RELATÓRIO DA ACTIVIDADE

SETEMBRO 2015 a DEZEMBRO 2016

Gabinete Cibercrime

MINISTÉRIO PÚBLICO
PORTUGAL

PROCURADORIA-GERAL DA REPÚBLICA
GABINETE CIBERCRIME

gabinete cibercrime
fevereiro 2017

cibercrime@pgr.pt
http://cibercrime.ministeriopublico.pt/

ÍNDICE

ANEXOS

A. O GABINETE CIBERCRIME

1. O Gabinete Cibercrime é uma estrutura informal da Procuradoria-Geral da República criada, nos termos dos Artigos 11º e 12º, nº 2, alínea b) do Estatuto do Ministério Público, pelo despacho do Procurador-Geral da República, de 7 de dezembro de 2011. Tem como propósito genérico a coordenação da atividade do Ministério Público na área da cibercriminalidade e da obtenção de prova digital.

Nos termos daquele despacho, o Gabinete Cibercrime tem como objetivos primordiais a coordenação interna do Ministério Público, o desenvolvimento de ações de formação específica nesta matéria e fomentar o funcionamento de canais de comunicação, em particular com órgãos de polícia criminal e com fornecedores de serviço de acesso às redes de comunicação e informação, que permitam apoiar a investigação criminal, tendo em vista melhorar a respetiva eficácia.

B. A CIBERCRIMINALIDADE

2. A Convenção de Budapeste de 2001 instituiu a expressão *cibercrime*, tomando como referência realidades anteriormente incluídas na categoria a que o direito português chamava (no quadro da antiga Lei da Lei nº 109/91) *criminalidade informática*. Este novo conceito veio a ser integrado no direito português, pela Lei do Cibercrime (Lei nº 10972009), herdeira da antiga Lei da Criminalidade Informática. Em ambos os diplomas se preveem específicos tipos legais de crime contra sistemas de computadores ou sistemas de informação. Porém, quer no senso comum, quer na prática judiciária, a cibercriminalidade tem-se revelado de muito maior espectro, incluindo muitos outros crimes, de natureza diversa, que têm de comum entre eles serem praticados com auxílio das tecnologias, ou por via das tecnologias. A eles se aplicam os mesmos métodos e modelos de investigação do cibercrime. Também quanto a eles (da mesma forma que acontece com os chamados *cibercrimes em sentido restrito*), é necessário obter prova em formato digital, por vezes por via de perícias. Estão dentro deste conceito alargado de cibercrime as burlas em plataformas de vendas na Internet, ou a difusão, *online*, de pornografia infantil, ou ainda as injúrias ou difamações cometidas por via dos sistemas de informação.

3. A atividade do Gabinete Cibercrime visa enquadrar todos estes fenómenos criminógenos, relacionados com as tecnologias ou praticados por via destas. Trata-se de uma realidade de difícil avaliação estatística. De facto, não há estatísticas que descrevam de forma cabal a dimensão dos crimes ocorridos *online*: havendo ferramentas que indicam quantos processos foram instaurados por cada um dos tipos de crime, as mesmas não permitem saber quais deles supuseram a utilização das redes de comunicações. As estatísticas disponíveis no sistema de justiça descrevem, por exemplo, as injúrias, mas não as injúrias cometidas por via das tecnologias. Descreve as burlas, mas não autonomiza as que são praticadas em plataformas na Internet.

Como se sublinhou em relatórios anteriores, o conhecimento da criminalidade *online* apenas é possível por via empírica, resultante do contacto com os magistrados encarregados das investigações.

4. Como mais abaixo melhor se referirá, no decurso do período a que se refere este relatório, foram realizadas sessões de coordenação em todas as comarcas do território de Portugal continental. No decurso dessas sessões, procurou aperceber-se a realidade da criminalidade de cada comarca, quanto a crimes relacionados com sistemas informáticos, com o propósito de melhor direcionar a sessão para os específicos problemas como que se deparam os magistrados. Esta análise permitiu, noutra vertente, identificar tendências criminógenas, algumas das quais comuns a todo o país.

5. Verificou-se assim que uma das mais importantes manifestações criminais que têm chegado ao Ministério Público são as burlas em vendas *online* (compra de objetos que, depois, não são entregues, mas também por vezes a venda de objetos, com entrega do mesmo, sem que o pagamento seja feito). Tais vendas fraudulentas têm sido denunciadas, quer em plataformas legítimas de vendas, quer em perfis do Facebook que, logo de seguida, são apagados, quer ainda em páginas *web* deliberadamente abertas para este efeito (em regra, domiciliadas em servidores estrangeiros).
Em todas as comarcas foi relatado que este é um fenómeno que, apesar de ser já muitíssimo expressivo é também grandemente crescente. Foi relatado que, por exemplo, no DIAP da Amadora (Comarca de Lisboa Oeste), cerca de um terço da criminalidade denunciada se refere a burlas *online*. Mesmo em comarcas de menor dimensão, foi sublinhada a expansão crescente deste fenómeno. Na Guarda, por exemplo, foi relatado haver, por ano, largas dezenas de casos de burlas cometidas pela Internet.
Algumas comarcas registam burlas desta natureza com contornos peculiares. Assim, na comarca de Faro, por exemplo, foi reportado ter muita expressão o número de burlas *online* no arrendamento de casas de férias.

6. Outras das realidades criminais com grande expressão é a do uso abusivo de dados de cartões de crédito. Tem sido denunciado com recorrência o uso de dados de cartões de crédito para pagamentos, sobretudo em *sites* de vendas na Internet – é menos significado o número de casos de pagamentos em lojas físicas e é ainda menor o dos casos de pagamentos em Portugal. Uma boa parte destes inquéritos têm origem em mensagens de alerta ou comunicações recebidas pelos clientes, do seu banco ou da entidade emissora do cartão de crédito em causa.

7. Foram igualmente noticiados muitos casos de queixas por prática de *phishing* bancário. Este tipo de fenómeno criminal assumiu já uma grande dimensão. Na comarca de Lisboa Norte foi referido que, em média, darão entrada, talvez, 20 a 30 casos novos, por mês. No DIAP de Lisboa este tipo de inquéritos está distribuído às 3ª e 8ª Secções, as quais investigam todo o tipo de burlas. Foi dada conta de que, nestas secções, cerca de um terço dos processos respeitam a *phishing*.
A este propósito, foi repetidamente comentado que é frequente serem identificados e criminalmente responsabilizados os chamados *money mules*, mas não os restantes interventores no processo criminoso. Além disso, apercebeu-se haver divergência e discussão sobre a qualificação jurídica desta atuação, dos *money mules*.

Foram ainda noticiados muitos casos em que os *money mules* foram angariados para esta prática por via de ofertas de emprego, o qual consistia precisamente em transferir e levantar quantias em dinheiro.

8. Foi em geral referido terem igualmente grande significado estatístico, as participações respeitantes à criação de perfis falsos em redes sociais (em particular no *Facebook*). Normalmente, estes perfis *falsos* estão associados, quer à disseminação de conteúdo injurioso (em especial textos ou fotografias), quer à divulgação de dados pessoais ou íntimos de terceiros, abusivamente obtidos. A par, foi referida a ocorrência de crimes contra a honra por via de *blogs* ou por meio de correio eletrónico.
Apurou-se também terem alguma expressão os casos de acessos ilegítimos a sistemas informáticos - quer a contas bancárias, quer a contas de correio eletrónico, sobretudo em contextos de relações pessoais que cessaram (ex-cônjuges ou ex-namorados).
Foram ainda assinalados um ou outro caso de *grooming*, ou outros tipos de abuso sexual de crianças. Por último, quanto aos crimes na área da pornografia infantil, têm também vindo a crescer.

9. A criminalidade na área da pornografia infantil foi objeto de um relatório do Gabinete Cibercrime que especificamente incidiu sobre esta realidade. Junta-se agora como Anexo 11.
Desse relatório resultava, em suma, que no contexto da cooperação desenvolvida com o *National Center For Missing & Exploited Children* (NCMEC), dos Estados Unidos da América, no segundo semestre de 2013, a Procuradoria-Geral da República, por via do Gabinete Cibercrime, estabeleceu um protocolo informal de cooperação com aquela organização não-governamental tutelada pelo Congresso dos Estados Unidos. Esta, dedica-se à recolha e transmissão às autoridades judiciais de informação que encontre disponível sobre crianças desaparecidas ou exploradas sexualmente – em especial, a sua atuação tem incidido sobre eventuais utilizadores de *sites* na Internet onde se divulgue pornografia infantil. 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 atos sexuais) com ligação a Portugal. Estas situações vinham sendo, no passado, transmitidas a autoridades portuguesas.
Sobre esta matéria foi emitida a Diretiva nº 4/2013 da Procuradoria-Geral da República, que atribuiu ao DCIAP competência para, de forma centralizada, 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 da Direção do DCIAP, que implementou, no concreto, aquela circular. Em consequência destas determinações, o NCMEC, por via de autoridades norte-americanas, passou a remeter diretamente ao DCIAP as suas participações, contendo imagens de pornografia infantil. O DCIAP passou a realizar as necessárias diligências à investigação das mesmas: identifica os utilizadores de Internet que sejam suspeitos e, uma vez identificados estes, encaminha os inquéritos para a comarca da respetiva residência.
Desde o início deste procedimento (em outubro de 2013) e até junho de 2016, o DCIAP recebeu 2880 participações vindas do NCMEC. Delas, 1350 deram origem à abertura de inquérito, dos quais foram remetidos para as comarcas 601. No DCIAP foram arquivados 634 inquéritos, após a

realização de diligências que demonstraram não ser tecnicamente possível reunir prova que permitisse apurar a identidade dos suspeitos. Até julho de 2016 foram proferidas, nestes inquéritos, 20 acusações, número esse que chegaria a 28 no fim do ano de 2016. Quanto a 10 destas acusações, foram, entretanto, realizados os respetivos julgamentos e proferidas sentenças de condenação. Sublinha-se que em nenhum dos julgamentos realizados houve decisão de absolvição.

A instauração destes processos deu origem a um grande número de buscas domiciliárias, de constituições de arguidos e de aplicação de medidas de coação – nelas se incluindo medidas de prisão preventiva. Alguns destes processos tiveram grande repercussão social, com bastante eco na comunicação social. Afigura-se que esta difusão, pelos *media*, de intervenções policiais e judiciárias a este respeito, teve a virtualidade de criar efeito de prevenção geral, profilático, que ultrapassará em muito o mero efeito processual endógeno. Aponta-se este resultado como muito positivo.

Aduz-se ainda que apesar da aparente desproporção entre o número de inquéritos e o número de acusações, este balanço é igualmente muito positivo. Na verdade, a investigação neste tipo de inquéritos reveste-se de grande dificuldade e complexidade, costumando ser demorada. O respetivo resultado tarda sempre em ser atingido.

Por outro lado, todos estes processos supõem a realização de perícia informática, a qual é quase sempre um imprescindível meio probatório. É sabido que as perícias, em regra a cargo da Polícia Judiciária, estão a ser realizadas – algo que decorre da carência de recursos humanos sinalizada pela própria PJ - com um enormíssima demora e atraso, que rondará os três anos.

Tendo todo este procedimento, de abordagem inicial concentrada no DCIAP, sido introduzido no terceiro trimestre de 2013 é, pois, natural que seja ainda pouco expressivo o número de inquéritos em que tenha sido deduzida acusação.

Até 2013, as eventuais notícias de crimes eram comunicadas e dissipadas pelas várias comarcas, onde se diluíam na massa dos restantes inquéritos, sem que se atendesse a que, neste caso, uma intervenção rápida do Ministério Público, sobretudo na fase inicial, é crucial para o sucesso da investigação.

A intervenção do DCIAP foi, assim, um elemento diferenciador da eficácia da intervenção do Ministério Público. Pode, pois, concluir-se que o estabelecimento deste mecanismo, tem permitido a investigação de processos que anteriormente não tinha sido possível investigar e que, como tal, muitas vezes acabavam arquivados. Este mecanismo procedimental veio alterar a situação e os resultados são já muito visíveis. Na fase processual dependente do Ministério Público foram deduzidas muitas acusações e determinado um número significativo de suspensões provisórias do processo. Quanto à fase de julgamento, começaram a surgir as primeiras condenações por crimes desta natureza.

Tendo em conta o tipo específico de criminalidade em causa (difusão de pornografia infantil) e a dificuldade de investigação da mesma, estas observações afiguram-se muitíssimo satisfatórias.

10. Noutra vertente, já em meados de 2016, anotou-se o surgimento, com tendência crescente, de casos de *ransomware*. Estas situações, que podem ser criminalmente enquadradas no dano informático ou na sabotagem informática traduzem-se, na perspetiva da vítima, no recebimento de uma mensagem de correio eletrónico, infetada com *malware* que, uma vez aberto, encripta os

dados do computador. Depois, surge no monitor uma mensagem a informar que os dados apenas serão libertados mediante um pagamento de uma quantia monetária.
Muitas destas queixas que foram surgindo, como se disse de forma crescente, foram apresentadas por empresas que, tendo *backups* dos seus dados, pretendiam reportar a situação para poderem vir a justificar (por exemplo, por razões societárias ou fiscais) a perda de documentos de gestão.

11. No que concerne a questões práticas processuais, de investigação, foi referido haver grande facilidade de contacto com os operadores de comunicações, funcionando globalmente bem o procedimento de pedido de informações aos mesmos. Foi dito que, em geral, os pedidos são respondidos de forma expedita e eficaz. Num ou noutro caso foram anotadas demoras. Noutras situações, de urgência, foi referido que houve respostas que vieram de imediato.
Com recorrência foi referido que o período legal e habitual de conservação de dados de tráfego, pelos operadores (que é de 6 meses), é curto e esta limitação prejudica o sucesso de muitas investigações. Num ou noutro caso foi dito que foi possível obter informação para lá dos seis meses por via da obtenção de informação bancária sobre o carregamento de cartões telefónicos.
De um modo generalizado, foi dada conta de imensa demora na realização de perícias informáticas, pela Polícia Judiciária. Esta demora tem prejudicado de forma excecionalmente grave as investigações.
Finalmente, anotou-se que, em bom número das comarcas, a criminalidade relacionada com a Internet já tem sido distribuída de forma concentrada a um ou mais magistrados, tirando-se assim proveito de alguma especialização que vai já surgindo.

C. A ATIVIDADE GERAL DO GABINETE

12. A explosão dos casos de cibercriminalidade e, sobretudo, de inquéritos em que se requere a obtenção de prova eletrónica, abriram uma enorme latitude de questões, sobretudo pela sua componente técnica, nem sempre fácil de enquadrar nas leis vigentes.
Tem sido propósito do Gabinete Cibercrime conciliar a diversidade de interpretações, atuações e entendimentos, de forma a que casos semelhantes não tenham soluções concretas diferentes. A vertente de coordenação empreendida pelo Gabinete visa assim, desde logo, que o entendimento dos diferentes magistrados possa levar a que os mesmos factos com relevância criminal sejam enquadrados juridicamente de forma coordenada e consistente pelo Ministério Público. Por outro lado, quanto ao processo de obtenção de prova em suporte digital, nos processos dirigidos pelo Ministério Público, visa-se que esta recolha seja efetuada de forma coerente.

C.1. NOTAS PRÁTICAS

13. Foi nesse contexto que surgiu a necessidade de emissão, pelo Gabinete, de notas de boas práticas que, embora não vinculativas e desprovidas de características de instrução hierárquica, possam ser vistas como auxiliares dos magistrados, na resolução de questões controvertidas concretas. No decurso do período de tempo a que se refere este relatório, foram emitidas quatro notas práticas.

Assim, a 30 de dezembro de 2015, foi emitida a Nota Prática nº 7/2015, respeitante à retenção de dados de tráfego e à Lei nº 32/2008, de 17 de julho. Esta Nota Prática pretendeu dar conta da discussão jurídica, em Portugal e na Europa, a propósito da obrigação de os operadores de comunicações procederem à retenção de dados. Tal questão tinha sido suscitada pelo Acórdão do Tribunal de Justiça da União Europeia de 8 de abril de 2014 que, no caso específico português veio questionar a continuação em vigor da Lei nº 32/2008, de 17 de julho.

Por outro lado, a 17 de fevereiro de 2016 foi emitida a Nota Prática nº8/2016, referente ao pedido de dados a operadores de comunicações. Com esta nota prática pretenderam descrever-se as informações guardadas por operadores de comunicações (telefónicas e Internet), que possam vir a ser usadas em investigações criminais, bem como referenciar os fundamentos jurídicos que delimitam os pedidos dessas informações.

Finalmente, a 21 de setembro de 2016 foram emitidas a Nota Prática nº 9/2016 e a Nota Prática nº 10/2016, ambas referenciando jurisprudência de tribunais superiores – a primeira delas incidindo sobre crimes informáticos e crimes cometidos por via de sistemas de computadores; a segunda, sobre prova digital.

Todas as notas práticas foram divulgadas no SIMP[1] e no Portal do Ministério Público[2]. Juntam-se como Anexo 1, Anexo 2, Anexo 49 e Anexo 50.

C.2. COOPERAÇÃO COM FORNECEDORES DE SERVIÇO NA INTERNET

14. Em relatórios anteriores do Gabinete Cibercrime tem-se sublinhado a importância de, na investigação criminal atual, se recorrer cada vez mais a elementos de prova em posse de fornecedores de serviço Internet. Esta necessidade impôs que se dialogasse com entidades dessa natureza. Como em anteriores relatórios se referiu, no segundo semestre do ano de 2013 foram abordados os operadores Microsoft, Google e Facebook, com o propósito, que foi aceite, de estabelecer critérios de entendimento e cooperação. Em resultado dessa abordagem, passou a ser possível formular diretamente pedidos àqueles fornecedores de serviços norte-americanos, sem necessidade de recurso aos canais da cooperação internacional. Este mecanismo veio a revelar-se de grande eficácia prática, por facilitar a obtenção de informação essencial à investigação criminal de forma expedita, sem necessidade das complexidades burocráticas dos mecanismos do auxílio judiciário mútuo. Por outro lado, criou-se a possibilidade de obter essa mesma informação em situações em que, anteriormente, tal informação não era, na prática, de todo, possível de obter.

Genericamente, deste diálogo resultou um enorme incremento dos pedidos de cooperação formulados, pelas entidades portuguesas responsáveis pela investigação criminal (*máxime*, o Ministério Público) aos operadores.

Embora neste procedimento se anotassem melhorias a introduzir, sobretudo ao nível da eficácia, este grande incremento teve, naturalmente, repercussão na eficácia de obtenção de prova. O resultado destes pedidos tem sido divulgado pelos fornecedores de serviço em causa.[3]

[1] O SIMP é o Sistema de Informação do Ministério Público.

[2] Todas as notas práticas emitidas pelo Gabinete Cibercrime estão presentemente disponíveis no micro-portal do Cibercrime, no Portal do Ministério Público, em http://cibercrime.ministeriopublico.pt/notas-praticas.

[3] Todos estes fornecedores de serviço divulgam relatórios a que chamam de transparência. Estão disponíveis *online*, tendo sido divulgados dados até ao segundo semestre de 2015. Vejam-se os relatórios Facebook em https://govtrequests.facebook.com/, os relatórios Google em https://www.google.com/transparencyreport/ e os relatórios Microsoft em https://www.microsoft.com/about/csr/transparencyhub/.

15. Na tabela que segue, descrevem-se os pedidos formulados por autoridades portuguesas à Facebook, entre 2013 e 2016 (apenas estão disponíveis dados até ao primeiro semestre).

	Jul – Dez 2013	Jan – Jun 2014	Jul – Dez 2014	Jan – Jun 2015	Jul – Dez 2015	Jan – Jun de 2016
Número total de pedidos	**148**	**354**	**305**	**488**	**545**	**782**
Percentagem de pedidos em que foram fornecidos dados	**25**%	**40,40**%	**34,75%**	**36,07%**	**30,09%**	**48,67%**

Por sua vez, na tabela que segue, descrevem-se os pedidos formulados por autoridades portuguesas à Microsoft, no período de 2013 a 2016 (apenas estão disponíveis dados até ao primeiro semestre).

