estas matérias, foi manifestada disponibilidade para ulteriormente se desenvolverem contactos e cooperação com a Procuradoria-Geral da República de Moçambique.

### 4.3.3. Finlândia

O Gabinete Cibercrime participou na sessão de trabalho, realizada a 17 de Outubro de 2013, com o Senhor Procurador-Geral da Finlândia. No decurso desta sessão foi possível apresentar o Gabinete e o seu modelo de funcionamento, bem como fazer uma breve apresentação sobre a temática "*Approach on issues relating to the «specialisation» of the Public Prosecution Service*".

## 5. Intervenções em sessões externas

Durante 2013, o Gabinete Cibercrime foi solicitado a intervir e participar em eventos externos, alguns dos quais, em representação da Procuradoria-Geral da República.

### 5.1.Na GNR de Santarém

A 23 de Janeiro de 2013, o Gabinete Cibercrime dinamizou uma sessão formativa no Comando Distrital de Santarém da Guarda Nacional Republicana, que contou com a presença dos cerca de 80 oficiais e sargentos ao serviço na GNR no Distrito de Santarém. Tratou-se de uma sessão formativa sobre cibercrime e prova digital, promovida pelo ponto de contacto do Gabinete Cibercrime no Círculo de Santarém.

### 5.2. No Centro de Estudos Judiciários

No decurso de 2013, o Gabinete Cibercrime cooperou na realização de duas ações de formação contínua do CEJ: uma delas ocorreu a 8 de Março de 2013 (o "Colóquio sobre Cibercriminalidade"); a outra ocorreu a 15 de março de 2013 (o "Colóquio sobre Prova Digital e Prova em Ambiente Digital").
Ambas as sessões decorreram no Auditório do Centro de Estudos Judiciários e se destinaram a juízes, magistrados do Ministério Público e outros profissionais da área forense. Neles intervieram, além do Gabinete Cibercrime, alguns dos seus pontos de contacto, com comunicações.
A 31 de Maio de 2013 o Gabinete Cibercrime participou numa outra sessão no CEJ, sobre a temática geral do cibercrime e da prova digital, destinada aos auditores do XXXº Curso Normal de Formação.
O Gabinete foi ainda solicitado a intervir numa ação não prevista no plano anual de atividades do CEJ, sobre "Sociedade da Informação e Direito", realizada a 19 de Dezembro de 2013. Foi solicitado ao Gabinete que moderasse um painel sobre "Internet e modelos de negócios, infraestruturas de Internet Básica e Serviços Básicos de Internet".
Também esta sessão decorreu no Auditório do Centro de Estudos Judiciários, destinando-se sobretudo a juízes e magistrados do Ministério Público.

### 5.3. Na Universidade Católica

O Gabinete Cibercrime foi solicitado para fazer e efetivamente fez, uma apresentação sobre "A obtenção de prova eletrónica e a lei do cibercrime", num seminário sobre "A internet e o direito", na

Universidade Católica Portuguesa – Escola de Lisboa, a 14 de Março de 2013. Este seminário destinou-se ao público universitário da área do direito e foi promovido pela ELSA (*European Law Students' Association*).

### 5.4. No Instituto Politécnico de Beja

Decorreram em Beja, no Instituto Politécnico, a 30 de Maio de 2013 as jornadas SimSIC, organizadas pelo Laboratório UbiNET - Segurança Informática e Cibercrime, daquele Instituto. O Gabinete Cibercrime foi solicitado a participar, num painel sobre cibercrime.

### 5.5. Na Faculdade de Direito da Universidade de Lisboa

Promovida pelo ICP-ANACOM, em colaboração com o Centro de Investigação Jurídica em Cibersegurança da Faculdade de Direito da Universidade de Lisboa, decorreu uma ação de "Formação sobre Segurança da Informação", a 28 de Junho de 2013. O Gabinete Cibercrime participou com apresentações sobre "Enquadramento legal – princípios e normas em matéria de segurança da informação" e sobre "A Eurojust e o cibercrime – as entidades reguladoras".

### 5.6. Com a Associação Portuguesa de Apoio à Vítima

A Associação Portuguesa de Apoio à Vítima – APAV realizou, a 23 e 24 de Setembro de 2013, em Lisboa, na Fundação Calouste Gulbenkian, o "Seminário Internacional Infovítimas - o Direito das Vítimas de Crime à Informação". O Gabinete Cibercrime foi solicitado a colaborar na moderação da sessão de *workshop* "Informação a crianças e jovens".