	Jul – Dez 2013	Jan – Jun 2014	Jul – Dez 2014	Jan – Jun 2015	Jul – Dez 2015	Jan – Jun de 2016
Número total de pedidos	**372**	**511**	**386**	**611**	**445**	**522**
Percentagem de pedidos recusados	**1,34**%	**1,17**%	**3,1%**	**9,66%**	**15,73%**	**14,94%**

Por último, na tabela que segue, descrevem-se os pedidos formulados por autoridades portuguesas à Google, no período de 2013 a 2016 (apenas estão disponíveis dados até ao primeiro semestre).

	Jul – Dez 2013	Jan – Jun 2014	Jul – Dez 2014	Jan – Jun 2015	Jul – Dez 2015	Jan – Jun de 2016
Número total de pedidos	**283**	**338**	**309**	**550**	**587**	**731**
Percentagem de pedidos em que foram fornecidos dados	**45**%	**53**%	**54%**	**54%**	**58%**	**63%**

16. De todas as tabelas resulta um aumento consistente dos pedidos de autoridades portuguesas a ISP dos Estados Unidos. No caso da Microsoft, anota-se um ajustamento do crescimento.

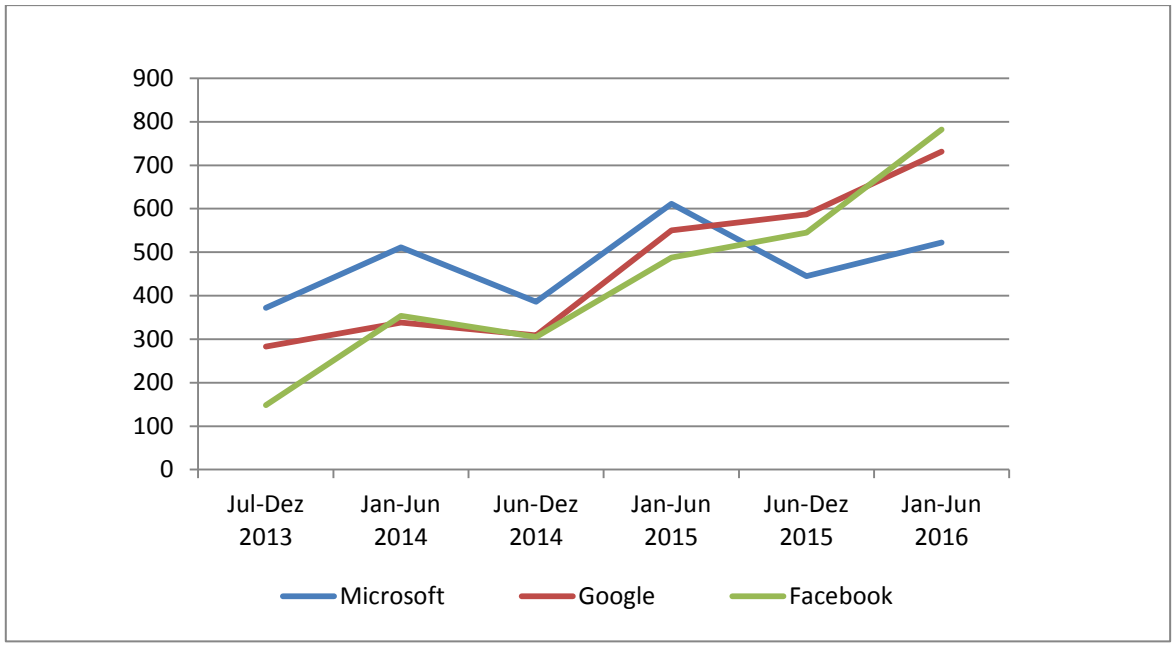
A este propósito, anota-se que, a partir de setembro de 2015 se deu inicio a um processo de comunicação sistemático, pela Microsoft ao Gabinete Cibercrime, de pedidos erroneamente formulados. Com efeito, apurou-se que esta entidade, porventura por estar legalmente representada em Lisboa, por um escritório de advogados, e ser assim mais facilmente contactável, vinha sendo destinatária de inúmeros pedidos (do Ministério Público, mas também diretamente de órgãos de polícia criminal), que visavam a obtenção de informações de outras

entidades. Portanto, recebia pedidos que lhe eram dirigidos de forma manifestamente errada. De forma sistemática, veio a Microsoft a remeter ao Gabinete Cibercrime todos estes pedidos que tivessem origem no Ministério Público. E também de forma sistemática, o Gabinete Cibercrime contactou, por telefone, todos os magistrados signatários, tendo em vista clarificar junto dos mesmos o método usado no pedido. Informalmente a Microsoft veio mais recentemente a referir que, progressivamente, tem vindo a receber menos pedidos grosseiramente mal endereçados, atribuindo-se este progresso à divulgação que tem havido, do modo correto de formular estas solicitações.

Estas razões explicam ter havido um ajustamento no crescimento dos pedidos à Microsoft – sem que, clarifique-se, possa anotar-se uma verdadeira quebra.

Por outro lado, anotou-se uma clara e consistente oscilação entre os pedidos formulados entre os dois semestres do ano: no primeiro semestre de todos os anos foram formulados mais pedidos do que no segundo. Esta nuance tem também fácil e clara explicação na quebra que ocorre durante os períodos de férias judiciais, sobretudo no verão, mas também durante parte do mês de dezembro.

Tudo o que fica dito resulta graficamente ilustrado no quadro de síntese que segue.



17. Porém, como acima se referiu, anotou-se haver, a este propósito, margem para melhorar a eficácia nos procedimentos, uma vez que, nalguns casos, a percentagem de pedidos que não têm resposta satisfatória dos operadores é significativa. Quanto à Google, a eficácia tem sido crescente, de semestre para semestre. No que respeita à Microsoft, a eficácia mantém-se em níveis muito bons. Já quanto aos pedidos à Facebook, que têm sofrido um grande incremento (sendo, sobretudo, formulados por magistrados de secções não especializadas), esta operadora não tem fornecido dados em muitos dos pedidos que lhe são dirigidos.

Foi abordada a *Facebook Ireland*, interlocutora do Gabinete Cibercrime, que esclareceu que esses casos, de resposta recusando o fornecimento de informação, correspondem em geral a casos em que os pedidos são formulados de forma errada ou deficiente. A *Facebook Ireland* identificou mesmo as causas mais importantes de recusa.

Indo ao encontro desta questão, entre 4 e 15 de janeiro de 2016, procedeu-se a uma campanha de divulgação diária, no SIMP, de regras práticas respeitantes aos pedidos ao Facebook. Por outro lado, incluiu-se esta temática nas sessões de coordenação realizadas nas comarcas, a que abaixo melhor vai aludir-se. Talvez como resultado destas iniciativas específicas, a eficácia dos pedidos formulados, que era de 30,09% no final de 2015, passou a 48,67% no fim do primeiro semestre de 2016.
Quanto à Microsoft, como acima se referiu (e também parcialmente quanto à Google), criaram-se as rotinas de comunicação para o Gabinete Cibercrime de pedidos originados no Ministério Público, formulados de forma errada ou deficiente, como já se descreveu acima. Estas rotinas permitiram ir ao encontro dos problemas do caso concreto, abordando-se especificamente os magistrados signatários dos pedidos, tendo em vista melhorar práticas futuras. Nestas circunstâncias foram assim, no período a que se refere este relatório, abordados trinta e sete magistrados do Ministério Público, por contacto telefónico.

C.3. PROTOCOLOS COM INSTITUIÇÕES UNIVERSITÁRIAS PÚBLICAS

18. Em investigação criminal, é pacífico afirmar-se que, cada vez mais, se torna necessário recorrer a perícias informáticas. Esta necessidade crescente extravasou os limites da estrita cibercriminalidade e estendeu-se a processos respeitantes a crimes comuns, em virtude da igualmente crescente prova disponibilizada em suportes digitais.
Não obstante, tem sido manifestado com recorrência em reuniões com magistrados, haver grandes dificuldades na realização de perícias informáticas no decurso dos inquéritos. Tais dificuldades traduzem-se, sobretudo, na enorme demora na realização dessas perícias, mesmo em casos mais simples. Magistrados têm referido que tem sido habitual que a Unidade de Telecomunicações e Informática, departamento especializado da Polícia Judiciária na realização deste tipo de perícias, tenha perícias em espera para serem realizadas durante cerca de três anos, o que provoca um atraso muito considerável nas investigações.

19. Foi neste contexto que, desde julho de 2013, se explorou uma possibilidade alternativa de realização de perícias informáticas, por via da celebração de protocolos de cooperação com instituições universitárias. Por estes protocolos, as mesmas comprometeram-se a elaborar e manter listas de peritos informáticos (incluindo, nomeadamente, docentes, investigadores, bolseiros e alunos de mestrado ou de doutoramento), que facilitem a respetiva indicação, em processos judiciais concretos, a solicitação de magistrados do Ministério Público. Esta indicação não tem suposto qualquer encargo financeiro para a Procuradoria-Geral da República, já que o pagamento dos honorários devidos pelos serviços dos peritos é efetuado, no próprio processo, de acordo com as regras e a tabela das custas processuais.
Foram assim celebrados protocolos com o Instituto Politécnico de Beja (em 2013) com a Universidade do Porto e com a Universidade de Aveiro (em 2014) e com o Instituto Politécnico e Leiria (em 2015). Prosseguem conversações com outras instituições universitárias, tendo em vista a celebração de novos protocolos, de idêntica natureza.

20. No final do ano de 2015 foi feito um balanço desta nova possibilidade operacional, tendo em vista avaliar o resultado prático da implementação dos protocolos com as universidades que visam a indicação de peritos informáticos ao Ministério Público. Na análise, tomaram-se em

consideração os dados em posse do Gabinete Cibercrime, resultantes da intervenção intermediária que tem entre os magistrados e as universidades. Não foram consultados os processos em que foram indicados peritos apesar de, quando necessário, ter sido solicitada informação complementar a estes últimos.
Procedeu-se à análise do tempo utilizado para a realização de perícias, mas também para o lapso temporal de indicação dos peritos pelas universidades, o qual tem igualmente alguma relevância na marcha dos processos e merecer consideração, tendo em vista a melhoria dos procedimentos.
Como assunção geral, resultou desta avaliação que este mecanismo permitiu, em concretos processos, a realização de um número já relevante de perícias de forma muito mais expedita que a usada na generalidade dos restantes casos. Com efeito, as quase três dezenas de perícias foram realizadas, em média, em 153 dias, equivalentes a 5 meses (recorda-se que na Polícia Judiciária tem ocorrido as perícias terem que aguardar por mais do que 3 anos, para serem realizadas). Porém, em vários dos casos, as perícias foram concluídas num prazo muito mais curto - um dos casos do Instituto Politécnico de Leiria foi concluído em 26 dias, no Instituto Politécnico de Beja concluíram-se várias das perícias entre 30 e 40 dias e na Universidade de Aveiro concluiu-se uma das perícias em 37 dias.
Por outro lado, quanto à qualidade das perícias, embora não tenha sido feita uma avaliação substancial do teor de cada relatório, os sinais indicadores emitidos por magistrados que ordenaram essas mesmas perícias foram extremamente positivos.

21. A solicitação de peritos, neste âmbito, tem sido feita por via Gabinete Cibercrime da Procuradoria-Geral da República que, por sua vez, solicita a indicação de peritos junto das instituições universitárias. Optou-se por este modelo, de canalizar todos os pedidos por via do Gabinete Cibercrime, que os encaminha para as universidades, de forma a permitir monitorizar-se e garantir a eficácia do sistema. Este procedimento, que abre espaço de interação entre os magistrados e o Gabinete Cibercrime, tem sido igualmente útil nalguns casos, para permitir aos magistrados fixar com mais nitidez o propósito das perícias que solicitam.
Como se adiantou, os dados que seguem resultam da consulta dos registos do Gabinete Cibercrime e ainda, no que respeita às datas das conclusões das perícias, de informação fornecida pelas instituições universitárias e, na falta dela, de consulta direta ao perito nomeado, em cada concreto processo.

22. No decurso dos anos de 2014 e 2015 foram solicitados ao Gabinete Cibercrime, e por este indicados às comarcas, 29 peritos informáticos. Do conjunto destas perícias, apenas estavam por realizar, no fim de fevereiro de 2016, data da realização de levantamento referido, 6 delas. Porém, importa considerar que um dos casos estava pendente por ter sido solicitado trabalho pericial adicional. Quanto a um outro, após a solicitação do perito e a sua indicação ao tribunal, nada mais sucedeu, uma vez que o respetivo magistrado titular optou por não ordenar a perícia. Num terceiro caso, a entrega do material, que tinha antes sido confiado à PJ, demorou mais de um ano e só ocorreu já em 2016. A perícia viria a ser concluída em março de 2016. Nos três restantes casos de 2015 ainda sem conclusão naquela data, as indicações de peritos aos magistrados tinham ocorrido a 10 de novembro e a 24 de dezembro de 2015 (neste caso, em duas situações), respetivamente.

Os dados que se apresentam de seguida respeitam aos prazos de indicação de perito pelo Gabinete Cibercrime e de conclusão da perícia.
Note-se que a avaliação feita a este propósito, quanto a 2014, incidia sobre um universo muitíssimo mais limitado de casos e, assim, foi possível levar em consideração o efetivo prazo da perícia (desde o momento da tomada do compromisso do perito até à efetiva entrega do relatório pericial).
Por razões objetivas e de facilidade de análise, optou-se por uma mudança de metodologia e passou-se a tomar em consideração o lapso de tempo decorrido entre o momento de indicação do perito ao processo e a data da perícia. O que significa que, os prazos que abaixo se descrevem são, necessariamente, mais extensos do que os que efetivamente se verificaram. Aliás, assinala-se que a interação com os peritos permitiu aperceber que, nalguns casos, decorreu algum tempo entre a indicação do perito ao processo e o efetivo início da perícia. Este lapso de tempo fica a dever-se, em geral, a aspetos processuais da realização de diligências, em regra, relacionados com a notificação do próprio perito ou com a tomada do seu termo de compromisso.

23. No decurso de 2015, o Instituto Politécnico de Beja foi solicitado a indicar peritos em 6 casos. Em 2014 tinham-lhe sido feitas oito solicitações. Das perícias de 2014, 3 transitaram para 2015. Das solicitações de 2015, foram cumpridas 3, transitando outras 3 para 2016. A perícia mais demorada foi realizada em 255 dias e a mais expedita foi concluída em 34 dias. Em termos médios, o tempo necessário para a realização de uma perícia foi de 100 dias.
A indicação de peritos, pelo Instituto Politécnico de Beja ao Gabinete Cibercrime, foi feita num lapso de tempo entre 1 e 37 dias. Anote-se que esta última foi a designação do primeiro perito, logo aquando da entrada em vigor do protocolo de cooperação. Com exceção desta, a designação mais demorada foi feita 28 dias após a respetiva solicitação. Em termos médios, os peritos foram designados 18 dias após terem sido solicitados.

24. O protocolo com o Instituto Politécnico de Leiria foi celebrado em abril de 2015. Após esta data, esta instituição foi solicitada a indicar peritos ao Ministério Público em três casos. De entre eles, a perícia mais demorada foi realizada em 266 dias e a mais expedita foi concluída em 26 dias. Sublinha-se que não provocou estranheza que a primeira destas perícias fosse mais demorada, por ter sido a primeira a ser solicitada ao Instituto Politécnico de Leiria. Em termos médios, o tempo necessário para a realização de perícias foi de 146 dias.
A indicação de peritos pelo Instituto Politécnico de Leiria ao Gabinete Cibercrime foi feita num lapso de tempo entre 1 e 7 dias. Em termos médios, os peritos foram designados 4 dias após terem sido solicitados.

25. No que respeita aos pedidos de indicação de peritos à Universidade de Aveiro, em 2014 tinham-lhe sido feitos dois pedidos. Em 2015, foram solicitadas mais duas indicações de perito. Em todos os casos, os relatórios periciais foram efetivamente realizados neste ano. A perícia mais demorada foi realizada em 306 dias e a mais expedita foi concluída em 37 dias. Em termos médios, o tempo necessário para a realização de perícias foi de 150 dias.

A indicação de peritos pela Universidade de Aveiro ao Gabinete Cibercrime foi feita num lapso de tempo entre 10 e 49 dias. Em termos médios, os peritos foram designados 26 dias após terem sido solicitados

26. Quanto aos pedidos de indicação de peritos à Universidade do Porto, em 2014 foram remetidos quatro. Nenhuma das perícias chegou a ser realizada nesse ano, transitando para o seguinte. Em 2015, foram solicitadas mais quatro indicações de perito. Em apenas um dos casos não tinha sido possível, à data da avaliação (março de 2016) concluir a perícia (sendo certo que a respetiva indicação de perito ao tribunal ocorreu apenas a 10 de novembro de 2015). A perícia mais demorada foi realizada em 354 dias e a mais expedita foi concluída em 75 dias. Em termos médios, o tempo necessário para a realização de uma perícia foi de 217 dias.
A indicação de peritos pela Universidade do Porto ao Gabinete Cibercrime foi feita num lapso de tempo entre 2 e 47 dias. Em termos médios, os peritos foram designados 24 dias após terem sido solicitados.

27. Em 2015 confirmou-se uma indicação que se apercebera em 2014: a cooperação com as universidades abriu a possibilidade de realizar perícias na área informática num tempo muitíssimo mais curto que aquele utilizado pela Polícia Judiciária para o mesmo efeito. O universo de casos concretos é ainda limitado para poder aferir-se da possível repercussão destas novas possibilidades operacionais na eficácia e celeridade na investigação criminal. Todavia, os sinais otimistas já registados em 2014 reforçaram-se fortemente no período a que respeita este relatório, sem prejuízo de se divisarem também melhorias a introduzir, em mais alargada análise futura.

28. Da informação que acima se deixou resulta que a designação de peritos pelas instituições universitárias foi feita no prazo mínimo de 1 dia (Instituto Politécnico de Beja e Instituto Politécnico de Leiria) e máximo de 49 dias (Universidade de Aveiro) após a respetiva solicitação. Casos houve também em que a designação foi feita 2 dias depois da solicitação (Universidade do Porto). Em termos médios, as universidades indicaram os peritos ao Gabinete Cibercrime 18 dias após a solicitação.
O Instituto Politécnico de Leiria destaca-se, por ter indicado todos os seus peritos num lapso muito curto de tempo – em média, em 4 dias (sendo o caso mais demorado indicado em 7 dias). Quanto às restantes instituições, afigura-se haver possibilidade de tornar mais expedito este processo, mediante sensibilização das universidades a este respeito.

29. Por outro lado, da informação que antecede resulta também que para a realização das perícias foram necessários entre 26 dias (um dos casos do Instituto Politécnico de Leiria) e 354 dias (um dos casos da Universidade do Porto). Anota-se que este último caso, de duração excecional, no contexto, respeitava a um processo em que se investigava o chamado *card sharing*, supondo a análise de centenas de dispositivos e suportes magnéticos). No entanto, além do Instituto Politécnico de Leiria, peritos de outras instituições universitárias puderam também concluir as suas perícias em prazos muitos curtos (do Instituto Politécnico de Beja concluíram-se várias das perícias que lhe foram confiadas entre 30 e 40 dias, da Universidade de Aveiro concluiu-se uma das perícias em 37 dias).

Em termos médios, as perícias foram realizadas em 153 dias, mais ou menos equivalentes a 5 meses. A este propósito, merece destaque o Instituto Politécnico de Beja que, em média, tem concluído as perícias em 100 dias, equivalentes a pouco mais que três meses.
Não pode deixar de dizer-se, a este respeito, que cada perícia tem naturalmente as suas especificidades. Algumas delas incidiram sobre uma grande quantidade de suportes digitais. Noutros casos (e em mais que uma situação assim foi reportado ao Gabinete Cibercrime), foi necessária a realização, para que a perícia pudesse ser prosseguida, de diligências de inquérito. Naturalmente que estas perícias sofreram um maior atraso.

30. Como já se deixou dito, não foi feita uma análise qualitativa dos relatórios periciais. Não obstante, aquando da indicação dos peritos, de forma rotineira foi solicitado que fosse providenciada informação de sequência. Nalguns casos, tal informação foi feita chegar ao Gabinete Cibercrime pelos magistrados.
Assim aconteceu num processo da comarca de Évora, em que a magistrada titular informou que "*a perícia foi realizada prontamente (foram necessários uns pequenos esclarecimentos e aditamento ao relatório pericial inicial, pelo que demorou um pouco mais, e eram muitos documentos) e correu tudo muito bem, e o senhor perito foi muito prestável e disponível. Já deduzi acusação e parece-me que a prova pericial é inabalável*".
Da mesma forma, num processo da comarca do Porto, a magistrada titular referiu que "*a perícia informática efetuada (…) com indicação de perito informático por parte do Gabinete Cibercrime da Procuradoria-Geral da República, decorreu muito bem e com grande celeridade (após tomada de compromisso a perícia foi concluída em cerca de 30 dias)*".
Ainda num processo à data da comarca Alentejo Litoral, a magistrada titular informou que "*o computador foi enviado ao perito por ofício de 4 de março e ele já tinha o relatório pronto no final de abril. Analisei-o com o perito e fiquei muito satisfeita com o resultado, a rapidez e conteúdo do relatório (claro e sucinto).*"
Por último, no âmbito dum inquérito da comarca de Lisboa, pela magistrada titular foi referido que, "*após ter estado parada na PJ entre outubro de 2013 e março de 2015, a perícia naquele processo veio a ser realizada, entre junho de 2015 e novembro do mesmo ano, sendo, porém, de referir que, por sugestão do perito, foram, entretanto, nesse período de tempo, realizadas diligências, que vieram a ser levadas em conta no relatório pericial*".
Não chegou ao Gabinete Cibercrime nota de qualquer reparo que os peritos ou as perícias pudessem merecer.

31. Quanto ao ano de 2016, foi solicitada ao Gabinete Cibercrime a indicação de peritos para 23 processos – recorda-se que em 2014 o tinha sido em 14 processos e no decurso de 2015, em 16 processos. Em dois deles, após contacto com o magistrado, acabou por ser desnecessária a indicação de perito e num outro foram solicitados peritos a duas instituições universitárias.
7 dos pedidos foram encaminhados para o Instituto Politécnico de Beja e 8 para o Instituto Politécnico de Leiria. Para a Universidade do Porto foram encaminhados 4 pedidos e para a Universidade de Aveiro foram encaminhados 2. Quanto a estas últimas, encaminharam-se menos pedidos por, a partir do meio do ano de 2016, estas universidades terem informado que, por contingências conjunturais, alheias a este processo, terem passado a ter menos facilidade em satisfazer tais pedidos.

C.4. PLATAFORMAS INFORMACIONAIS

32. Em cumprimento de um dos seus objetivos, o Gabinete Cibercrime deu continuidade à manutenção regular e atualizada da área temática do SIMP dedicada ao Cibercrime – a qual existe desde 13 de março de 2012. Ao longo do período a que se refere este relatório, estruturalmente, o SIMP manteve a mesma matriz que vem tendo desde 2012.
Assim, continua a incluir secções de apoio funcional (referente à Rede de Pontos de Contacto, formulários de solicitação de dados a operadores de comunicações e de peritos, ferramentas e recursos operacionais) e secções de apoio quanto a temáticas substantivas de cibercrime (Notas Práticas, livros e outro material de referência, entre outros). Neste contexto, foi introduzida uma nova secção, contendo os chamados "Alertas Cibercrime". Tal secção veio incorporando, ao longo do período a que se refere este relatório, documentos de alerta, dirigidos aos magistrados na dupla vertente de potenciais vítimas e também de investigadores criminais. Nalguns casos, estes alertas visaram também reunir indícios de práticas criminosas, que poderão potencialmente vir a ser utilizados por colegas em investigações criminais concretas.
Manteve-se ativa a coluna central, da Divulgação. Nesta secção, foram introduzidas, no período a que se refere este relatório, 116 novas entradas. Foram também frequentemente introduzidas atualizações nas secções de Comunicação Social (35 novas entradas, ao longo do período a que se refere o relatório) e de Jurisprudência (foram anotadas, neste período, 31 novas decisões jurisprudenciais achadas pertinentes na área do cibercrime e da prova digital).

33. Por outro lado, foi sendo mantida *online* e atualizada uma página *web*, em fonte aberta, com chamada na página *web* da Procuradoria-Geral da República (www.pgr.pt) e, depois, no Portal do Ministério Público. http://www.ministeriopublico.pt/.
A partir de 23 de fevereiro de 2016 passou a estar disponível, com chamada no Portal do Ministério Público, o novo micro portal Cibercrime (http://cibercrime.ministeriopublico.pt). Procurou-se que este novo micro portal fosse mais funcional e orientado para o utilizador que a antiga página. Para além da divulgação de informação sobre a área da cibercriminalidade e sobre a atividade desenvolvida pelo Gabinete Cibercrime, passou a disponibilizar-se uma funcionalidade de recebimento de denúncias, remetidas para a caixa de correio do Gabinete Cibercrime. Dela se dará informação mais abaixo.

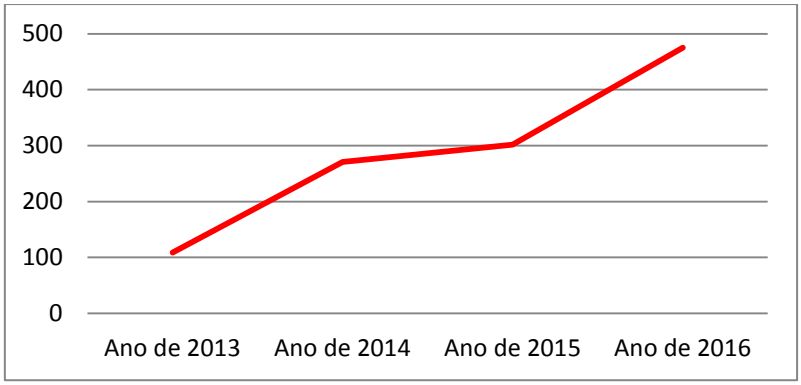
34. Da mesma forma, foi mantido disponível o endereço eletrónico do Gabinete (cibercrime@pgr.pt), o qual está divulgado no micro portal.
Desde a sua disponibilização, em 2012, este endereço de correio eletrónico revelou-se como uma importante via de comunicação da comunidade em geral com o Gabinete Cibercrime. Em 2015 e 2016, tal como acontecera em anos anteriores, esta caixa de correio continuou a receber um grande número de mensagens de correio eletrónico, a relatar crimes, métodos criminais e incidentes informáticos, entre outras. A todas[4] foi dada resposta. Como melhor resulta na tabela que segue (que inclui dados desde 2013), no período compreendido entre setembro de 2015 e agosto de 2016, foram movimentadas por este endereço de correio eletrónico 414 mensagens (das quais, 108 entre 1 de setembro e 31 de dezembro de 2015 e 306 entre 1 de janeiro e 31 de

[4] Com natural exceção de mensagens de *spam* e de mensagens que canalizassem queixas, remetidas a múltiplas instituições, sem que as mesmas tivessem relação com a atividade do Gabinete Cibercrime ou do Ministério Público.

agosto de 2016). No restante período de 2016 foram movimentadas 119 mensagens. Ou seja, no decurso do ano de 2016, foram movimentadas 455 mensagens, quando em 2015 tinham sido 302 e em 2014 apenas 271. Tudo, como melhor resulta da tabela que segue.

2013	2014		2015		2016	
(apenas foram consideradas as mensagens a partir de julho)	até 31 de agosto	após 1 de setembro	até 31 de agosto	após 1 de setembro	até 31 de agosto	após 1 de setembro
109	195	76	194	108	306	149
109	**271**		**302**		**455**	

35. Estes dados mostram haver um progressivo e constante incremento no movimento de mensagens registado por via deste endereço. No gráfico que segue incluem-se dados referentes aos anos de anos de 2013 a 2016



36. Esta conta de correio eletrónico (cibercrime@pgr.pt) confirmou-se também como uma importantíssima forma de comunicar com magistrados de todo o país. Desde que se disponibilizou este endereço, com grande regularidade, magistrados recorrem ao Gabinete Cibercrime por esta via, para colocar questões, sobretudo técnicas, de natureza processual, a propósito de dúvidas que se lhe suscitam em processos concretos. Assim ocorreu, também no período a que se refere este relatório. Como aconteceu com as restantes mensagens a todas estas foi também dada resposta, embora por vezes o tenha sido por telefone, tendo em vista facilitar a comunicação e permitir diálogo.

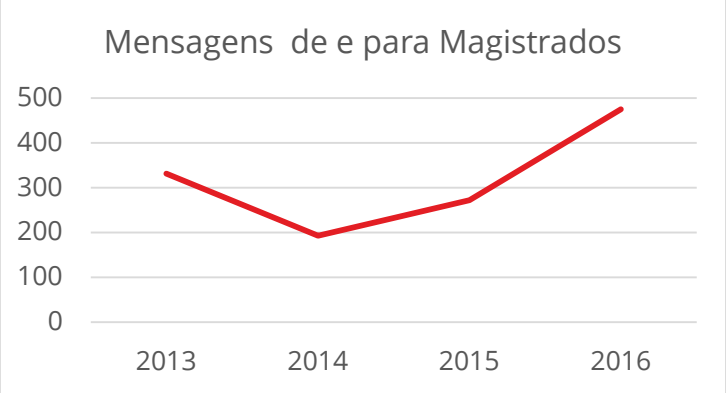
37. Na tabela que segue descrevem-se as mensagens de colegas para o Gabinete Cibercrime e as respostas às mesmas, no período de 2013 a 2016. Estas mensagens acrescem às que acima se referiram, da comunidade em geral.

2013		2014		2015		2016	
até 31 de agosto	após 1 de setembro	até 31 de agosto	após 1 de setembro	até 31 de agosto	após 1 de setembro	até 31 de agosto	após 1 de setembro
0	210	152	41	175	97	336	139
331		**193**		**272**		**475**	

Como resulta da tabela, no período de setembro de 2015 a agosto de 2016, foram movimentadas 433 mensagens de e para colegas (das quais, 97 entre 1 de setembro e 31 de dezembro de 2015 e 336 entre 1 de janeiro e 31 de agosto de 2016). Anote-se que no período

correspondente anterior (1 de setembro de 2014 a agosto de 2015) tinham sido movimentadas por via desta caixa do correio 216 mensagens. Por sua vez, no período de setembro a dezembro de 2016, foram movimentadas mais 139 mensagens. Ou seja, no decurso de 2016, foram movimentadas 475 mensagens – quando em 2015 haviam sido 272 e em 2014 apenas 193. Anotou-se, pois, de um ano para outro, um enorme incremento destas mensagens de e com magistrados. Ou seja, um número muito maior de magistrados passou a recorrer ao Gabinete Cibercrime para colocar questões ou dúvidas em casos concretos. Este incremento tem vindo a ser consistente. De 2013 para 2014 anotou-se uma aparente quebra – aparente, porque desde então, por determinação superior, muitas das comunicações passaram a ser efetuadas pelo sistema de mensagens do SIMP.

38. Este progressivo e constante incremento no movimento de mensagens de e para magistrados resulta também claramente do gráfico que segue, onde se indicam dados referentes aos anos de 2013 a 2016.



39. A estes contactos, de colegas, por via de correio eletrónico, acrescem 75 outros contactos telefónicos da mesma natureza, estabelecidos no período de janeiro a dezembro de 2016.

C.5. INTERAÇÃO COM O GABINETE DE IMPRENSA

40. No período a que se refere este relatório, as matérias relacionadas com a cibercriminalidade ganharam grande visibilidade pública e nos meios de comunicação social, sendo frequentemente abordadas nos *media*. Por este motivo, com recorrência, o Gabinete de Imprensa da Procuradoria-Geral da República solicitou a cooperação do Gabinete Cibercrime a propósito de questões que lhe foram colocadas. Em consequência, no período de setembro de 2015 a dezembro de 2016, foram movimentadas, entre o Gabinete Cibercrime e o Gabinete de imprensa, 159 mensagens de correio eletrónico.

41. Além disso, de acordo com instruções superiores, foram recebidos jornalistas e prestadas declarações a alguns meios de comunicação social. Tais contactos vieram a ter repercussão, sendo incluídas em peças jornalísticas radiofónicas, da Rádio Renascença, emitida a 13 de fevereiro de 2016 (que pode ser consultável em http://rr.sapo.pt/noticia/46824/cibercrime_tem_aumentado_mas_nao_ha_estatisticas), e da Antena 1, emitida a 30 de março de 2016, (que pode ser consultável em http://www.rtp.pt/noticias/grande-reportagem/www-uma-rede-para-atacar_a907604).

D. PLANO DE AÇÃO CIBERCRIME 2015-2016

42. Por despacho da Senhora Procuradora-Geral, de 15 de outubro de 2015, foi aprovado o Plano de Ação Cibercrime do Ministério Público para o ano judicial 2015-2016 – junta-se o plano, como Anexo 3. Foi ainda fixado que tal plano deveria ser executado entre setembro de 2015 e julho de 2016.

Era objetivo geral deste plano de ação "dotar o Ministério Público de mais eficácia no tratamento de todos os fenómenos de natureza criminal ocorridos nas redes de comunicações ou cometidos por via delas". Além disso, pretendia desenvolver-se o conhecimento deste fenómeno, sensibilizando em particular os magistrados para as problemáticas que o envolvem. Em particular, pretendia também desenvolver-se formação de magistrados do Ministério Público, especificamente nesta área, criando especialização nesta temática nas comarcas.

D.1. REFORMULAÇÃO DA REDE DE PONTOS DE CONTACTO DO CIBERCRIME

43. Desde a sua criação, em dezembro de 2011, o Gabinete Cibercrime criou e manteve uma rede de pontos de contacto em todos os antigos círculos judiciais. A tais pontos focais foi dada a missão de recolher informação sobre as problemáticas da realidade processual na área da cibercriminalidade, para introduzir à discussão nas reuniões de pontos de contacto, devendo depois transmitir aos colegas da circunscrição as conclusões destas mesmas reuniões. Ou seja, aos pontos de contacto tem cabido estabelecer a comunicação do Gabinete Cibercrime com os restantes colegas da respetiva circunscrição. Além disso, têm também assumido o importante papel de recolha de casos e decisões preferidas nos tribunais, tendo em vista a sua partilha.

Entretanto, a orgânica judiciária foi alterada e os círculos judiciais deixaram existir. Acresce que a atividade dos pontos de contacto, muitíssimo dinâmica em muitos casos foi, num ou noutro, menos consequente ao nível da circunscrição.

44. O Plano de Ação previa que, em colaboração com os Magistrados Coordenadores das Comarcas, por um lado, se redefinisse a rede de pontos de contacto, conciliando-a com a nova orgânica judiciária. Mas por outro, previa que esta reforma comportasse uma outra vertente: pretendia que a rede renovada tivesse mais consequências práticas ao nível local e ao nível da partilha de informação (no SIMP). Era propósito do Plano que, sempre que possível, os pontos de contacto da rede fossem magistrados especializados, a quem pudessem ser privilegiadamente distribuídos inquéritos destas temáticas. Sendo certo que algumas Comarcas já anteriormente tinham dado passos nesse sentido, aquilo que se pretendia agora era que o ponto (ou pontos, consoante a dimensão da Comarca) fosse o embrião de uma futura especialização na distribuição de processos nesta área (por exemplo de casos em que haja particulares exigências na obtenção de prova digital, ou em que estejam em causa crimes previstos na Lei do Cibercrime e burlas informáticas, ou ainda em que se investiguem factualidades particularmente complexas, praticadas com o uso de tecnologias).

45. Durante setembro e outubro de 2015 diligenciou-se junto dos Magistrados Coordenadores das Comarcas, no sentido da indicação, pelos mesmos, dos novos pontos de contacto, vindo a resultar, desta iniciativa, a redefinição da rede de pontos de contacto. A 18 de novembro de 2015 veio a ser publicada no SIMP / Cibercrime uma nova lista de pontos de contacto.

Entretanto, porque após as férias judiciais do verão de 2016 houve um novo movimento de magistrados, tornou-se necessário ajustar de novo a lista de pontos de contacto – fixou-se assim uma renovada lista de pontos de contacto, a qual ficou, desde então, consultável por todos os magistrados do Ministério Público, no SIMP.

Reunião dos Pontos de Contacto – 23 de fevereiro de 2016

D.2. REUNIÃO DOS PONTOS DE CONTACTO

46. Estabilizada, no fim de 2015, a nova rede de pontos de contacto, já ajustada à nova orgânica judiciária, convocou-se uma reunião dos mesmos, a qual veio a realizar-se em Lisboa, na Procuradoria-Geral da República, a 23 de fevereiro de 2016. Junta-se, como Anexo 5, a agenda da reunião. Tratando-se de uma reunião de trabalho, não se procedeu a avaliação da mesma, como geralmente ocorre com outras sessões do Gabinete Cibercrime.

Nesta reunião, a cuja abertura procedeu a Conselheira Procuradora-Geral da República, foram abordadas algumas das propostas práticas, em investigação criminal, do Gabinete Cibercrime. Foi ainda solicitado aos colegas que se pronunciassem quanto aos fenómenos criminógenos e quanto às questões problemáticas mais significativos nas respetivas comarcas.

Noutra vertente, foi dada nota de novos projetos, em desenvolvimento, na área da pornografia infantil nas redes (apresentação a cargo de Marta Viegas, do DCIAP), da linguística forense, da articulação do Ministério Público com os OPC na área do cibercrime e da obtenção de prova digital e ainda na área das burlas *online*.

Primeira reunião do Grupo de Apoio Técnico ao Gabinete Cibercrime 11 de fevereiro de 2016

D.3. CONSTITUIÇÃO DO GRUPO TÉCNICO DE APOIO

47. O Plano de Ação Cibercrime do Ministério Público 2015 – 2016 previa diversas linhas de atividade que supunham o desenvolvimento de diálogo com entidades externas ao Ministério Público. Por outro lado, essas mesmas linhas de atividade supunham um debate interno alargado, que permitisse consolidar perspetivas de abordagem e firmar convicções quanto à forma como devia o Ministério Público explorar as opções estratégicas descritas naquele Plano de Ação.

Importou, pois, promover um diálogo técnico interno, com magistrados com especiais conhecimentos e por isso particularmente aptos e vocacionados em matérias de cibercriminalidade e de obtenção de prova digital. Este diálogo teve em vista contribuir para a melhor conformação do perfil das diversas atividades, permitindo assim, a seu tempo, fundar as opções na densificar das ações que vieram a empreender-se.

Optou-se assim pela constituição de um Grupo de Apoio Técnico ao Gabinete Cibercrime, composto por magistrados de proveniências diversas: Rui Batista e Raúl Farias, em serviço no Gabinete da Procuradora Geral da República, Marta Viegas, em serviço no Departamento Central de Investigação e Ação Penal, João Conde Correia e José Eduardo Lima, em serviço na Procuradoria-Geral Distrital do Porto, Miguel Rodrigues, em serviço no DIAP da Comarca de Leiria e Nuno Serdoura dos Santos, em serviço no DIAP da Comarca do Porto – Matosinhos. Veio a realizar-se uma primeira reunião do Grupo Técnico de Apoio a 11 de fevereiro de 2016. Junta-se a respetiva agenda Anexo 43.

D.4. REALIZAÇÃO DE SESSÕES DE COORDENAÇÃO NAS COMARCAS

48. Em execução do Plano de Ação Cibercrime 2015/2016, entre novembro de 2015 e julho de 2016, o Gabinete Cibercrime, realizou sessões de coordenação nas Comarcas do território nacional continental. Fora ainda realizada, em junho de 2015, uma sessão piloto em Santarém.

Tais sessões dirigiram-se a magistrados do Ministério público com funções de investigação criminal em cada comarca. Porém, em muitas delas, foi solicitado e permitido que assistissem juízes, militares da GNR, agentes da PSP, inspetores da Polícia Judiciária e ainda funcionários da Autoridade Tributária.

Sessão de Coordenação na Comarca da Guarda
14 de janeiro de 2016

No caso do Porto, a sessão foi desdobrada em duas, pelo grande número de participantes. Quanto a Lisboa, realizaram-se três sessões diferentes: uma delas, destinada a magistrados em funções nos núcleos do DIAP de Lisboa a sul do Tejo, abrangendo, portanto, os núcleos de Almada, do Barreiro, da Moita, do Montijo e do Seixal; outra para os magistrados das secções de competência indiferenciada do DIAP de Lisboa; uma última, visando os magistrados das secções de competência especializada do DIAP de Lisboa, tendo nela participado, igualmente, magistrados das secções especializadas do DIAP da Comarca de Lisboa Oeste (Sintra, Cascais e Amadora).