### 5.7. Com a Associação Internacional das Comunicações de Expressão Portuguesa

A 27 de Setembro de 2013, a Associação Internacional das Comunicações de Expressão Portuguesa – AICEP, realizou em Lisboa, na Fundação Portuguesa das Comunicação, o Seminário "PROJEP Direito das Comunicações", solicitando a intervenção, do Gabinete Cibercrime, que veio efetivamente a ocorrer, com uma comunicação.

### 5.8. Com a Autoridade Nacional das Comunicações

A Autoridade Nacional das Comunicações – ANACOM, em colaboração com a Direção Geral das Atividades Económicas – DGAE, organizou, a 30 de Setembro de 2013, na Fundação Portuguesa

das Comunicações, em Lisboa, um *workshop* sobre "Cibersegurança: aspectos económicos", com o objetivo de informar, debater e avaliar o impacto económico da Diretiva para implementação de medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União Europeia (Diretiva SRI). Foi solicitado ao Gabinete Cibercrime que efetuasse uma comunicação sobre a "Vertente económica do cibercrime".

### 5.9. Com a Fundação Portuguesa A Comunidade Contra a Sida

A 7 de Novembro de 2013 decorreu, na Faculdade de Ciências Médicas da Universidade de Lisboa, uma sessão solicitada ao Gabinete Cibercrime pela Fundação Portuguesa A Comunidade Contra a Sida, em cooperação com a Associação Nacional de Estudantes de Medicina. Esta sessão submeteu-se ao tema "Perigos da Internet" e inseriu-se na Formação Científica para Voluntários Universitários de Intervenção no "Projeto Nacional de Educação pelos Pares".

### 5.10. Na Direção-Geral da Política de Justiça do Ministério da Justiça

A Direção-Geral da Política de Justiça – DGPJ, promoveu, a 21 de Novembro de 2013, nas suas instalações no Campus da Justiça, os "Encontros de Direito Internacional 2013", submetidos à temática geral da "Prevenção e combate à cibercriminalidade". Foi solicitado ao Gabinete Cibercrime que interviesse com duas comunicações: uma delas sob a "Abordagem internacional do combate à cibercriminalidade e o contexto interno" e a outra sobre as "Dificuldades e limitações práticas do quadro jurídico interno no combate à cibercriminalidade".

### 5.11. Na Comunidade dos Países de Língua Portuguesa

A Comunidade dos Países de Língua Portuguesa - CPLP, em colaboração com a Agência para a Modernização Administrativa - AMA, e a Associação para a Promoção e Desenvolvimento da Sociedade de Informação - APDSI, promoveram a 1ª Conferência CPLP de Governo Eletrónico, em Lisboa, na sede da CPLP, a 29 de Novembro de 2013. O Gabinete Cibercrime participou na conferência, em representação da Procuradoria-Geral da República, por determinação da Senhora Conselheira Procuradora-Geral da República.

### 5.12. Com a Secretaria de Estado de Cultura de Espanha

Realizou-se, em Lisboa, na Fundação Gulbenkian, a 2 de Dezembro de 2013, um encontro promovido pela Secretaria de Estado de Cultura de Espanha, sobre "Propriedade intelectual na Internet". Foi solicitado ao Gabinete Cibercrime que efetuasse, no decurso desse encontro, uma apresentação sobre "Partilha de conteúdos *online* e direito de autor".

## 6. Participação, em representação da PGR, em projetos de outras entidades

### 6.1. Com a Procuradoria-Geral da Holanda

A Procuradoria-Geral da República apresentou-se, como parceira da PGR da Holanda, em candidatura a financiamento da União Europeia, ao desenvolvimento de um projeto na área do cibercrime – sem que, em todo o caso, isso implicasse qualquer custo financeiro para a Procuradoria-Geral da República ou o Estado Português. Esta participação foi autorizada por despacho do Senhor Vice Procurador-Geral da República de 4 de Março de 2013.