49. Foram assim realizadas as sessões que constam da tabela que segue.

Comarca	Data	Participantes	Participantes Magistrados
Santarém	26.06.2015	17	17
Elvas	26.10.2015	42	6
Beja	06.11.2015	10	6
Évora	27.11.2015	8	8
Vila Real	08.01.2016	8	8
Viseu	13.01.2016	17	17
Guarda	14.01.2016	10	10
Lisboa Oeste	14.03.2016	15	15
Lisboa	20.04.2016 (Barreiro)	15	15
	02.05.2016 (Lisboa Genéricas)	12	12
	26.04.2016 (Lisboa Especializadas)	16	16
Porto Este	04.05.2016	22	22
Setúbal	09.05.2016	22	13
Braga	11.05.2016	36	32
Viana do Castelo	12.05.2016	21	10
Coimbra	18.05.2016	19	19
Leiria	19.05.2016	26	13
Lisboa Norte	31.05.2016	8	8
Aveiro	06.06.2016	42	32
Castelo Branco	07.06.2016	20	13
Faro	23.06.2016	20	10
Bragança	01.07.2016	7	7
Porto	05.07.2016 (Porto e Maia)	43	43
	05.07.2016 (restantes municípios)	30	30
TOTAL		**486**	**313**

No conjunto destas 24 sessões participaram 486 pessoas, das quais 313 eram magistrados do Ministério Público.

50. As sessões tiveram, naturalmente, a mesma estrutura: em todas foi feita uma apresentação descrevendo as manifestações mais frequentes de cibercriminalidade e a lei penal substantiva que lhes é aplicável. Por outro lado, em todas foi abordada a temática da prova digital – em particular, foram apresentadas algumas das propostas concretas de métodos de investigação desenvolvidos pelo Gabinete Cibercrime. Transversalmente, também em todas as sessões foram discutidos casos concretos trazidos pelos colegas da Comarca. A sessão destinada às secções especializadas das Comarcas de Lisboa e Lisboa Oeste foi ajustada, sendo-lhe dado um enfoque menos genérico.

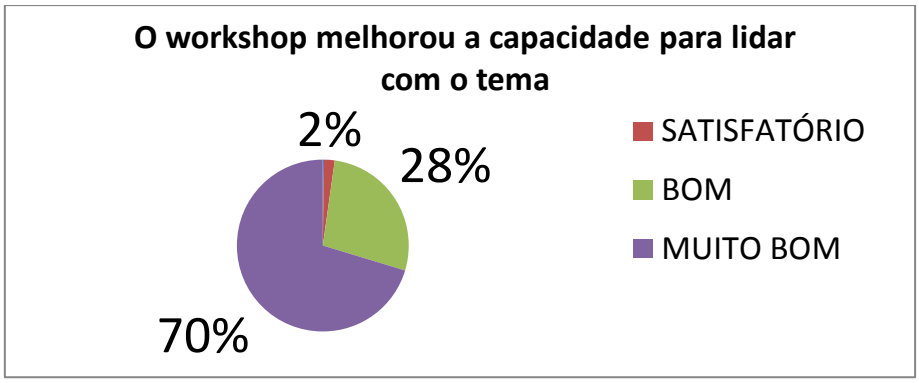
D.5. AVALIAÇÃO DAS SESSÕES DE COORDENAÇÃO

51. Em todas as sessões foi solicitado aos participantes que fizessem a avaliação da sessão, através da distribuição de fichas individuais, de preenchimento não identificado. A generalidade

dos participantes preencheu e entregou essa ficha de avaliação. Foram assim recolhidas, no conjunto das 24 sessões, 448 fichas de avaliação.

52. A análise das avaliações do conjunto das sessões revela um balanço muitíssimo positivo. Desde logo, quanto à apreciação global da reunião, sendo perguntado aos participantes se a sessão melhorou a capacidade para lidar com o tema, com uma única exceção, não há respostas de "fraco"[5]. Por outro lado, o número de participantes que acham que o resultado é "satisfatório" é muito diminuto, representando apenas 2% das respostas. Acresce ainda que, do conjunto das 448 respostas, 70% delas, correspondentes a 315 respostas, responderam "muito bom". É o que consta da tabela e do gráfico que seguem.

	FRACO	SATISFATÓRIO	BOM	MUITO BOM	NÃO RESPONDEU
O *workshop* melhorou a capacidade para lidar com o tema	1	9	123	315	0



53. Estas respostas, por um lado, sublinham claramente o interesse dos participantes pelas temáticas exploradas nas sessões. Dito de outra forma, esta avaliação revela grande interesse por estes assuntos ou, pelo menos, um grande reconhecimento da importância dos mesmos e da sua inclusão em sessões de formação.

Mas por outro lado, estas respostas também se revelam muitíssimo positivas ao manifestarem agrado pelo método seguido, de introdução de casos concretos nas exposições. Resulta da análise dos inquéritos de avaliação que, com grande expressividade, a generalidade dos participantes sentiu que a análise de casos

Sessão de coordenação na Comarca de Lisboa Norte, Loures 31 de maio de 2016

[5] A ficha na qual a sessão foi avaliada como fraca continha o seguinte comentário: *a avaliação a nível de apreciação global prende-se obviamente que com os conhecimentos que considero ter sobre a matéria, bem como com as expetativas com a frequência desta sessão.* Afigura-se que, com esta observação, o respetivo subscritor pretende justificar porque considerou, na sua apreciação global (parâmetros "o workshop melhorou a capacidade para lidar com o tema" e "satisfação das expetativas") que a sessão estava ao nível de "fraco".

concretos foi muito relevante.

54. No contexto global, o único aspeto em que a avaliação não é tão expressivamente muito boa é, no contexto da organização da reunião e, em particular, o do local da sessão.

D.6. DESENVOLVIMENTO DE INICIATIVAS ESPECÍFICAS – BURLAS *ONLINE*

55. Uma das linhas concretas do Plano de Ação era o desenvolvimento de iniciativas específicas dirigidas a práticas criminosas específicas.
Na verdade, o Plano reconhecia a relevância que têm vindo a assumir alguns particulares fenómenos criminógenos nas redes de comunicações, por atingem um número muito significativo de vítimas. É, por exemplo, o caso das vendas fraudulentas de produtos na Internet, nas quais o agente dos factos põe à venda um produto, que vende a múltiplas pessoas, recebendo o respetivo preço, sem nunca o entregar a nenhuma delas. Muitas delas acabam por apresentar queixa na comarca onde residem, dando-se assim origem a múltiplos processos de inquérito em que a vítima é diferente, mas o agente do crime e a sua ação criminosa são a mesma. Estes casos, que suscitam frequentemente questões de conexão, em geral dão origem a investigações isoladas (quando poderia proceder-se a uma só investigação, concentrando vários casos em conexão), multiplicando-se assim o mesmo tipo de diligências, num inglório esforço de investigação e num desnecessário consumo de recursos processuais.

56. Indo ao encontro desta questão, procurou criar-se um mecanismo operacional que permitisse, aos magistrados titulares de processos desta natureza, perceber se um determinado processo de inquérito está em relação, designadamente de conexão, com outros também pendentes.
Em conjugação com o Gabinete de Coordenação dos Sistemas de Informação da Procuradoria-Geral da República, desenvolveu-se o conceito de um registo de dados de processos (não pessoais), no SIMP. Tal estrutura informática veio a ser desenvolvida e, experimentalmente, foram introduzidos na mesma dados de alguns processos. À data da elaboração deste relatório decorria a introdução de um número mais alargado de dados processuais, que foram usados como dados de teste, tendo em vista a realização de testes ao funcionamento e à eficácia da ferramenta. Tais dados de teste foram fornecidos pela 8ª Secção do DIAP de Lisboa e referiam-se a processo reais, não sujeitos a segredo de justiça.

57. Uma primeira e breve análise da essência destes processos de inquérito permitiu perceber que um muitíssimo significativo número deles, embora catalogados como burla *online*, respeitam a uso fraudulento de cartões de crédito. Na generalidade destas situações é denunciado o uso de cartão de crédito (ou dos dados do mesmo) em lojas no estrangeiro e, sobretudo, em compras na Internet. Em regra, o queixoso tem muito pouca informação sobre o local e demais circunstâncias da compra – apenas sabe o que vem mencionado no seu extrato.
Na generalidade destes processos, a vítima/denunciante tem uma postura pouco cooperadora com a investigação. Muitas das vezes, o cartão já foi cancelado e o seguro ativado – esta ativação do seguro é, com frequência, a verdadeira motivação da queixa. Por via da queixa, o denunciante espera vir a ser ressarcido pelo seguro.

Anote-se que os bancos emissores do cartão nem sempre detetam este uso indevido – embora tal também ocorra, sobretudo com montantes mais elevados. Muitas das situações apenas são descobertas quando o lesado recebe, pelo correio, o extrato do cartão de crédito, o que ocorre, por vezes mais de um mês após o uso fraudulento.

58. Além destes processos, foram também introduzidos na base de dados inquéritos por factos de outra natureza, designadamente de *phishing* bancário, que causa prejuízos significativos, bem como de outras burlas, na venda de objetos que depois nunca são entregues e em ofertas de trabalho que, de alguma forma, suponham pagamento antecipado. Quanto às vendas, é muito frequente a utilização de plataformas de vendas *online* baseadas em Portugal, mas também a utilização de perfis falsos no Facebook.

D.7. DESENVOLVIMENTO DE INICIATIVAS ESPECÍFICAS – CRIMES NA *DARKWEB*

59. Outro dos fenómenos criminógenos que procurou encarar-se, nesta vertente do Plano, foi o da criminalidade emergente na chamada *darkweb* – e, em especial, das vendas, em grande escala, de produtos ilegais na Internet (drogas, armas, órgãos humanos, moeda falsa, documentos falsos, entre muitos outros). Foi identificado haver ocultamente venda de produtos cujo comércio não é legalmente permitido, a qual é livremente desenvolvida na *darkweb*, sem qualquer controlo. Este comércio está aberto a todos os que o pretendam, bastando para isso que se munam de *software* de anonimização livremente disponível na Internet.
Entendeu-se que importava desenvolver o conhecimento sobre estas realidades, por via da troca de experiências entre as entidades públicas com intervenção no setor, tendo em vista vir a desenhar uma estratégia multidisciplinar e interinstitucional que permitisse melhor enfrentar este fenómeno criminoso global. Entendeu-se igualmente avaliar a eficácia das ferramentas de investigação existentes, neste contexto, e lançar a discussão sobre eventuais necessidades de intervenção, legislativa ou de outra natureza.
Tendo em vista prosseguir estes propósitos, desenvolveram-se duas iniciativas: por um lado, realizou-se uma conferência, a 11 de março de 2016, na Procuradoria-Geral da República, submetida ao tema "Desafios da Criminalidade na *Darkweb*"; por outro lado, realizou-se uma reunião fechada, com outras entidades públicas com potencial intervenção no setor, a qual ocorreu igualmente na Procuradoria-Geral da República, no mesmo dia 11 de março de 2016.

60. Quanto à conferência "Desafios da Criminalidade na Darkweb", foi dirigida à comunidade jurídica (magistrados, advogados e outros juristas) e teve em vista a discussão da temática, numa perspetiva técnico-jurídica, pretendendo fazer-se uma avaliação da eficácia das ferramentas de investigação existentes, bem como lançar a discussão sobre eventuais necessidades de intervenção, legislativa ou de outra natureza.
Nas apresentações foram abordadas temáticas gerais relacionadas com os "*Desafios da criminalidade na* darkweb" (apresentação do Gabinete Cibercrime), a genérica realidade da *darkweb* (apresentação sobre "O que é a *darkweb*?", de Lino Santos, do Centro Nacional de CiberSegurança), a "Experiência prática na Europa (apresentação de Carlos Nunes, Inspetor da Polícia Judiciária) e "O quadro legal português e a *darkweb*: obstáculos legais à obtenção de prova" (apresentação de David Silva Ramalho, advogado). Junta-se a agenda do evento, como Anexo 7.

A conferência contou com 57 participantes, maioritariamente magistrados do Ministério Público. Foi solicitado aos participantes que fizessem a avaliação da sessão, através da distribuição de fichas individuais, de preenchimento não identificado. 28 dos participantes preencheram e entregaram essa ficha de avaliação. Nas mesmas, foram expressas as respostas que seguem.
As respostas às questões respeitantes à **organização** foram as seguintes:

	FRACO	SATISFATÓRIO	BOM	MUITO BOM	NÃO RESPONDEU
Preparação, informação preliminar	1	4	15	7	1
Pontualidade	0	0	10	17	1
Local	0	6	13	9	0

Por sua vez, as respostas às questões respeitantes ao **conteúdo** foram as seguintes:

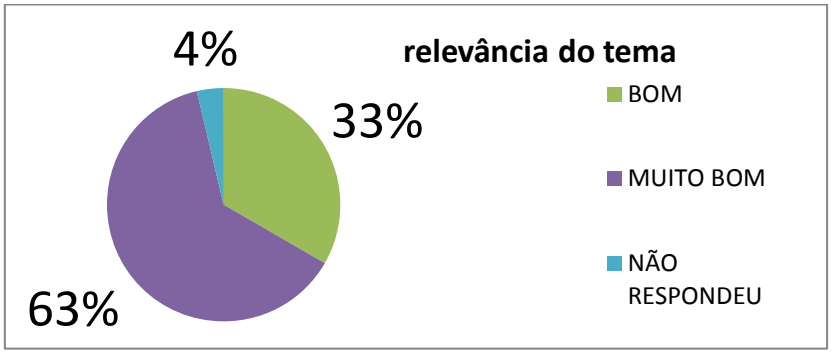
	FRACO	SATISFATÓRIO	BOM	MUITO BOM	NÃO RESPONDEU
Relevância dos temas	0	0	9	18	1
Organização dos conteúdos	0	1	15	12	0
Qualidade dos oradores	0	0	13	15	0
Qualidade do Debate	0	1	17	8	2

Por último, as respostas às questões respeitantes à **apreciação global** da conferência foram as seguintes:

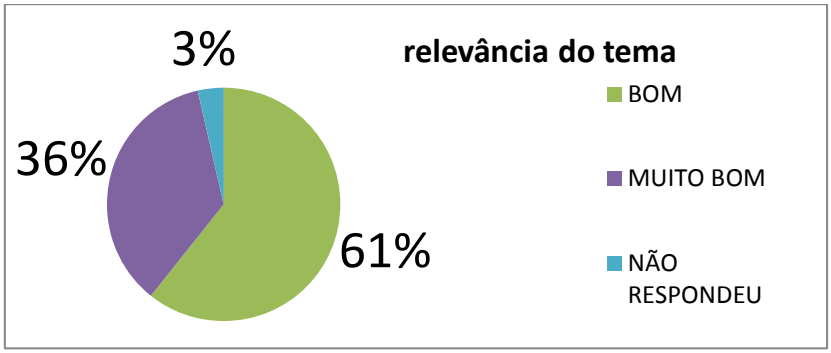
	FRACO	SATISFATÓRIO	BOM	MUITO BOM	NÃO RESPONDEU
A sessão melhorou o meu conhecimento do tema	0	1	16	11	0
Satisfação das expetativas	0	0	17	10	1

No conjunto das fichas de avaliação, foram expressos apenas quatro comentários: sobre a logística da sessão (questionando, por exemplo, a "*identificação inequívoca do local da conferência*" ou a "*sonorização*"), mas também sobre o conteúdo – por exemplo, reclamando ("*algumas das apresentações foram demasiado técnicas*"), mas igualmente manifestado apreço ("*agradeço a oportunidade. Congratulo o Gabinete Cibercrime pela iniciativa*").

61. Dos quadros que antecedem destaca-se, quanto à relevância do tema escolhido, que uma grande maioria (de 63%) das respostas foi de "muito bom".



Por outro lado, quanto à satisfação de expetativas, todos os participantes responderam de forma positiva (17 responderam "bom" e 10 "muito bom").



62. Quanto à reunião reservada a instituições públicas com competência no estudo, deteção e combate a fenómenos criminais na *darkweb*, compareceram representantes de estruturas do Ministério Púbico (Departamento Central de Investigação e Ação Penal, Departamento de Investigação e Ação Penal Distrital do Porto e Departamento de Investigação e Ação Penal Distrital de Lisboa), mas também da Polícia Judiciária, da Polícia de Segurança Pública, da Guarda Nacional Republicana, do Centro Nacional de Cibersegurança e ainda do Serviço de Informações de Segurança. Não foi sido possível contar com a presença do Serviço de Estrangeiros e Fronteiras.

As diversas instituições representadas discutiram os desafios estratégicos nacionais trazidos pelo desenvolvimento da criminalidade na *darkweb*, sublinhando a necessidade de se vir a desenhar uma estratégia multidisciplinar e interinstitucional que permita melhor enfrentar este fenómeno criminoso global. Obtiveram-se algumas conclusões sobre a situação presente destes fenómenos ilícitos e a forma de os encarar em Portugal. De modo informal veio igualmente a lançar-se a ideia da necessidade e vantagem de criação de uma rede não formal de especialistas na matéria, que possa vir a enriquecer futuros debates e a flexibilizar eventual cooperação operacional, quer em prevenção criminal, quer em futuras investigações concretas.

D.8. COOPERAÇÃO COM ORGÃOS DE POLÍCIA CRIMINAL

63. Constituía prioridade do Plano de Ação potenciar a cooperação com os órgãos de polícia criminal na obtenção de prova digital. Na verdade, é sabido que o mecanismo rotineiro de delegação de competência para investigação nos órgãos de polícia criminal supõe, em geral, algum percurso burocrático, de troca de expediente entre o Ministério Público e o OPC. Nesta rotina, de remessa física do processo ao OPC, após despacho de delegação de competência pelo Ministério Público, decorre um lapso de tempo significativo, durante o qual nem sempre é realizado qualquer ato de investigação criminal.

Porém, nos casos em que, logo no início da investigação, se torna necessária a recolha de prova digital – sobretudo de registo de comunicações (em especial referente a endereços IP) –, pertencendo à autoridade judiciária a competência para esta diligência de prova, aquele percurso burocrático acaba por ser infrutífero, porque o processo tem que ser, de novo, levado a despacho ao Ministério Público. Nestes trâmites esgota-se tempo que, muitas vezes, torna inviável a obtenção daquela prova, por já estar indisponível.

Noutra vertente, é também pacificamente reconhecido ser cada vez mais corrente a necessidade de, em inquérito, proceder à apreensão de dispositivos de comunicação móveis (telemóveis, *smartphones*, *tablets*, etc). O regime de apreensão e de obtenção da eventual prova nele contida é complexo – por exemplo, em certas situações pode ser necessária a intervenção do juiz de instrução (será, por exemplo o caso da apreensão de mensagens eletrónicas ou de dados suscetíveis de pôr em risco o respeito pela privacidade do visado).
Por último, tem sido notado que não tem chegado aos OPC suficiente conhecimento dos novos métodos de investigação e de obtenção de prova, implementados pelo Ministério Público (por exemplo, sobre os procedimentos expeditos para solicitação de informação aos operadores de comunicações portugueses e internacionais, ou sobre as novas possibilidades de realização de perícias, com recurso às universidades).

64. Nestas circunstâncias, na sequência de contacto exploratório da Guarda Nacional Republicana, foi realizada uma reunião na Procuradoria-Geral da República, a 31 de março de 2016, à qual compareceram responsáveis da área da investigação criminal da GNR. A reunião teve como propósito específico aperceber eventuais linhas de evolução e iniciativas futuras neste domínio, do cibercrime e, sobretudo, da obtenção de prova digital.
Após a reunião, foram disponibilizadas à GNR todas as notas práticas do Gabinete Cibercrime, para distribuição interna. Também foi manifestada disponibilidade para contactos, para esclarecimento de questões operacionais, por via do endereço cibercrime@pgr.pt.

65. Globalmente, conclui-se nesta reunião que será muito vantajoso o desenvolvimento, em conjunto com os OPC, de modelos ou formulários de apreensão de elementos de prova. Por exemplo, será facilitador das investigações vir a estabelecer um formulário de apreensão de telefones e outros dispositivos móveis, acompanhada de uma nota prática a propósito do tema.
Da mesma forma, foi julgado muito interessante promover sessões formativas e de partilha de boas práticas, com a participação de agentes policiais com funções na área da investigação criminal, dos diversos órgãos de polícia criminal.
Mais tarde, após esta reunião, passou a dar-se regular conhecimento à GNR da realização das sessões de coordenação nas comarcas, de que acima se deu conta. Desta forma, passou a haver participação sistemática de militares daquela corporação nas sessões nas Comarcas.