O propósito deste projeto é, em termos genéricos, o estudo dos mercados ilegais em zonas escondidas da Internet (por exemplo com utilização do protocolo TOR) e o desenvolvimento de ações multidisciplinares e multilaterais contra esta atividade. Anote-se que a Procuradoria-Geral da República foi o único parceiro da PGR da Holanda neste projeto, que veio a ser aprovado pela União Europeia a 18 de Setembro de 2013, sendo-lhe conferido um financiamento de 393.763,97 €, que deverão representar 90% dos custos totais do mesmo. Junta-se, em anexo, a decisão da Comissão Europeia (Anexo 4).

O arranque no desenvolvimento do projeto decorrerá em 2014.

### 6.2. Com a Associação Portuguesa de Apoio à Vítima

A Procuradoria-Geral da República apresentou-se, como parceira da Associação Portuguesa de Apoio à Vítima – APAV, em candidatura a financiamento da União Europeia, ao desenvolvimento de um projeto na área do roubo da identidade – também este projeto não implica nenhum custo financeiro para a Procuradoria-Geral da República ou o Estado Português. Esta participação foi autorizada por despacho do Senhor Vice Procurador-Geral da República de 21 de Fevereiro de 2013.

A este propósito, o Gabinete Cibercrime contactou ainda congéneres de Espanha, da Roménia e do Reino Unido, tendo em vista a respetiva participação no projeto. Veio a ser obtida resposta favorável de Espanha (*Fiscalía Especialista en Materia de Delincuencia Informática*) e da Roménia (*Cybercrime Unit*, do *Prosecutor's Office attached to the High Court of Cassation and Justice*).
O projeto foi aprovado para financiamento da União Europeia e espera-se o respetivo arranque para 2014.

## 7. Plano de ação "Crimes contra Crianças na Internet"

### 7.1. O plano de ação

O decurso do ano de 2013 revelou vários sintomas do risco da exposição de crianças e jovens a conteúdos nocivos na Internet e a ações criminosas utilizando as vulnerabilidades da sua conectividade permanente às redes de comunicação. Entendeu, por isso, a Procuradoria-Geral da Republica lançar um Plano de Ação sobre "Crimes contra Crianças na Internet".
Como objetivo geral deste plano de ação pretende-se que os magistrados do Ministério Público venham a lidar mais eficientemente com todos os fenómenos criminais contra crianças, quando cometidos com o uso das tecnologias da informação e da comunicação. Este propósito requer, de cada magistrado, um melhor conhecimento desta realidade e das suas manifestações em Portugal, mas também supõe que se suscite o interesse da comunidade – das crianças em particular – pelo tema. Além disso, visa o plano de ação que o Ministério Público (e toda a comunidade judiciária, na verdade) sejam sensibilizados para a importância crescente desta realidade, por exemplo, por meio de formação específica. Por último, mas não menos importante, uma abordagem eficaz desta problemática requer que se promova o permanente diálogo entre os magistrados do Ministério Público e outras entidades e intervenientes na área, de forma a mais facilmente permitir o intercâmbio de informações, sempre que necessário, no caso concreto.
O plano de ação foi publicamente anunciado durante a conferência "As crianças e a Internet - uso seguro, abuso e denúncia", a 4 de Outubro de 2013, em Lisboa. Esta conferência decorreu na Procuradoria-Geral da República e contou com 60 participantes (a maior parte dos quais, magistrados do Ministério Público).

Desta conferência, ela mesma uma atividade formativa, foram retiradas conclusões, que se juntam em anexo (Anexo 5). Por outro lado, foi feita a respetiva avaliação, a partir de inquéritos aos participantes, cujo relatório se junta igualmente em anexo (Anexo 6). Do mesmo pode retirar-se que, dos 8 participantes que responderam, quanto ao conteúdo do colóquio (organização dos conteúdos, relevância prática dos temas, qualidade dos oradores e das comunicações), nenhum deles achou ter sido fraco ou satisfatório, sendo todas as respostas na área do bom e, sobretudo, do muito bom. O mesmo sucedeu quanto à apreciação global do colóquio.

**7.2. Brochura "Tu e a Internet - (ab)uso, crime e denúncia",**

Nessa mesma ocasião, 4 de Outubro de 2013, foi lançada a brochura "Tu e a Internet - (ab)uso, crime e denúncia", dirigido a crianças e adolescentes, com textos da responsabilidade da Senhora Procuradora-Geral da República e do Gabinete Cibercrime e com ilustrações (desenhos) elaboradas por alunos de escolas de Lisboa.

O objetivo desta brochura foi contribuir, através da informação e da consciencialização, para a utilização mais segura da Internet, abordando os comportamentos em relação a crianças que possam constituir infração criminal. Dão-se explicações sobre essas infrações e sobre como apresentar queixa das mesmas, mas também se aponta para a existência de outras respostas, além da criminal, que podem garantir os direitos das crianças e dos jovens que sejam vítimas do mau uso da Internet.

A brochura foi traduzida para inglês. Está livremente disponível, para leitura ou *download* em formato pdf, em português e em inglês, em http://cibercrime.pgr.pt.

Esta brochura, “Tu e Internet”, veio a ser referenciada pelo Conselho da Europa, a 31 de Outubro de 2013, e apresentada na Rede de Parlamentares de Referência para a Convenção de Lanzarote. Foi referenciada pelo Conselho da Europa, sendo colocada em destaque na área Cibercrime do respetivo *site* Internet, sendo mencionada como uma iniciativa que deve constituir um exemplo para outros países. Por outro lado, a brochura foi apresentada, a 13 de Novembro de 2013, em Genebra, na Reunião da Rede de Parlamentares de Referência para a Convenção de Lanzarote. Segundo a representante da Assembleia da República naquela Rede, Deputada Maria de Belém Roseira, o projeto suscitou grande agrado nos parlamentares europeus, que o acharam magnífico.

### 7.3. Plano de formação de magistrados

Ainda no âmbito deste plano de ação, foi estabelecido um programa de formação para magistrados do Ministério Público, com sessões previstas para todos os distritos judiciais (Coimbra, Évora, Lisboa e Porto).

Ainda no decurso de 2013, foi realizada a sessão para os magistrados do Distrito de Lisboa, em Almada, a 10 de Dezembro de 2013, ficando agendadas para 2014 as restantes sessões (para 9 de Janeiro, na Figueira da Foz, para o Distrito de Coimbra, para 7 de Março, em Ponte de Lima, para o Distrito do Porto e para 12 de Março, em Beja, para o Distrito de Évora). À sessão de Almada compareceram 32 magistrados do Ministério Público.

## 8. Contacto com a Sociedade Portuguesa de Autores

No decurso de 2013, o Gabinete Cibercrime estabeleceu contactos com a Sociedade Portuguesa de Autores - SPA, em sequência de instruções recebidas, após audiência concedida pela Senhora Procuradora-Geral à SPA. Tais contactos tiveram em vista explorar possíveis formas de cooperação entre a PGR e a SPA, que viessem depois a ser acordadas em protocolo entre as duas instituições.

Decorreu uma primeira reunião a 19 de Junho de 2013, que veio a dar origem, durante o verão, a um esboço de protocolo de entendimento. Este esboço veio a ser aprovado pelas duas instituições. Porém, por razões de agenda, a assinatura do protocolo apenas veio a ser agendada para 13 de Janeiro de 2014.

## 9. Contacto com oficiais de ligação dos Estados Unidos tendo em vista a investigação de crimes relacionados com a exploração sexual de crianças

O Gabinete Cibercrime foi solicitado para receber, em reunião, representantes do *Federal Bureau of Investigation* (FBI) e do *Immigration and Customs Enforcement* (ICE) do *Department of Homeland Security* junto da Embaixada dos Estados Unidos da América.

Em consequência, decorreram duas reuniões na Procuradoria-Geral da República, a 3 de Julho de 2013, com o FBI e a 5 de Julho de 2012, com o ICE. Nesta última, foi apresentado ao Gabinete

Cibercrime o trabalho do *National Center for Missing and Exploited Children* (NCMEC) dos Estados Unidos.

Esta organização não-governamental, mas tutelada pelo Congresso dos Estados Unidos, tem como propósito recolher, com vista à sua transmissão às autoridades policiais/judiciais territorialmente competentes, quer dentro dos Estados Unidos, quer noutros países, toda a informação disponível sobre crianças desaparecidas e sobre crianças exploradas sexualmente: informação sobre eventuais utilizadores de *sites* Internet onde se divulgue pornografia infantil, bem como de canais de assédio a crianças para a prática de atos sexuais ou de prostituição.