66. Suscitou ainda a GNR a necessidade de receber orientações genéricas do Ministério Público a propósito do recebimento de queixas por via de correio eletrónico. Foi referido que estes tipos de queixas têm sido crescentemente recebidos pela Guarda, sem que haja uma orientação clara quanto à forma de as processar e tramitar.

67. Ainda no contexto da cooperação com a GNR, a 6 de junho de 2016, fez-se uma visita ao Núcleo Técnico Informático da GNR em Coimbra. Este núcleo tem como tarefa proceder a exames a equipamento informático (suportes de dados informáticos), apreendidos em processos-crime cuja investigação esteja delegada na GNR.
Nesta breve visita percebeu-se que a GNR vem procedendo a exames informáticos que, anualmente, estão na ordem das centenas. Fá-lo sem grande demora, assim permitindo que as investigações a que respeitam vão avançando. Afigura-se que este núcleo constitui uma mais

valia, já que permite debelar as dificuldades com que o Ministério Público se tem deparado na realização de perícias informáticas, de que já acima se deu conta.
Deu a GNR notícia de que está a ser implementado um novo núcleo deste tipo, em instalações da Guarda, em Alcabideche.

D.9. RECEBIMENTO DE DENÚNCIAS POR CORREIO ELETRÓNICO

68. Como noutros pontos, acima, se referiu, tem-se anotado, com crescente regularidade, o recebimento de mensagens por via do endereço eletrónico do Gabinete Cibercrime (cibercrime@pgr.pt) – muitas delas, igualmente em número crescente, veiculam queixas da prática de crimes. O Plano de Ação sublinhava a necessidade de dar enquadramento a estas últimas.
Na verdade, entre muitas mensagens que dificilmente se distinguem de vulgar *spam*, algumas das queixas de crimes recebidas descrevem, com algum detalhe, situações factuais que, a serem verdadeiras, consubstanciam crime. Nem sempre provêm de pessoas que se identifiquem. Porém, apercebe-se com frequência, nos casos relatados, haver alguma urgência na recolha de prova que, a não ser de imediato recolhida, poderá deixar de existir.
Previa o Plano de Ação que se explorasse a possibilidade de criar canais expeditos que permitissem encaminhar para os serviços do Ministério Público competentes estas denúncias, para que, por um lado, possam ser praticados, sem esperar pelos habituais trâmites burocráticos, atos urgentes de recolha de prova e, por outro, serem desenvolvidas diligências no sentido do preenchimento de eventuais condições formais em falta na denúncia (por exemplo, a cabal identificação do denunciante).

69. Indo ao encontro destes objetivos, passou a disponibilizar-se no micro portal do Cibercrime na Internet, a que acima se aludiu, uma chamada para a possibilidade de se poderem encaminhar denúncias, por via do endereço do Gabinete Cibercrime. Esta disponibilização ocorreu aquando a reestruturação do micro portal, do qual acima se deu conta, em fevereiro de 2016.
Além disso, estabeleceu-se contacto com a 9ª Secção do Departamento de Investigação e Ação Penal de Lisboa, a quem estão distribuídos os processos relacionados com a criminalidade informática, tendo em vista definir os parâmetros de um procedimento experimental de recebimento e encaminhamento de denúncias. Este procedimento experimental procurou, por um lado, testar uma solução para o inexorável crescimento das denúncias recebidas por correio eletrónico; por outro, procurou satisfazer algumas das exigências formais (do Código de Processo Penal) a que o recebimento de queixas por correio eletrónico não consegue dar resposta.

70. Assim, por exemplo, embora se aceitassem as queixas efetuadas por esta via, do correio eletrónico, disponibilizou-se uma advertência no micro portal, alertando para as formalidades da queixa – as quais, não estando reunidas, porventura criarão necessidade de tal queixa ser ulteriormente ratificada pelo queixoso.
Por outro lado, criaram-se também critérios de análise destas queixas, tendo em vista a triagem daquelas que são remetidas ao DIAP de Lisboa e aquelas que o não são. O Gabinete Cibercrime apenas encaminha, por correio eletrónico, as mensagens recebidas, em benefício dos respetivos

remetentes (tendo em vista a celeridade na realização de eventuais diligências urgentes na obtenção de prova digital). Por isso, quanto a todas as denúncias recebidas em que se referiam crimes particulares (registaram-se muitas delas em que se denunciavam difamações) informou-se o remetente da mensagem de que existe a possibilidade de queixa, bem como da forma e dos locais onde a mesma pode ser efetuada. Procedeu-se de igual modo quanto a crimes de burla de pequenos montantes, em compras ou vendas na Internet, por tal tipo de crime ser, em geral, de natureza semipública. Neste caso específico, apenas assim não se fez quando se anteviu, naquilo que se denunciava, urgência na recolha de prova. Por último, não foram transmitidas ao DIAP de Lisboa mensagens cujos factos fossem demasiado genéricos ou inverosímeis – sem prejuízo de se informar o remetente da possibilidade legal que sempre existe, de apresentar queixa formal.
No período que decorreu entre janeiro e dezembro de 2016 foram registadas pelo Gabinete Cibercrime 108 queixas. Em muitas delas o denunciante não estava identificado – nem era legal ou tecnicamente identificável de imediato. Em muitas outras denunciavam-se crimes contra a honra, de natureza particular. Outras, ainda, apenas reportavam meras suspeições, ou factos muito genéricos.
20 destas 108 queixas foram remetidas ao DIAP, para inquérito. Os seus remetentes foram informados do mesmo, sendo-lhes posteriormente dado conhecimento do número processual atribuído a essa queixa (NUIPC), bem como da secção do DIAP correspondente. A estas participações remetidas para o DIAP, acrescem outras três, remetidas para o Gabinete da Procuradora-Geral da República, com vista a serem encaminhadas para departamentos do Ministério Público noutras jurisdições (não penais).
Quanto às queixas não remetidas, foi dada resposta às mesmas, informando da possibilidade de queixa formal.

D.10. ARTICULAÇÃO COM OUTRAS ENTIDADES

71. O Plano de Ação Cibercrime do Ministério Público 2015 – 2016 previa, como uma das linhas de ação a desenvolver, a articulação e a cooperação com entidades responsáveis pela segurança informática. No Plano assumia-se que a ocorrência de atos criminosos contra estruturas de comunicação e informação – por exemplo, os ataques informáticos – consubstancia, em geral, a prática de crimes. A sua deteção é frequentemente feita por estruturas privadas (*CERTs* de entidades privadas: universidades, operadores de comunicações ou bancos) e também por estruturas públicas (Centro Nacional de Cibersegurança ou CERT-PT), sendo a apresentação da queixa pelas entidades lesadas muitas vezes efetuada bastante tempo depois dos factos, o que torna menos viável a investigação.
Procurou-se, pois, dialogar, em especial, com o Centro Nacional de Cibersegurança, mas também, por razões específicas, com o Ministério dos Negócios Estrangeiros.

a) MINISTÉRIO DOS NEGÓCIOS ESTRANGEIROS – EMBAIXADOR PARA A CIBERSEGURANÇA

72. A Procuradoria-Geral da República foi oficialmente informada, pelo Ministério dos Negócios Estrangeiros, da designação do Embaixador Luís Barreira de Sousa como Embaixador para a Cibersegurança. Este cargo diplomático tem como função reforçar a interação com os diferentes atores internos envolvidos na matéria, bem como facilitar uma adequada representação de Portugal no plano externo. Solicitava o Ministério dos Negócios Estrangeiros apoio à atividade do Embaixador para a Cibersegurança.

73. Na sequência da informação oficial, tomou-se a iniciativa de contactar o Embaixador para a Cibersegurança tendo, em sequência, sido realizadas duas reuniões exploratórias de coordenação. Uma delas, ocorreu a 15 de abril de 2016, e a outra, a 16 de maio de 2016. Ambas decorreram em instalações da Procuradoria-Geral da República.

b) CENTRO NACIONAL DE CIBERSEGURANÇA

74. Como se deixou expresso em relatórios anteriores, a partir de junho de 2015, o Gabinete Cibercrime passou a integrar, como observador, em representação do Ministério Público, a Rede Nacional de CSIRT. Os CSIRT (ou *Computer Security Incident Response Teams*) são núcleos ou equipas técnicas, responsáveis pela resolução de incidentes relacionados com a segurança de sistemas informáticos. Alguns serviços públicos integram um CSIRT, o mesmo acontecendo com algumas empresas privadas de maior dimensão. Há também empresas especializadas, que prestam este tipo de serviços a título comercial e profissional.
A Rede de CSIRT é uma estrutura informal, criada no âmbito das atividades da ex-FCCN (atual FCT – Fundação para a Ciência e a Tecnologia) com abrangência nacional. Conta com o apoio do Centro Nacional de Cibersegurança (integrante do Gabinete Nacional de Segurança). Constitui um fórum de cooperação entre equipas de resposta a incidentes de segurança informática do setor público e privado. Tem como objetivo geral estabelecer laços de confiança entre elementos responsáveis pela segurança informática de forma a criar um ambiente de cooperação e assistência mútua no tratamento de incidentes e na partilha de boas práticas de segurança. Além disso, pretende criar indicadores e informação estatística nacional sobre incidentes de segurança informática com vista à melhor identificação de contramedidas pró-ativas e reativas e criar os instrumentos necessários à prevenção e resposta rápida num cenário de incidente de segurança informática de grande dimensão.

75. O Gabinete Cibercrime foi também solicitado para integrar a chamada Comissão Doutrina do Centro Nacional de Cibersegurança, tendo participado na primeira reunião da mesma a 12 de outubro de 2015.
Ainda no contexto da articulação com o Centro Nacional de Cibersegurança, o Gabinete Cibercrime participou e interveio no Curso Geral de Cibersegurança, organizado pelo CNCS, a 17 de maio de 2016, como mais abaixo melhor se referirá.

76. Em resultado da cooperação e articulação com o Centro Nacional de Cibersegurança, o Gabinete Cibercrime passou a ter acesso a informações de alerta de segurança, algumas das quais vieram a mostrar-se relevantes para a atividade do Ministério Público. Por essa razão, o Gabinete Cibercrime passou a anunciar as mesmas no SIMP. Nestes anúncios, compilaram-se informações técnicas sobre as ameaças cibernéticas em causa, que pudessem servir de informação de investigação para colegas, em investigações concretas – dito de outra forma, estes anúncios de segurança pretenderam ser um repositório de informações de investigação, para casos em que essa informação já não esteja disponível.
Neste contexto, no período a que se refere este relatório, foram emitidos no SIMP cinco anúncios de Alerta Cibercrime (que se juntam como Anexo 14, Anexo 15, Anexo 16, Anexo 51 e Anexo 52),

datados de 7 de dezembro de 2015, 17 de dezembro de 2015, 18 de fevereiro de 2016, 5 de setembro de 2016 e 6 de setembro de 2016).
Quanto ao anúncio de 7 de dezembro de 2015, referia-se a chamadas fraudulentas efetuadas em nome da Microsoft. Dava-se conta de que estava em curso uma campanha de chamadas fraudulentas em que era invocado o apoio técnico da Microsoft tendo como alvos utilizadores no território nacional. Nesta atividade criminosa, os *atacantes* contactavam os alvos selecionados por telefone, fazendo-se passar pela equipa de Assistência Técnica da Microsoft. No contacto, a vítima era informada de que tinha um problema no seu computador (normalmente um vírus) para o qual o assistente teria resolução. A vítima era depois "conduzida" a instalar *software* que lhe era remetido e que resolveria o suposto problema. O *software* instalado era de origem maliciosa e, entre as várias ações, poderia danificar, roubar dados, cifrar (casos de *ransomware*) ou até mesmo inutilizar o sistema.
Quanto aos anúncios de 17 de dezembro de 2015 e de 18 de fevereiro de 2016, reportavam-se a campanhas de *phishing* dirigido a utilizadores de um determinado banco português. Dava-se conta de que, como habitual nestes casos, o processo começou com a expedição, para muitos destinatários, de mensagens de *email* fraudulentas. Estas mensagens anunciavam que o destinatário teria a conta bancária bloqueada até que procedesse a atualizações na mesma. Era remetido um *link*, que se dizia ser do banco em causa, mas apontava para falsas páginas. As páginas fraudulentas eram, em ambos os casos, muitíssimo parecidas, praticamente iguais, em aparência, aos olhos do utilizador comum, à autêntica página do banco. Se a vítima acedesse a ela e nela introduzisse a informação que se lhe solicitava, forneceria aos autores destes factos todos os dados necessários a proceder a todos os movimentos bancários na sua respetiva conta.
O anúncio de 5 de setembro, reportava uma campanha de *ransomware*.
Por último, o anúncio de 6 de setembro de 2016, dava conta de que estava em curso uma campanha de *phishing* especificamente dirigida a *smartphones*, transmitida por SMS, que encaminhavam as vítimas para páginas falsas de duas entidades bancárias portuguesas.
O Gabinete Cibercrime preservou os dados comunicacionais e de geolocalização disponíveis em fontes abertas na Internet e ainda dados de mensagens expedidas pelos autores dos factos, bem como informação referente ao alojamento/localização dos *sites* fraudulentos, de modo a poder remeter os mesmos a colegas que venham a ter a seu cargo inquéritos a este respeito.

E. OUTRAS ATIVIDADES DO GABINETE

E.1. ACOMPANHAMENTO DO PROJETO PROTEUS

77. A Procuradoria-Geral da República foi, por via do Gabinete Cibercrime, parceira da Associação Portuguesa de Apoio à Vítima – APAV, num projeto financiado pela União Europeia, na área do *roubo de identidade*. Este projeto não implicou nenhum custo financeiro para a Procuradoria-Geral da República ou o Estado Português. A participação da PGR foi determinante no mesmo, sobretudo na fase de procura de parceiros – o Gabinete Cibercrime estabeleceu, com sucesso, contactos com os parceiros *Fiscalía Especialista en Materia de Delincuencia Informática*, de Espanha e *Cybercrime Unit*, do *Prosecutor's Office attached to the High Court of Cassation and Justice*, da Roménia. Mas foi também muito ativa no desenvolvimento das respetivas actividades – disso mesmo se deu conta em relatórios respeitantes a períodos temporais anteriores.

No período a que se refere este relatório, o projeto entrou na fase final. Esta fase final supunha a realização de um produto final do projeto e a realização de uma conferência internacional de apresentação do mesmo.
Como produto final, foi elaborado o "*Manual Proteus – Prevenção, informação e apoio a vítimas de furto de identidade online*", em português, e em inglês, publicamente disponibilizado pela APAV. A conceção e elaboração dos textos deste manual contaram com a intervenção ativa do Gabinete Cibercrime. Quanto à conferência internacional, decorreu em Lisboa, a 29 e 30 de outubro de 2015. O Gabinete Cibercrime interveio na mesma, num painel submetido ao tema "*O que é o furto de identidade* online*; enquadramento legal internacional*".

E.2. INTERCÂMBIO COM A GOOGLE INC.

78. Desde 2013 que o Ministério Público tem desenvolvido contactos com a Google Inc., dos Estados Unidos da América, pela importância que esta sociedade tem na cooperação com concretas investigações criminais.
Neste contexto, a 19 de maio de 2016 decorreu uma reunião de representantes da Google Inc. com o Gabinete Cibercrime, em instalações da Procuradoria-Geral da República. Nesta reunião, realizada a pedido da Google, estiveram presentes em representação daquela entidade, vindos dos escritórios centrais da Google, em Mountain View, California e ainda do escritório da Google em Madrid.
Foi propósito desta reunião, em que a Google fez participar responsáveis pela cooperação com as autoridades públicas, partilhar as políticas da Google no relacionamento com estas autoridades e os mecanismos que a companhia instituiu nesse sentido. Foi afirmado que os formulários e canais de comunicação que se criaram entre o Ministério Público e a Google estão a funcionar muito bem e a produzir efeitos (fazendo de Portugal um dos países da Europa que mais eficácia tem, na cooperação com a Google, ao nível da investigação criminal). Foi sugerido que, em futura revisão do formulário, o mesmo se tornasse mais curto.

E.3. ACOMPANHAMENTO DA CRIAÇÃO DA "*EUROPEAN JUDICIAL CYBERCRIME NETWORK*" (EUROJUST)

79. Desde o segundo semestre de 2014 que o Ministério Público da Holanda e a sua delegação na EUROJUST vieram a desenvolver a ideia de vir a ser constituída uma rede europeia de magistrados do Ministério Público dedicada a temáticas específicas da área da cibercriminalidade.
No período a que respeita este relatório, a própria EUROJUST tomou a iniciativa de discutir o projeto, que partilhou com representantes dos Ministérios Públicos de toda a União Europeia. Para o efeito, convocou duas reuniões, ambas realizadas na Haia. Uma delas, o "*Eurojust Meeting on Cybercrime - Towards a Judicial Cybercrime Network*" foi especificamente dedicada a este tema e decorreu a 25 de novembro de 2015; a outra, inseriu-se no contexto do "*Strategic Seminar Keys to Cyberspace*" (do qual mais abaixo melhor se dará conta) e decorreu a 2 de junho de 2016. O Gabinete Cibercrime participou em ambas as reuniões, em representação da Procuradoria-Geral da República.
Além destas duas reuniões, veio a realizar-se uma terceira, já de constituição formal da rede europeia a 24 de novembro de 2016.

80. Quanto ao "*Eurojust Meeting on Cybercrime - Towards a Judicial Cybercrime Network*" realizado a 25 de novembro de 2015, teve como específico propósito discutir os possíveis caminhos na criação formal de uma rede judiciária na área do cibercrime. Junta-se o relatório que a propósito se elaborou, como Anexo 18.
As discussões, dinamizadas pela EUROJUST, mas também pela representação da Holanda naquele organismo, abordaram eventuais vertentes práticas e concretas. Porém, incidiram também sobre questões de âmbito mais geral: assumiu-se que a criação efetiva e formal de uma rede de procuradores na área do cibercrime assumiria um papel importante, ao permitir contruir ligações mais fáceis e sólidas entre quem tem que dirigir a investigação nos vários Estados Membros da União Europeia, abrindo canais para a partilha de boas práticas, novidades legislativas ou jurisprudência. Por outro lado, foi vincado que uma rede desta natureza deveria ser orientada para a ação e os casos concretos, permitindo facilitar a ultrapassagem de eventuais dificuldades na cooperação internacional, por exemplo. Poderia igualmente ser uma sua mais-valia a monitorização de decisões judiciais ou a partilha de atualizações sobre tendências criminógenas.

81. Quanto ao "*Strategic Seminar Keys to Cyberspace*", que decorreu a 2 de Junho de 2016, tinha um propósito de âmbito mais geral, como abaixo se especificará: congregar representantes dos Estados Membros da União Europeia com experiência prática em cibercrime, com o objetivo de identificar e encontrar possíveis soluções para os desafios da investigação e prossecução de casos de cibercrime – precisamente, uma das soluções propostas à discussão era a da criação daquilo que se propunha viesse a chamar-se *European Judicial Cybercrime Network*, ou Rede Judicial Europeia para matérias do Cibercrime. Junta-se o relatório que a este propósito se elaborou, como Anexo 20.
Na parte do seminário dedicado a este tema, discutiram-se ideias gerais do conceito, tendo em vista apresentar conclusões, para discussão e aprovação no Conselho de Ministros das áreas Justiça e Administração Interna (JAI) da União Europeia que se realizaria a 9 e 10 de junho de 2016. Assim veio, de facto, a acontecer.
Ainda no decurso da reunião foi apresentado um primeiro "produto" dessa rede embrionária: o nº 1 do *Cybercrime Judicial Monitor*, uma publicação que virá no futuro a divulgar atualizações legais nos Estados Membros, análises de decisões judiciais e ainda abordagem de tópicos especiais de interesse. Foi ainda apresentado um projeto de *site web* de acesso restrito, que se destina especificamente a servir de apoio à rede (e que viria a ser disponibilizado *online* em https://restricted.eurojust.europa.eu/my.policy).