Desde há vários anos que o NCMEC tem vindo a identificar, anualmente, centenas de situações de eventual crime relacionado com crianças (pornografia infantil ou assédio para actos sexuais) com ligação a Portugal – ou seja, cujo eventual autor utilizou, para aceder à Internet, um endereço IP pertencente a um operador de comunicações português. Estas situações têm sido comunicadas pelo NCMEC ao ICE, que as tem retransmitido a autoridades policiais portuguesas. Foi manifestado que o *Department of Homeland Security* gostava de passar a encaminhar diretamente para a PGR estes dados recolhidos pelo NCMEC, tendo em vista a eventual abertura de investigações pelo Ministério Público.

Sobre esta matéria veio a ser emitida a Circular nº 02/2013 da Procuradoria-Geral da República, de 17 de Outubro de 2013 (publicada no Diário da República, 2.ª série, nº 213, de 4 de Novembro de 2013), que atribuiu ao DCIAP competência para iniciar, exercer e dirigir a ação penal relativamente a crimes sexuais praticados contra menores com recurso a meios informáticos ou divulgados através destes, cuja notícia de crime seja adquirida através de comunicações provindas de outros Estados e organizações internacionais. Foi ainda emitido o despacho nº 12/2013 do Senhor Diretor do DCIAP, que implementou, no concreto, aquela circular.

Desde, 24 de outubro de 2013, data deste último despacho, até ao final do ano de 2013, derem entrada no DCIAP 52 participações provenientes do NCMEC e remetidas pelos oficiais de ligação Norte-Americanos. Destas 52 participações, 34 respeitavam a *upload* de imagens pornográficas de crianças, 17 a *upload* de vídeos desse mesmo teor e 1 a uso de *webcam* para obtenção desse tipo de imagens. Por outro lado, tendo também como referência o final do ano de 2013, quanto aos inquéritos a que essas denúncias deram origem, que foram 33, 1 deles foi arquivado no DCIAP e noutros 15 estavam a ser desenvolvidas diligências de investigação. Os 17 restantes tinham já sido

remetidos a outras comarcas, por ter sido identificado um suspeito residente nas respetivas circunscrições.

## 10. Protocolo com o Instituto Politécnico de Beja

A partir de 8 de Julho de 2013, foram estabelecidos contactos, da iniciativa do Gabinete Cibercrime, com o Instituto Politécnico de Beja – e em particular com o Laboratório UbiNET - Segurança Informática e Cibercrime, no seio da Escola Superior de Tecnologia e Gestão.

Este diálogo veio a culminar com a assinatura, a 17 de Outubro de 2013, de um protocolo de cooperação da Procuradoria-Geral da República com o Instituto Politécnico de Beja, com particular incidência na área informática e das tecnologias da informação e comunicação. Por via deste protocolo, o Instituto Politécnico de Beja comprometeu-se a criar uma bolsa de peritos informáticos, de entre os seus docentes e alunos do mestrado em Engenharia de Segurança Informática, à qual o Ministério Público poderá recorrer, quando tiver necessidade de fazer intervir um perito, em processo penal. Deste protocolo resultou, em termos práticos, que quando um magistrado entender necessitar da intervenção de um perito, passa a poder solicitar a sua indicação (embora o deva fazer por via do Gabinete Cibercrime e deva usar, para o efeito um formulário disponível no SIMP Temático Cibercrime).

O primeiro resultado prático da celebração deste protocolo foi o da designação de um perito para intervir em processo pendente na Comarca do Alentejo Litoral, a 2 de Janeiro de 2014.

# IV. Linhas de Ação para 2014

A experiência adquirida recomenda, no decurso de 2014, além de outras iniciativas:

- desenvolver o conhecimento sobre a realidade do cibercrime em Portugal, de forma a ter um mais aproximado diagnóstico da mesma;
- estudar formas especiais de encarar alguns dos tipos de criminalidade online (por exemplo burlas *online*, ou *phishing*);
- avaliar a eficácia e mais valia dos mecanismos processuais desenvolvidos em 2013 (por exemplo, os respeitantes ao relacionamento com os operadores de comunicações);

- desenvolver contactos com novas instituições universitárias, tendo em vista ampliar as possibilidades de estabelecer protocolos com as mesmas, tendo em vista alargar a capacidade de recrutar peritos para os processos concretos;
- fortalecer os contactos com os órgãos de polícia criminal, sobretudo tendo em vista partilhar conhecimentos respeitantes à obtenção de prova em formato digital e
- desenvolver ações específicas de formação sobre a investigação dos crimes online mais frequentes.