82. Em momentos prévios ao de cada uma das duas reuniões foi solicitado ao Gabinete Cibercrime que emitisse contribuição escrita tendo em vista vir a ser submetida à discussão dos restantes participantes. Tais contribuições foram efetivamente remetidas (juntam-se como Anexo 22 e Anexo 23) e incidem sobre a estrutura da rede, os seus membros, as suas tarefas (e expetativas) e, por último, a vantagem de ser apoiada por uma página *web*.

83. Como acima se adiantou, decorreu finalmente a 24 de novembro de 2016, na EUROJUST, a primeira reunião daquilo que viria a chamar-se *European Judicial Cybercrime Network*, ou rede judicial europeia para matérias do cibercrime - EJCN. Nela tomaram parte os pontos de contacto especificamente designados para esta rede por 26 dos Estados Membros da União Europeia.

A criação formal da EJCN resultou das conclusões do Conselho da União Europeia de 9 de junho de 2016. De acordo com este ato, esta rede deve congregar representantes dos Ministérios Públicos (nalguns casos, representantes judiciais) dos Estados Membros da União Europeia, especializados em temas de cibercriminalidade. Tem como propósito geral facilitar o intercâmbio de informação sobre cibercriminalidade e prova digital, constituindo um fórum de partilha de boas práticas, novidades legislativas e jurisprudência. A rede deve constituir também um canal de diálogo disponível para a coordenação de investigações em casos concretos.
Tendo em vista materializar estes objetivos, a EJCN realizará duas reuniões por ano, publicará anualmente o boletim *Cybercrime Judicial Monitor* e manterá uma plataforma de acesso reservado na Internet, com fins colaborativos. Em cada uma das suas reuniões serão abordados específicos temas de interesse na área da cibercriminalidade e da obtenção da prova digital.

84. Esta reunião inaugural teve como temas técnicos específicos a encriptação e as investigações encobertas. Junta-se, como Anexo 54 o relatório que a este propósito se elaborou.
Quanto à encriptação, instrumento técnico absolutamente necessário à manutenção de standards mínimos de cibersegurança, foi anotado ser, por outro lado, um grande obstáculo à investigação criminal. Na verdade, na atualidade, todas as atividades criminosas podem potencialmente utilizar meios de comunicação encriptados para comunicar – WhatsApp, Skype, Telegram são, entre muitos outros recursos, vastamente utilizados por quem pratica crimes. Importa, pois, reconsiderar a encriptação numa perspetiva legislativa, reconhecendo-a como um direito, mas igualmente ponderando eventuais limitações ao seu uso, sobretudo quando em confronto com outros direitos e deveres.
Quanto às investigações encobertas, foi assumido serem uma ferramenta essencial nas investigações de criminalidade online, em particular quanto a crimes cometidos na *darkweb*.

85. Durante a reunião foi apresentado o nº 2 do *Cybercrime Judicial Monitor*, publicação da rede que, como acima se referiu, pretende divulgar atualizações legais nos Estados Membros, análises de decisões judiciais e ainda explorar tópicos de especial interesse. No corrente número, o tópico especial abordado é o do acesso remoto a sistemas de computadores. A abordagem deste tópico foca-se, sobretudo, na análise dos regimes legais já consagrados nos diversos Estados Membros. Tal análise foi feita a partir das respostas a um questionário elaborado e distribuído para o efeito. A seu tempo, Portugal respondeu a esse questionário, que atempadamente remeteu – junta-se o mesmo como Anexo 56.

Foi ainda apresentada a versão finalizada do *site web* de acesso restrito, que serve de apoio à rede (a chamada *EU Judicial Cybercrime Network Restricted Area*, acessível em https://restricted.EUROJUST.europa.eu/my.policy).

E.4. ORGANIZAÇÃO DE ATIVIDADE DA AIAMP

86. A XXII Assembleia Geral da AIAMP – Associação Ibero Americana de Ministério Públicos, que decorreu em Montevideu, no Uruguai, em 2014, deliberou que, no decurso de 2015, se organizaria um "Seminário sobre cibercrime e prova digital", ficando a respetiva organização a cargo do Ministério Público de Portugal. Por razões logísticas e de financiamento, agregou-se, coorganizando, a *Fiscalia General del Estado*, de Espanha.

Tal seminário veio a decorrer entre 5 e 9 de outubro de 2015, no Centro de Formação da AECID (Agência Espanhola de Cooperação Internacional e Desenvolvimento) de Santa Cruz de La Sierra, na Bolívia. Participaram representantes dos Ministérios Públicos e *Fiscalias* da Argentina, Brasil, Bolívia, Cuba, Equador, Espanha, Honduras, México, Panamá, Paraguai e Portugal. Junta-se a respetiva agenda como Anexo 24.

97. Este evento teve como propósito primordial sensibilizar os Ministérios Públicos do espaço ibero-americano para o significado e dimensão do cibercrime e para a importância da prova digital na atividade judiciária moderna. Por outro lado, pretendeu-se que, durante o mesmo, se detetassem eventuais lacunas legislativas e, bem assim, se identificasse a necessidade de adoção de novos diplomas normativos que as colmatem. Nesta mesma vertente, avaliou-se a conformidade das legislações nacionais dos Estados participantes com aquilo que resulta dos quadros normativos internacionais e das recomendações de organismos internacionais nesta matéria. Por último, partilharam-se experiências práticas já realizadas pelo Ministério Público, em matérias organizativas e operacionais nas áreas da cibercriminalidade e da obtenção da prova digital.

No decurso da reunião foram abordadas temáticas de direito penal substantivo: pornografia infantil, ataques a sistemas de informação, burlas através da Internet, delitos contra a propriedade intelectual e ilícitos relacionados com os crimes de ódio e terrorismo com auxílio da Internet. Foram também discutidas questões processuais: preservação de dados, buscas em sistemas informáticos, interceção de comunicações e operações encobertas nas redes. Por último, foram trocadas experiências sobre as dificuldades inerentes à cooperação internacional, avultando-se, a este propósito, a Convenção de Budapeste como a referência de harmonização normativa e de cooperação internacional.

87. Este seminário foi avaliado de forma muito positiva. Foram trocadas experiências, registando-se um elevado nível de intervenção de todos os participantes. A partilha das responsabilidades

organizativas, entre a *Fiscalía General del Estado* de Espanha e a Procuradoria-Geral da República, de Portugal foi muito enriquecedora.
Uma segunda nota positiva foi a resultante da efetiva vantagem no intercâmbio de experiências: permitiu aos presentes recolher diferentes perspetivas tendo em vista definir futuras linhas de ação, que facilitarão a cooperação entre as Procuradorias/*Fiscalías* dos diferentes países. Esta vantagem assume maior importância por se referir a ilícitos relacionados com as tecnologias de comunicação e informação, por definição transfronteiriços e que, pela sua própria natureza, nunca se confinam às fronteiras nacionais.

88. No final do seminário foi emitido um documento, enumerando as respetivas conclusões, o qual se junta como Anexo 25. Destas conclusões, salientam-se três aspetos principais: por um lado, os participantes sublinharam a necessidade de encarar os fenómenos da cibercriminalidade como supranacionais, impondo-se uma abordagem internacional conjugada, de cooperação; tal cooperação supõe, por sua vez, harmonização legislativa, à luz dos instrumentos internacionais vigentes. Em segundo lugar foi realçada a enorme complexidade técnica e a evolução constante das novas tecnologias, exigindo-se uma intervenção especializada por parte do Ministério Público o que, por sua vez, desde logo, requer um esforço permanente de formação. Em terceiro lugar, salientou-se a necessidade e vantagem de criação de uma rede de pontos de contacto especializados sobre cibercriminalidade, a serem designados por cada uma das Procuradorias/*Fiscalías*.

E.5. PREPARAÇÃO DA CRIAÇÃO DA CiberRede / *CiberRed*

89. Como fica dito, na última referência às conclusões do "Seminário sobre cibercrime e prova digital", foi declarada a importância da criação de uma rede de pontos de contacto especializados sobre cibercriminalidade, em cada uma das Procuradorias/*Fiscalías*. Esta conclusão apontava para uma ação concreta da Associação Ibero Americana de Ministério Públicos, no sentido de dotar o conjunto das Procuradorias/*Fiscalías* de um novo recurso operacional. Deste, esperava-se que pudesse potenciar o intercâmbio de experiências práticas referentes aos sistemas penais substantivos e processuais de cada país, bem como que criasse e disseminasse boas práticas, fortalecendo a cooperação – formal e informal – tendo em vista permitir solicitar e transmitir, com mais agilidade, informação eventualmente necessária a investigações.

90. Estas conclusões do seminário foram apresentadas pela Senhora Procuradora-Geral da República à XXIII Assembleia Geral da AIAMP (que decorreu igualmente em Santa Cruz de la Sierra, na Bolívia), a qual deliberou a constituição de uma tal rede. Deliberou ainda que Portugal se articulasse com a Secretaria Geral da AIAMP tendo em vista a constituição de um grupo de trabalho, constituído por diversos membros da AIAMP, que dinamizasse e definisse as linhas essenciais para o desenvolvimento, implementação e funcionamento da rede.
Após esta reunião da Assembleia Geral, tendo em vista a concretização do mandato que lhe foi conferido por aquela, a Senhora Procuradora-Geral da República determinou que o Gabinete Cibercrime, em articulação com a Divisão de Cooperação Judiciária Internacional da PGR e com o Gabinete da Procuradora-Geral, desenvolvesse as diligências necessárias à constituição do grupo de trabalho e impulsionasse e coordenasse os trabalhos de criação da rede, com vista à sua

apresentação, para aprovação, na XXIV Assembleia-Geral da AIAMP, a realizar nos dias 10 e 11 de outubro de 2016, em Lisboa. Junta-se o despacho como Anexo 26.

91. Em execução desta decisão, foi elaborado um documento de conceito dessa futura rede, o qual veio a ser remetido à AIAMP, para difusão pelos seus membros e ainda com a solicitação de indicação, desde logo, dos representantes de cada uma das instituições nacionais nesta rede. Em resposta a esta solicitação, um bom número das Procuradorias/*Fiscalías* Ibero-americanas indicaram representantes.
De seguida, dando-se disso conta à Secretaria Geral da AIAMP, solicitou-se aos representantes indicados que remetessem contributos escritos para a discussão do documento de trabalho acima referido. Solicitou-se à Secretaria Geral da AIAMP que interviesse também nestas discussões, sobretudo tendo em vista a criação de condições para que a futura rede viesse a explorar as potencialidades já providenciadas pela rede *Iber@*. Alguns dos representantes indicados reagiram a esta solicitação.

92. Veio a elaborar-se um documento final de conceito, para apresentação à Assembleia Geral, o qual se junta como Anexo 27. Este documento aponta para a criação de uma estrutura de pontos de contacto que se sugeria viesse a designar-se como CiberRede / *CiberRed*, a qual se sugeria viesse a utilizar a plataforma de comunicações *Iber@.*
Como propósito geral desta rede, propunha-se a intensificação do relacionamento entre os Ministérios Públicos na área da cibercriminalidade e da prova digital, bem como a facilitação da troca de experiências e de boas práticas, conducentes à mais eficaz cooperação no caso concreto.
Propunha-se ainda que a rede constituísse um fórum permanente, de contacto e intercâmbio, propiciando a discussão de tendências na cibercriminalidade e na obtenção de prova digital.

E.6. INTERVENÇÃO NA XXIV ASSEMBLEIA-GERAL DA AIAMP - CRIAÇÃO DA CiberRede / *CiberRed*

93. Como se referiu, decorreu entre 10 e 11 de outubro de 2016, a XXIV Assembleia-Geral da AIAMP, em Lisboa, sob os auspícios da Procuradoria-Geral da República de Portugal.

Fez parte da respetiva agenda, no dia 10 de outubro, uma sessão destinada à "Apresentação e aprovação da Rede Cibercrime", a cargo de Portugal. No decurso dessa sessão introduziu-se o documento de conceito (que acima se referiu e se junta como Anexo 27).

CiberRede
REDE IBERO-AMERICANA DE MINISTÉRIOS PÚBLICOS ESPECIALIZADOS EM CIBERCRIME
RED IBEROAMERICANA DE FISCALES ESPECIALIZADOS EN CIBERDELINCUENCIA
CiberRed

105. Após esta apresentação, a Assembleia-Geral da AIAMP, por unanimidade, aprovou a constituição da CiberRede / *CiberRed,* nos termos propostos no documento de conceito, portanto como uma rede de magistrados especializados, com vocação para a intensificação do relacionamento entre os Ministérios Públicos na área da cibercriminalidade e da obtenção de prova digital, bem como para a facilitação da troca de experiências e de boas práticas.

Deliberou ainda a Assembleia-Geral que a coordenação desta rede seria assegurada por Portugal e que a Secretaria Geral da *IberRed* apoiaria esta coordenação na implementação das atividades futuras, bem como assumiria o encargo de integrar a Rede na *Iber@.* Além disso, deliberou ainda que se realizasse uma reunião fundadora da CiberRede / *CiberRed* durante o primeiro trimestre de 2017, já com a participação dos pontos de contacto entretanto indicados. Os temas desta primeira reunião seriam, como temática estratégica específica, o "cibercrime no espaço Ibero-Americano - os fenómenos criminais e a legislação"; como outros assuntos, deveriam definir-se os objetivos estratégicos da CiberRede / *CiberRed* para o próximo triénio e ainda fixar a temática estratégica específica e o formato da subsequente reunião.
Até ao encerramento da reunião, indicaram representantes para integrarem esta rede 17 das 21 Procuradorias-Gerais associadas na AIAMP.

E.7. INTERVENÇÃO NO XIV ENCONTRO DE PROCURADORES-GERAIS DA CPLP - CRIAÇÃO DO FORUM LUSÓFONO SOBRE CIBERCRIME E PROVA DIGITAL

94. Decorreu, em Lisboa, na Procuradoria-Geral da República, entre 13 e 14 de outubro 2016, o XIV Encontro de Procuradores-Gerais da CPLP.
Foi solicitado ao Gabinete Cibercrime que interviesse no mesmo, numa sessão específica, agendada para o dia 14 de outubro, sobre "Cibercrime e prova digital no espaço CPLP. Manifestações mais frequentes de cibercriminalidade. Criação de uma rede de pontos de contacto". A apresentação efetuada abordou ainda a temática das necessidades legislativas no espaço CPLP- PALOP, em sede de crimes na Internet.

95. Pretendia-se ainda que no decurso dessa sessão fosse discutida a criação, entre as Procuradorias-Gerais da CPLP, de uma estrutura de coordenação na área do cibercrime e da obtenção de prova digital. O impulso nesse sentido resultou da verificação de que, reconhecendo-se que as atividades ilícitas nas redes de comunicações são alheias aos conceitos de território, nacionalidade ou jurisdição, desconhecem fronteiras, podendo ser perpetradas a partir de qualquer ponto do globo, contra vítimas em qualquer ponto do globo, não obstante, encontram na língua uma das últimas fronteiras. A língua constitui um dos motivos mais importantes que levam os cibercriminosos a escolher e estabelecer contacto com as vítimas dos seus atos. Esta conclusão cria a necessidade de fortalecer a cooperação, nesta matéria, entre países que partilhem a mesma língua.
Por outro lado, é bem-sabido que, no contexto global, apenas se poderão alcançar resultados efetivos na luta contra a cibercriminalidade com uma atuação especializada, coordenada, articulada e ágil. Porém, é igualmente verdade que esta especialização, coordenação e articulação somente são possíveis em ambientes de confiança e de partilha de informação.
Este foi o contexto que levou à proposta de criação, no âmbito dos Ministérios Públicos dos Países Lusófonos, de um fórum de magistrados especializados, onde participassem representantes de todas as Procuradorias-Gerais.

96. Tendo em vista a sua discussão a aprovação pelos Procuradores-Gerais, foi apresentada uma proposta de deliberação a este propósito, que se junta como Anexo 61.

Este documento veio a ser aprovado, sendo assim deliberada a criação do Fórum Lusófono sobre Cibercrime e prova Digital, com o objetivo de partilhar informação e conhecimento sobre os quadros jurídicos dos diversos países lusófonos, no âmbito da cibercriminalidade, bem como facilitar o intercâmbio de experiências e boas práticas processuais necessárias com vista à ultrapassagem dos múltiplos problemas técnicos e jurídicos com que os magistrados se defrontam nesta área, dos crimes informáticos e cometidos com o auxílio das tecnologias e das redes de informação e comunicação.

Foi ainda deliberado que este fórum permanente, de contacto e intercâmbio, fosse corporizado por pontos de contacto de cada uma das Procuradorias-Gerais, que deveriam realizar uma reunião anual, que permitisse a partilha de eventuais atualizações legislativas ou operacionais que tenham ocorrido em cada um dos países e também a discussão de novas práticas e métodos de investigação criminal nesta matéria. Nestas reuniões anuais discutir-se-ão também temas específicos, como a formação e especialização de magistrados, a harmonização legislativa entre os países lusófonos ou a adesão a instrumentos internacionais.

Deliberaram ainda os Procuradores-Gerais que o fórum deverá explorar possibilidades de criação de uma plataforma *online* de partilha de informação (legislativa e jurisprudencial, por exemplo) e de auxílio ao trabalho dos magistrados, na investigação e prossecução criminal nesta área.

E.8. ACOMPANHAMENTO DA ATIVIDADE DO COMITÉ NACIONAL DA CAMPANHA MOVIMENTO CONTRA O DISCURSO DE ÓDIO – JOVENS PELOS DIREITOS HUMANOS *ONLINE*

97. O Gabinete Cibercrime foi solicitado a participar em reunião do Comité da Campanha Contra o Discurso do Ódio, pela dimensão e importância que tem a vertente *online* do discurso do ódio. Posteriormente, veio a ser solicitado que o Ministério Público passasse a integrar em permanência o Comité da Campanha. Foi superiormente determinado que assim acontecesse.

Esta Campanha é uma iniciativa do Instituto Português do Desporto a Juventude, mas integrada numa muitíssimo mais alargada iniciativa, promovida pelo Conselho da Europa. Na verdade, na sua vertente nacional, a Campanha é apenas a materialização interna de um projeto que se desenrola em muitos outros Estados Membros do Conselho da Europa.

Integram o Comité da Campanha várias outras instituições e entidades públicas e privadas, designadamente, o Ministério da Educação (Direção Geral da Educação), Comissão da Igualdade de Género, Alto Comissariado para as Migrações, Ministério dos Negócios Estrangeiros (Comissão Nacional da Unesco), Fundação para a Ciência e a Tecnologia (Centro Internet Segura), Fundação Calouste Gulbenkian, Cooperativa Movijovem, Associação Nacional de Professores, Associação Portuguesa de Ética e Filosofia, Federação Nacional das Associações Juvenis, ILGA Portugal, Associação Bué Fixe, Juventude Cruz Vermelha e Associação Dínamo, entre outras.

No seio do Comité existe um grupo de trabalho, mais reduzido, que operacionaliza com mais proximidade os trabalhos. Esse grupo de trabalho, de voluntários, incluiu representantes do IPDJ e ainda da Direção Geral da Educação, da Comissão da Igualdade de Género, da Fundação Gulbenkian, da ILGA Portugal, da Associação Bué Fixe, da Juventude Cruz Vermelha e da Associação Dínamo.

98. A Campanha, que é essencialmente de divulgação pública, tem como ideia de fundo a necessidade de educação para os direitos humanos no contexto do discurso de ódio. Esta necessidade educativa pretende enquadrar em democracia o discurso de ódio, como um abuso dos direitos humanos. É ainda propósito da Campanha a implementação de ferramentas que permitam detetar e denunciar o discurso do ódio, bem como difundir ferramentas existentes de combate a este fenómeno. Pretende atingir-se este desiderato por via da promoção da literacia para os *media* e para a cidadania digital, bem como por via da promoção do envolvimento dos jovens na governança da Internet.

Existe interesse do Ministério Público em acompanhar a temática do combate ao discurso do ódio e às suas manifestações, sobretudo quando *online*. Este interesse tem repercussão na área criminal, mas também na área das crianças e jovens. Aliás, o Ministério Púbico empreendeu já iniciativas passadas nesta área - em especial, o Plano de Ação sobre Crimes Contra Crianças na Internet, que decorreu em 2013 e 2014 e os colóquios sobre comentários em meios de comunicação *online*, realizados no final de 2013.

E.9. VISITA DE DELEGAÇÃO TURCA À PROCURADORIA-GERAL DA REPÚBLICA

99. A 21 de janeiro de 2016, a Procuradoria-Geral da República foi visitada por representantes do Ministério da Justiça da Turquia, sendo recebidos no Gabinete Cibercrime. O propósito da visita era especificamente contribuir para a discussão da reforma da legislação turca na área do cibercrime, ao encontro das boas práticas no seio da União Europeia e das previsões da Convenção de Budapeste – Convenção sobre Cibercrime do Conselho da Europa.

A pedido da delegação, a agenda da reunião inclui apresentações sobre o marco legal português na área da cibercrimalidade e sobre as atividades do Gabinete Cibercrime da PGR. Junta-se o programa da visita, como Anexo 28.

E.10. VISITA DO *FISCAL GENERAL* DE CUBA À PROCURADORIA-GERAL DA REPÚBLICA

100. A 13 e 14 de outubro de 2016, decorreu uma visita oficial da *Fiscalia General* de Cuba à Procuradoria-Geral da República, sendo a respetiva delegação composta pelo *Fiscal General*, Dario Delgado Cura e pela Diretora da Cooperação Internacional da *Fiscalia*, Patricia Rizo Cabrera. No âmbito dessa visita teve lugar uma reunião com o Gabinete Cibercrime, no dia 13 de outubro.

Foi solicitado ao Gabinete Cibercrime que efetuasse uma breve explicação do contexto nacional em matérias de cibercriminalidade e, também, das atividades do Gabinete.

E.11. PARTICIPAÇÃO NAS III JORNADAS JURÍDICAS DO MINISTÉRIO PÚBLICO DE MOÇAMBIQUE

101. Decorreram, entre 19 e 21 de setembro de 2016, as III Jornadas Jurídicas do Ministério Público de Moçambique, nas instalações da Procuradoria-Geral da República de Moçambique, em Maputo, submetidas ao tema *Por um Ministério Público mais Eficiente na Defesa da Legalidade*.
Foi solicitado ao Gabinete Cibercrime que representasse o Ministério Público de Portugal nesta reunião. Junta-se o relatório a este propósito elaborado como Anexo 65.
Esta participação inseriu-se num contexto de cooperação e troca de experiências entre a PGR e o Ministério Público de Moçambique, que assumiu os custos desta participação. No convite, foi manifestado interesse específico em que se incluísse na agenda das Jornadas uma comunicação sobre a experiência portuguesa na prevenção e combate ao crime informático.

102. Por essa razão, focou-se a intervenção no quadro legislativo português, bem como na estrutura e funções do Gabinete Cibercrime e nas experiências realizadas pela Procuradoria-Geral da República na interação com os fornecedores de serviço Internet globais (Facebook, Google e Microsoft). Por outro lado, abordou-se a forma como a legislação moçambicana encara os crimes no ciberespaço – a este propósito, foi referido que está em curso a revisão do Código Penal (já em sede parlamentar) e a do Código de Processo Penal, sendo informalmente solicitada a cooperação da Procuradoria-Geral de Portugal, na eventual formulação de sugestões, ao poder legislativo moçambicano, pela Procuradoria-Geral de Moçambique. Foi manifestada a total disponibilidade para o efeito.

F. PARTICIPAÇÃO EM OUTRAS ATIVIDADES EXTERNAS

103. Foi o Gabinete Cibercrime solicitado a participar – e participou –, em ações e reuniões promovidas por outras entidades. Fê-lo em representação do Ministério Público e, por vezes, a título próprio. Entre outros, o Gabinete participou, com intervenções, nos eventos que de seguida se referem.

F.1. PROJETO VISIT (*VICTIM SUPPORT FOR IDENTITY THEFT*)

104. A Procuradoria-Geral da República foi solicitada para participar, a 15 de outubro de 2015, numa reunião, em Lisboa, do Projeto VISIT (*Victim Support for Identity Theft*). Trata-se de um projeto desenvolvido, pela Guarda Nacional Republica, com financiamento da União Europeia, em parceria com a Universidade de Jyväskylä, da Finlândia, a Universidade de Ciências Aplicadas de Lübeck, da Alemanha, a Associação PUAC, do Reino Unido e o Result Group, da Alemanha.

Nesta reunião, de Lisboa, promovida pela Guarda Nacional Republicana em colaboração com os restantes parceiros do projeto VISIT, foi solicitado ao Gabinete Cibercrime que fizesse uma apresentação sobre "*The Portuguese Legal framework on Identity Theft*".

F.2. SEMINÁRIO "CONTRA O DISCURSO DE ÓDIO *ONLINE*"

105. A Procuradoria-Geral da República foi solicitada para participar no seminário "Contra o Discurso de Ódio *online*", promovido pelo Instituto Português do Desporto e Juventude, a 23 de outubro de 2015, em Lisboa. Pedia-se a intervenção num painel dedicado ao tema "*Discurso de Ódio no ciberespaço, extremismo violento e cibersegurança*".

F.3. EXERCÍCIO CIBER PERSEU 2015

106. A Procuradoria-Geral da República foi solicitada para participar no exercício CIBER PERSEU 2015, tendo efetivamente participado na respetiva sessão de encerramento, que decorreu a 26 de novembro de 2015. Trata-se de um exercício militar na área da cibersegurança, promovido pela Academia Militar, na Amadora, com a participação de diversas entidades públicas da área da segurança e da defesa, mas também de operadores de telecomunicações.

F.4. VII FORUM TÉCNICO FORENSE "A BUSCA DO VESTÍGIO EM AMBIENTE DIGITAL"

107. A Procuradoria-Geral da República foi solicitada para participar no VII Fórum Técnico Forense - "A busca do vestígio em ambiente digital", organizado pela Polícia de Segurança Pública, no Instituto Superior de Ciências Policiais e Segurança Interna, o qual decorreu a 2 de dezembro de 2016.

O Gabinete Cibercrime participou, sendo representado pelo Sr. Dr. Rui Batista, membro do Gabinete da Procuradora-Geral, que apresentou o tema "*Meios Processuais de Obtenção de Prova em ambiente digital: a Lei do Cibercrime*".

F.5. "*JURIX 2015 (28TH INTERNATIONAL CONFERENCE ON LEGAL KNOWLEDGE AND INFORMATION SYSTEMS)*"

108. O Gabinete Cibercrime foi solicitado para participar – e participou – num *workshop*, sobre "*Electronic Discovery and Digital Evidence*", integrado na JURIX 2015 (*28th International Conference on Legal Knowledge and Information Systems*), organizada pela Escola de Direito da Universidade do Minho. Este *workshop* veio a decorrer a 9 de dezembro de 2015, na Universidade do Minho, em Braga.

F.6. *WORKSHOP ON DATA RETENTION* e REUNIÃO DO *CONSULTATIVE FORUM OF PROSECUTORS GENERAL AND DIRECTORS OF PUBLIC PROSECUTIONS OF THE MEMBER STATES OF THE EUROPEAN UNION*

109. Decorreu, no dia 10 de dezembro de 2015, na Haia, o *Workshop on Data Retention*, promovido pela EUROJUST. De seguida, teve lugar o Fórum Consultivo de Procuradores-Gerais dos Estados Membros da União Europeia, que se realizou a 11 de dezembro, no mesmo local. O Gabinete Cibercrime foi solicitado a participar no primeiro, em representação da Procuradoria-Geral da República. Por outro lado, foi solicitado a assistir à participação no segundo, acompanhando o Senhor Vice-Procurador-Geral da República.

A temática do *workshop* respeitava aos efeitos do Acórdão do Tribunal de Justiça da União Europeia de 8 de abril de 2014, que anulou a chamada Diretiva Europeia de Retenção de Dados. Este era também o tema de uma das sessões do Fórum, razão pela qual o subscritor nele participou.

110. Do *workshop* retiram-se ideias genéricas, mas firmes, que vieram a ser apresentadas como conclusões no decurso do Fórum. Assim, desde logo, foi sublinhada a necessidade de existir retenção de dados, como ferramenta auxiliar de investigação criminal A sua falta, nos países que a revogaram, tem privado as autoridades destes de uma importante fonte de informação e prova. Em todo o caso, esta retenção de dados deve ser circunscrita a processos de investigação no seio da justiça penal – não devendo ser permitida para fins de segurança nacional ou *inteligence*.
Foi igualmente assumido que, sendo a retenção imprescindível, aquilo que importa discutir não é a sua existência, mas antes as condições em que se processa: as salvaguardas de segurança na guarda e acesso, a destruição dos dados, após o período de retenção e o controlo judicial na sua utilização – designadamente pela restrição à investigação de crimes mais graves.
A Procuradoria-Geral da República foi solicitada para emitir a sua opinião, por escrito, sobre um dos pontos específicos em discussão, relacionado com os efeitos do Acórdão do Tribunal de Justiça da União Europeia de 8 de abril de 2014, que anulou a chamada Diretiva Europeia de Retenção de Dados. Em resposta a esta solicitação remeteram-se os comentários entendidos pertinentes, juntando-se os mesmos, agora, como Anexo 42.

F.7. CIBERSEGURANÇA – PERSPETIVAS MULTIDISCIPLINARES

111. A Procuradoria-Geral da República foi solicitada para participar na conferência "*Cibersegurança – perspetivas multidisciplinares*", a qual decorreu a 4 de janeiro de 2016, na Faculdade de Direito da Universidade de Lisboa. Era solicitado ao Ministério Público que, integrada num painel sobre "*A Política Europeia de Cibersegurança*", se fizesse uma apresentação sobre "*Cibercrime: o outro lado da cibersegurança – o quadro legal português*".

F.8. *WEBINAR* SOBRE CIBERCRIME EM AMBIENTE ESCOLAR

112. O Gabinete Cibercrime foi solicitado para colaborar com a Equipa de Recursos e Tecnologias Educativas do Ministério da Educação (estrutura integrada na Direção-Geral da Educação) na dinamização de um *webinar* cujos destinatários são os professores do ensino público. Em concretização desta colaboração, veio a ser gravada uma sessão em vídeo, que foi depois disponibilizada na Internet, a 11 de fevereiro de 2016 (em http://webinar.dge.mec.pt/2016/02/11/cibercrime-no-ambiente-escolar/). O conteúdo de tal sessão foi repristinado a partir das sessões do Plano de Ação sobre Crimes Contra Crianças na Internet, desenvolvido entre 2013 e 2014 pelo Gabinete Cibercrime.

F.9. *"ELECTRONIC EVIDENCE IN CRIMINAL PROCEEDINGS - COLLECTION, ANALYSIS AND PRESENTATION OF E-EVIDENCE IN COURT"*

113. O Gabinete Cibercrime foi solicitado para participar no curso "*Electronic Evidence in Criminal Proceedings*", organizado pela ERA (*Europäische Rechtsakademie*) no Centro de Estudos Judiciários,

a 29 de fevereiro e 1 de março de 2016. Foi solicitado ao Gabinete Cibercrime que fizesse uma apresentação enquadrada um painel sobre "*Computer Forensics and Electronic Evidence*".

F.10. "*PROTEÇÃO CIVIL, VIGILÂNCIA E SEGURANÇA – O CONTRIBUTO DOS DRONES*"

114. O Gabinete Cibercrime foi solicitado para colaborar na conferência "*Drones: o futuro nas nossas mãos*", no âmbito do evento *iDrone Experience*, no Parque de Exposições de Braga, o qual decorreu a 22 de abril de 2016. Interveio nessa conferência, no painel "*Proteção civil, vigilância e segurança: o contributo dos drones*", Nuno Serdoura dos Santos, à data Procurador-adjunto no DIAP do Porto e Ponto de Contacto do Gabinete Cibercrime naquela comarca (e ainda membro do Grupo Técnico de apoio ao Gabinete Cibercrime).

F.11. "*CONSEDE – CONGRESSO SEGURANÇA E DEMOCRACIA*"

115. O Gabinete Cibercrime foi solicitado para participar no "*CONSEDE – Congresso Segurança e Democracia*", que decorreu na Universidade Nova de Lisboa, a 2 e 3 de maio de 2016. Trata-se de um evento académico, com propósitos de realização científica, que tem reunido anualmente especialistas nos temas de Direito, Segurança e Democracia. Pediu-se ao Gabinete Cibercrime que fizesse uma apresentação num painel sobre "*Cibersegurança: que desafios à estratégia nacional de segurança no ciberespaço?*"

F.12. CURSO GERAL DE CIBERSEGURANÇA

116. Como já acima se referiu, no contexto da articulação com o Centro Nacional de Cibersegurança, o Gabinete Cibercrime participou e interveio no Curso Geral de Cibersegurança, organizado pelo CNCS, a 17 de maio de 2016.

Este Curso Geral de Cibersegurança assume uma perspetiva que apelida de "*whole-of-society*". Na verdade, o Centro Nacional de Cibersegurança tem pretendido, no âmbito das suas atribuições, promover a formação e qualificação de recursos humanos na área da Cibersegurança, uma vez que entende ser a qualificação e o reforço de competências nacionais de cibersegurança determinantes para a capacidade nacional nesta matéria.

Foi solicitado ao Gabinete Cibercrime que efetuasse uma apresentação sobre a temática da "*Regulação do Ciberespaço e enquadramento normativo da Cibersegurança - Legislação do Cibercrime*".

F.13. *STRATEGIC SEMINAR "KEYS TO CYBERSPACE"*

117. O Gabinete Cibercrime participou, em representação da Procuradoria-Geral da República, no "*Strategic Seminar Keys to Cyberspace*", organizado pela EUROJUST, que decorreu no dia 2 de junho de 2016, na Haia. Como já acima se deixou expresso, esta reunião congregou representantes dos Estados Membros da União Europeia, com experiência prática em cibercrime, com o objetivo de identificar e encontrar possíveis soluções para os desafios da investigação e prossecução de casos concretos nesta área. Como também acima se referiu, junta-se o relatório que a este propósito se elaborou, como Anexo 20.

Quanto às temáticas abordadas, genericamente incluíram a jurisdição no ciberespaço, em especial em relação com os fenómenos da chamada *cloud*, a cooperação com fornecedores de serviço Internet sedeados nos Estados Unidos da América e a encriptação de dados. Uma das sessões, especial, focou-se, como acima se descreveu, na criação da Rede Judicial Europeia para

matérias do Cibercrime, tendo em vista apresentar conclusões, para discussão e aprovação no Conselho de Ministros das áreas Justiça e Administração Interna (JAI) da União Europeia que se realizaria a 9 e 10 de Junho de 2016.

F.14. *"EXPERT MEETING ON PRINCIPLES AND OPTIONS FOR AN E-EVIDENCE EXCHANGE PLATFORM"*

118. Decorreu em Bruxelas, a 9 de novembro de 2016, em instalações da Comissão Europeia, uma reunião de peritos nacionais sobre *Principles and options for an e-evidence exchange platform*. Tratou-se de uma reunião exploratória, na qual a Comissão pretendia aperceber as sensibilidades dos Estados Membros da União Europeia quanto ao estabelecimento de uma plataforma eletrónica que permita trocar, dentro da União Europeia, pedidos de cooperação judiciária referentes a prova eletrónica, no quadro da futura Decisão Europeia de Investigação.
O Gabinete Cibercrime participou, conjuntamente com a Sra. Dra. Carla Botelho, da Divisão de Cooperação Judiciária Internacional da Procuradoria-Geral da República, em representação do Ministério da Justiça de Portugal (Direção-Geral da Política de Justiça).

119. A agenda foi essencialmente preenchida com a discussão de um documento previamente preparado pela Comissão Europeia (*Principles and options for an e-evidence exchange platform - Discussion paper prepared by DG Justice and Consumers for the Expert Group on e-evidence*). Junta-se, como Anexo 69, o relatório a este propósito elaborado.

F.15. CONFERÊNCIA ANUAL DE CIBERSEGURANÇA – C-DAYS 2016

120. O Gabinete Cibercrime participou, em representação da Procuradoria-Geral da República, na Conferência Anual de Cibersegurança C-Days 2016, em Lisboa, a 29 e 30 de novembro de 2016. Trata-se de um evento internacional organizado pelo Centro Nacional de Cibersegurança, no qual se debatem anualmente temáticas teóricas, práticas e organizativas a propósito da cibersegurança.

121. Foi solicitado ao Gabinete Cibercrime que participasse num dos painéis, abordando a temática da *responsible disclosure*, com isto se tendo em referência o quadro legal envolvente da descoberta, pelos chamados *hackers éticos*, de vulnerabilidades de sistemas informáticos e de eventuais divulgações das mesmas, bem como dos limites legais deste tipo de atuação.

ANEXOS

ANEXO 1

Nota Prática 7

NOTA PRÁTICA nº 7 / 2015
30 de Dezembro de 2015

Retenção de dados de tráfego e Lei nº 32/2008, de 17 de Julho

Pretende-se com esta nota prática dar conta da discussão jurídica, em Portugal e na Europa, a propósito da obrigação de os operadores de comunicações procederem à retenção de dados. Esta questão foi suscitada pelo Acórdão do Tribunal de Justiça da União Europeia de 8 de Abril de 2014. No caso específico português supõe ponderar se está em vigor, ou não, a Lei nº 32/2008, de 17 de Julho.

1.

A Lei nº 32/2008, de 17 de Julho, transpôs para o ordenamento jurídico português a chamada Diretiva Europeia de Retenção de Dados[1]. Este diploma legal nacional, em cumprimento da obrigação de transposição daquela Diretiva, veio obrigar os operadores de comunicações a proceder à retenção de dados (designadamente de tráfego).

O Acórdão do Tribunal de Justiça da União Europeia de 8 de Abril de 2014, no chamado caso *Digital Rights Ireland*[2], declarou inválida a Diretiva de Retenção de Dados.

2.

É pacificamente aceite a necessidade da retenção de dados, como ferramenta auxiliar de investigação criminal. A sua falta, naqueles países onde a mesma não tem consagração legal, tem privado as autoridades criminais e judiciárias de uma importante fonte de informação e prova. É também assumido que esta retenção

[1] Diretiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de Março de 2006, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações

[2] Processos apensos C 293/12 e C 594/12, respetivamente *Digital Rights Ireland Ltd* (C 293/12) contra *Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána*, Irlanda, *The Attorney General*, sendo intervenientes: *Irish Human Rights Commission*, e *Kärntner Landesregierung* (C 594/12), Michael Seitlinger, Christof Tschohl e outros.

de dados deve ser primacialmente circunscrita a processos de investigação criminal, no seio da justiça penal – não é consensualmente admitido que seja utilizável para fins de segurança nacional ou *inteligence*.

É igualmente assumido que, sendo a retenção de dados (em especial de tráfego) imprescindível, aquilo que importa discutir não é a sua existência, mas antes as condições em que se processa: as salvaguardas de segurança na guarda e acesso, a destruição dos dados, após o período de retenção e o controlo judicial na sua utilização – designadamente pela restrição à investigação de crimes mais graves.

O próprio texto do Acórdão do Tribunal de Justiça da União Europeia de 8 de Abril de 2014 é explícito neste sentido, da necessidade da retenção, regulamentada, de retenção de dados.

3.

Não obstante, na sequência daquele acórdão do TJUE, por decisão parlamentar ou de tribunais constitucionais, 10 dos Estados-Membros da União Europeia vieram a declarar inválidas as leis nacionais que transpunham a Diretiva de Retenção de Dados. Noutros 16 Estados-membros, pelo contrário, não aconteceu assim. Nestes últimos, tem sido sustentado, por um lado, que a validade formal das leis domésticas não foi posta em causa; por outro lado, que as exigências substanciais da deliberação do Tribunal do Luxemburgo, de uma forma ou outra, estavam previamente satisfeitas.

4.

Portugal é um dos 16 Estados-Membros nos quais se tem entendido que a decisão de 8 de Abril de 2014 não interferiu no quadro legal vigente. Com efeito, desde logo no campo legislativo, não foi sentida necessidade de introdução de qualquer alteração normativa – não foi mesmo apresentada, até à data, nenhuma iniciativa legislativa a este propósito.

Quanto à jurisprudência respeitante à aplicação prática da Lei nº 32/2008, a mesma é muito escassa. Além disso, nenhuma das decisões conhecidas de tribunais superiores portugueses se pronunciou especificamente quanto ao impacto do Acórdão de 8 de Abril na lei portuguesa. Assim aconteceu com as decisões proferidas durante 2015 pelos tribunais superiores a este propósito, que são apenas três, todas elas do Tribunal da Relação de Évora: o Acórdão de 6 de Janeiro de 2015, no processo 6793/11.2TDLSB-A.E1, o Acórdão de 20 de Janeiro de 2015, no processo 648/14.6GCFAR-A.E1 e o Acórdão de 19 de Maio de 2015, no processo 54/15.5GCBNV-A.E1. Em todas estas deliberações se refere a Lei 32/2008, que é aplicada ao caso concreto, assumindo-se portanto que está em vigor. Todas são muito posteriores à decisão de 8 de Abril de 2014. Todavia, em nenhuma delas, de forma alguma, se põe em causa a validade da lei.

5.

A específica questão objeto de deliberação pelo TJUE não foi, desde Abril de 2014 até ao presente, especificadamente submetida aos tribunais portugueses – sem prejuízo de poder, naturalmente, ainda vir a sê-lo no futuro. Afigura-se porém que o não foi até agora porque o entendimento comum, pacificamente partilhado pela comunidade judiciária e pelos operadores de telecomunicações, é o de que a Lei 32/2008 está em vigor.

É importante sublinhar que a Lei 32/2008, além da transposição da Diretiva 2006/24/CE, introduziu um mais alargado quadro, muito complexo, de regulamentação do processo de retenção de dados (por exemplo, entre outras, as regras que devem ser observadas na retenção, as pessoas habilitadas a aceder os dados ou as condições de armazenamento e de acesso aos dados). Neste exercício, a lei nacional foi muito para lá das exigências da Diretiva. Desta forma, a maior parte das exigências que vieram a ser feitas pelo acórdão do TJUE estariam já anteriormente consideradas no direito interno. Por essa razão, tem sido entendido que a decisão do tribunal do Luxemburgo não afeta a validade da lei nacional.

Como exemplo do que se disse, a lei portuguesa estipula condições de acesso aos dados, exigindo que a divulgação seja precedida de ordem de um juiz (Artigo 9º, nº 1, da Lei nº 32/2008). Esta condição coincide com a exigência do Tribunal de Justiça, quando declara e tira consequências negativas do facto de a Diretiva não prever, no acesso aos dados, a exigência de autorização de uma autoridade independente.

Por outro lado, o Tribunal valora negativamente a circunstância de a Diretiva não prever a obrigação de destruir os dados após o período de retenção. A lei portuguesa estatui exatamente o oposto, impondo a destruição dos dados após o período de retenção (artigo 7º, nº 1, alínea e, da Lei nº 32/2008).

Em relação à conservação dos dados, o TJUE sublinhou também a falta de requisitos reguladores da mesma. Mais uma vez, a lei portuguesa prevê regras que traduzem importantes salvaguardas a este propósito (por exemplo, definindo quem são aqueles que estão autorizados a aceder os dados, as estritas condições de armazenamento e outros).

Estas considerações, aplicadas a Portugal, foram confirmadas, no âmbito europeu, pelas conclusões da 10ª Reunião do *Consultative Forum of Prosecutors General of the Member States of the European Union*, realizada na Haia, a 11 de Dezembro de 2015[3].

[3] Nesta reunião todos os presentes, procuradores-gerais europeus ou seus representantes, foram unânimes em considerar a retenção de dados uma ferramenta essencial na investigação criminal, reconhecendo-se, embora, haver necessidade de a submeter a condições (salvaguardas e garantias): desde logo, a limitação a formas sérias de criminalidade; depois, a sujeição do acesso a uma autoridade judicial, independente; em terceiro lugar, à circunstância de os dados retidos serem conservados em segurança, de forma regulada, dentro da União Europeia. Por outro lado, a fixação mais rigorosa de um período de retenção, bem como a ulterior destruição dos dados retidos foram apontados como condicionalismos necessários. O *Consultative Forum* apelou mesmo a uma nova iniciativa europeia a este propósito, como forma de, após a decisão do TJUE de 8 de Abril de 2014, se repor o equilíbrio entre o direito à privacidade, por um lado, e o direito à segurança dos cidadãos, por outro.

6.

Sem embargo, é consensualmente reconhecido que algumas das condições descritas pelo acórdão do TJUE, pela sua natureza, serão objetivamente insuscetíveis de serem satisfeitas. Ou seja, o Tribunal de Justiça aponta para condições que não são viáveis ou que, sendo-o, tornam a retenção inútil. Assim, o Tribunal afirma que a retenção de dados não pode ser permitida no quadro da Diretiva, por ser indiscriminada (deveria, de acordo com o Tribunal, incidir apenas sobre alvos suspeitos de criminalidade grave) e, por outro lado, por os dados conservados não se referirem apenas a pessoas suspeitas, mas ao comum dos cidadãos. Além disso, o tribunal censura a retenção generalizada e indiscriminada de dados (e não a retenção de dados especificados), cobrindo toda a informação respeitante às comunicações, o que é visto como desproporcional.

7.

Sem prejuízo de todo o respeito que merece a decisão do Tribunal, afigura-se que aponta, com estas últimas questões, para uma discussão inconsistente e inconsequente. Na verdade, é o próprio Tribunal quem reconhece que a retenção de dados é necessária e útil. Porém, se assim é, a retenção de dados tem que ser indiscriminada, por um lado e tem que abranger todos os cidadãos, por outro. De facto, no momento em que os dados são retidos e conservados, não é possível saber se, porventura, aqueles dados poderão vir a ser necessários, como prova de um crime. Somente após ter ocorrido um crime, os dados entretanto retidos de forma generalizada e indiscriminada assumirão valor probatório. Nos casos em que há um suspeito já identificado em investigação, existem outros instrumentos para obter a informação a ele respeitante que venha a ser necessária (interceção de comunicações, por exemplo). É precisamente quando não se obteve previamente prova dos factos ou da identidade do suspeito que é útil o recurso a dados retidos – estes podem aliás ser a única forma de descobrir quem praticou um determinado crime. Porém, nessa altura, é necessário que os ditos dados estejam já retidos e conservados (todos os dados, em relação a todos os cidadãos). É por isso que a retenção de dados, tal como é entendida no quadro da Diretiva e da Lei nº 32/2008, apenas é útil se os dados se referirem a todos os cidadãos, de forma indiscriminada.

Aliás, por toda a Europa, de forma generalizada, a comunidade jurídica não tem conseguido alcançar, nesta parte, o sentido da decisão afirmação do Tribunal.

ANEXO 2

Nota Prática 8

NOTA PRÁTICA nº8/2016
17 de Fevereiro de 2016

Pedido de dados a operadores de comunicações

Pretende-se com esta nota prática, sumariamente, descrever as informações guardadas por operadores de comunicações (telefónicas e Internet), que podem vir a ser usadas em investigações criminais, bem como referenciar os fundamentos jurídicos que delimitam os pedidos dessas informações.

1. Dados em posse dos operadores

Em concretas investigações criminais, é cada vez mais frequente ser necessário obter informações de operadores de comunicações – sobretudo, referentes à identificação de quem efetuou uma determinada comunicação.

Os operadores de comunicações guardam informação:

- respeitante à identificação dos seus clientes (nome, morada, etc. - tradicionalmente conhecida como *dados de base*) e
- respeitante às comunicações efetuados por aqueles – os chamados *dados de tráfego*.

Os operadores não guardam – é proibido fazê-lo[1] –, o conteúdo das concretas comunicações. Obter o conteúdo de comunicações apenas é possível por via da interceção de comunicações, em *tempo real*, nos termos dos Artigos 187º e 188 do Código de Processo Penal e do Artigo 18º da Lei do Cibercrime.

2. Quadro legal

Estão simultaneamente em vigor três diplomas legais que regulam, em sede de processo penal, a obtenção de dados em posse de fornecedores de serviços de comunicações: o Código de Processo Penal (*maxime* o nº 2 do Artigo 189º), a Lei nº 32/2008, de 17 de Julho e, finalmente, a Lei do Cibercrime (Lei nº 109/2009, de

[1] Por força do nº 2 do Artigo 1º da Lei nº 32/2008, de 17 de Julho, que estipula que "a conservação de dados que revelem o conteúdo das comunicações é proibida" e também do nº 2 do Artigo 4º da Lei nº 41/2004, de 18 de Agosto, que proíbe, foram do contexto processual penal, a *escuta*, *interceção* e *armazenamento de comunicações*. Esta proibição decorria já dos Artigos 32º, nº 8 e 34º, nº 4, da Constituição da República.

15 de Setembro). Porém, nem sempre as respetivas redações são facilmente conjugáveis. Daqui resulta, por um lado, insegurança jurídica na aplicação da lei ao caso concreto. Por outro lado, tratando-se de regras sobre obtenção de prova, estas incertezas criam dúvida sobre a validade dos elementos probatórios eventualmente obtidos.

O Artigo 189º do Código de Processo Penal (que foi introduzido pela alteração de 2007 - Lei nº 48/2007, de 29 de Agosto) regula a obtenção em inquérito, entre outros, "de registos da realização de conversações ou comunicações". Determina que esta diligência probatória siga o regime processual das interceções de comunicações telefónicas.

Por sua vez, a Lei nº 32/2008, regulamenta a chamada conservação de dados de tráfego. Cria a obrigação, para os operadores, de conservarem dados dos seus clientes (entre eles, os de tráfego), pelo prazo de um ano. Instituiu um específico e especialíssimo regime processual de acesso a esses dados que, além do mais, faz depender o acesso aos mesmos de "despacho fundamentado do juiz de instrução, se houver razões para crer que a diligência é indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter no âmbito da investigação, deteção e repressão de crimes graves" (Artigo 9º, nº 1).

A conciliação destes três regimes não foi expressamente feita pelo legislador, exigindo assim esforço adicional do intérprete. Apenas ficou expressa a necessária convivência, com ambas em vigor, entre a Lei nº 32/2008 e a Lei do Cibercrime. Com efeito, no nº 2 do Artigo 11º da Lei do Cibercrime, determina-se que aquilo que nela se estipula *não prejudica* o regime da Lei nº 32/2008.

3. Dados de tráfego

Por aplicação das regras gerais da sucessão de leis no tempo, tem que concluir-se que o Artigo 189º do Código de Processo Penal foi parcelarmente revogado pela Lei do Cibercrime. Porém, apesar de ter sido substancialmente revogado, para o que agora está causa releva apenas que o trecho referente a *registos da realização de conversações ou comunicações*, incluído no nº 2 do Artigo 189º, se mantém em vigor. De facto, não foi nunca expressamente revogado. Por outro lado, o teor desta disposição não coincide com nenhuma outra, designadamente da Lei do Cibercrime, motivo pelo qual não operou a este específico propósito qualquer revogação tácita. Anote-se que também a Lei nº 32/2008 não produziu, neste aspeto em particular, qualquer revogação tácita, uma vez que, ao contrário do Código de Processo Penal, que é uma lei geral, esta lei de 2008 é especial – apenas se aplica à retenção de dados com a finalidade de investigação de uma gama muito reduzida de crimes.

Ou seja, a obtenção de dados de tráfego ou, no contexto telefónico, da chamada *faturação detalhada*, mantém-se regulada pelo Artigo 189º, nº 2 do Código de Processo Penal. É pois de acordo com este regime

que tem que processar-se a respetiva solicitação, à qual se aplica, por remissão, o regime de autorização das interceções telefónicas, previsto no Artigo 187º do Código de Processo Penal.

4. Dados de identificação dos clientes

Já quanto ao tipo de informação a que a doutrina e a jurisprudência chamam tradicionalmente *dados de base*, está atualmente referida no Artigo 14º da Lei do Cibercrime. Ali se diz que a solicitação aos operadores de comunicações / fornecedores de serviço de "*dados relativos aos seus clientes ou assinantes, neles se incluindo qualquer informação diferente dos dados relativos ao tráfego ou ao conteúdo*" é da competência da autoridade judiciária - o Ministério Público, portanto, no decurso do inquérito.

Neste conjunto de dados está porém incluída informação sobre o concreto endereço de IP utilizado numa determinada comunicação, já identificada na investigação. Ou seja, é igualmente da competência do Ministério Público solicitar aos operadores que indiquem a identidade do seu cliente que, num determinado contexto temporal (dia e hora) utilizou um determinado endereço IP. O mesmo raciocínio é aplicável à situação em que a investigação tem necessidade de saber qual o concreto endereço IP utilizado por um determinado cliente de um operador[2]. Assim, apesar de este tipo de informação ser tecnicamente agrupado na informação referente a tráfego, o regime jurídico da sua obtenção é o mesmo dos chamados *dados de base* (modernamente referidos como *dados relativos aos clientes*).

Anote-se que os dados aqui em causa terão que ser "*dados informáticos ou sob qualquer outra forma, detida pelo fornecedor de serviços*". Quer isto dizer, por um lado, que esta medida processual não se confunde com a preservação de dados nem com a revelação expedita de dados preservados – a preservação é proactiva e visa a conservação de dados que de outra forma não seriam conservados. Por outro lado, aquela fórmula legal quer dizer que o operador apenas está obrigado a fornecer aqueles dados que efetivamente detenha – e que detenha, naturalmente, dentro dos parâmetros legais.

5. Prazo de conservação dos dados

A conclusão que acaba de retirar-se requer, de quem solicita os dados, que conheça as condições e termos nos quais os operadores detêm os dados. Quanto à informação de tráfego (nela se incluindo, como se disse, os respeitantes à identificação do seu cliente que, em dadas circunstâncias temporais, usou um determinado IP), de forma simplificada, pode dizer-se que os operadores guardam os dados de acordo com dois diferentes regimes legais:

- o regime geral, previsto na Lei do Cibercrime, na Lei nº 41/2004 e no Artigo 189º, nº 2 do Código de Processo Penal e
- o regime especial, previsto na Lei nº 32/2008.

[2] Sobre este particular aspeto foram emitidas as Notas Práticas 1 e 2, para as quais se remete.

6. Regime especial da Lei nº 32/2008

A Lei 32/2008 prevê a obrigação de os operadores de comunicações conservarem dados de tráfego (entre outros) pelo período de um ano. Porém, estipula de forma expressa (Artigo 1º, nº 1), que tal conservação de dados é efetuada "para fins de investigação, deteção e repressão de crimes graves". Esta norma estabelece, de forma taxativa, corroborada pelo nº 1 do Artigo 3º da mesma Lei, que "a conservação e a transmissão dos dados têm por finalidade exclusiva a investigação, deteção e repressão de crimes graves". Por outro lado, o mesmo diploma fixa, no Artigo 2º, nº1, alínea g), que são crimes graves os "crimes de terrorismo, criminalidade violenta, criminalidade altamente organizada, sequestro, rapto e tomada de reféns, crimes contra a identidade cultural e integridade pessoal, contra a segurança do Estado, falsificação de moeda ou títulos equiparados a moeda e crimes abrangidos por convenção sobre segurança da navegação aérea ou marítima".

Portanto, em suma, além de vários outros requisitos, apenas podem solicitar-se estes dados, retidos ao abrigo da Lei 32/2008, se estiver em investigação um dos tipos de crime acima referenciados. Tal solicitação deve ser feita por ordem judicial, nos termos do Artigo 3º, nº 2 e do Artigo 9º da Lei nº 32/2008. Pela reduzida ocorrência prática de situações que possam aqui enquadrar-se, não se explora mais alargadamente este regime.

7. Regime geral

Fora do contexto da Lei nº 32/2008, não existe qualquer outro prazo específico para guarda de dados de tráfego. Porém, no seu conjunto, o quadro normativo permite aos operadores que conservem tais dados por seis meses. Ou seja, não se estando no âmbito de investigações de crimes referidos na Lei nº 32/2008, é pois de seis meses o prazo durante o qual os operadores podem dispor desses dados e, reflexamente, é esse o prazo durante o qual dispõem dos mesmos para os fornecer às autoridades de investigação criminal. A motivação jurídica desta conclusão é que a segue.

7.1.

O Artigo 4º, nº 2, da Lei nº 41/2004 estipula a proibição genérica de guarda de dados de tráfego, salvaguardando apenas as exceções determinadas pela própria lei. Esta proibição é corroborada pelo Artigo 6º, nº 1, da mesma Lei, que estipula que, "sem prejuízo do disposto nos números seguintes, os dados de tráfego relativos aos assinantes e utilizadores tratados e armazenados pelas empresas que oferecem redes e ou serviços de comunicações eletrónicas devem ser eliminados ou tornados anónimos quando deixem de ser necessários para efeitos da transmissão da comunicação". Ou seja, o quadro legal vigente determina, como princípio geral, a obrigação de eliminação de dados de tráfego logo que a comunicação terminar. Sublinhe-se

que esta disposição não está em conflito com a Lei nº 32/2008, que é posterior e, de forma clara, introduziu exceções adicionais a esta proibição.

7.2.

É o mesmo Artigo 6º da Lei nº 41/2004 que, nos números 2 e 3, introduz exceções a esta proibição do nº 1, estipulando que os dados de tráfego *necessários à faturação dos assinantes e ao pagamento de interligações* podem ser guardados e tratados até ao final do *período durante o qual a fatura pode ser legalmente contestada ou o pagamento reclamado*.

Este diploma não fixa este *período legal*, durante o qual o pagamento pode ser reclamado. Porém, a Lei nº 23/96, de 26 de Julho, diploma legal que define regras respeitantes à prestação de serviços públicos essenciais, já fixava no seu Artigo 10º, nº 1, que "o direito ao recebimento do preço do serviço prestado prescreve no prazo de seis meses após a sua prestação". Esta orientação é corroborada pelo nº 4 do mesmo Artigo 10º, que fixa igualmente em 6 meses o prazo para eventual propositura da ação pelo prestador de serviços. Recorde-se que o regime deste diploma é aplicável aos serviços de comunicações eletrónicas, por força do respetivo Artigo 1º, nº 2, alínea d).

Em suma, estando em causa a prestação de serviços de comunicações eletrónicas, o prazo que o fornecedor de serviço tem para reclamar o respetivo preço é de seis meses. Uma vez decorridos esses seis meses, tem efetiva aplicação a obrigação de eliminação dos dados de tráfego, fixada pelo Artigo 6º, nº 1 da Lei nº 41/2004. É também apenas nessa altura que se torna efetiva a proibição genérica de guarda de dados de tráfego, consagrada no Artigo 4º, nº 2, da mesma lei.

7.3.

Ou seja, por força da lei, depois de decorridos seis meses sobre uma determinada comunicação, os dados de tráfego por ela gerados têm que ser eliminados. Por essa razão, tais dados já não podem ser legalmente detidos pelos fornecedores de serviços.

Entre os dados que a autoridade judiciária está legitimada a solicitar, com fundamento no Artigo 14º, nº 4 da Lei do Cibercrime estão, como se disse, os dados de identificação e localização dos seus clientes – os tradicionalmente chamados *dados de base*. Quanto a estes, a lei não impõe qualquer prazo de guarda ou eliminação.

Esta norma legal, do Artigo 14º, nº 4 da Lei do Cibercrime, é também aquela que fundamenta a obtenção, em inquérito, do endereço de IP utilizado por um determinado cliente de um operador, desde que relacionado com uma concreta investigação. Porém, sendo o endereço de IP agrupado na categoria técnica de informação de tráfego, os operadores apenas o pode conservar por seis meses. Por isso, a autoridade judiciária apenas está legitimada a solicitar os dados referentes a comunicações que tenham ocorrido nos

seis meses anteriores ao pedido que é efectuado, uma vez que apenas esses dados podem ser legitimamente detidos pelo fornecedor de serviços.

8. Possibilidade de preservação dos dados

Importa ainda sublinhar que a lei prevê a possibilidade de preservar dados que estejam em risco de "deixar de estar disponíveis" (Artigo 12º, nº 1, da Lei do Cibercrime). Assim, se numa investigação em concreto se aperceber que determinados dados, incluindo dados de tráfego, estiverem em *risco de deixar de estar disponíveis*, é possível ordenar a "quem tenha disponibilidade ou controlo desses dados, designadamente a fornecedor de serviço, que preserve os dados em causa".

Esta possibilidade legal, que é expedita, é particularmente útil quando a investigação se apercebe de que o prazo de conservação de dados está próximo do seu termo. Pode mesmo ser despoletada por iniciativa de órgão de polícia criminal, "quando haja urgência ou perigo na demora" (Artigo 12º, nº 2 da Lei do Cibercrime).

Anexo – Legislação

Código de Processo Penal

Artigo 187º
Admissibilidade

1 - A intercepção e a gravação de conversações ou comunicações telefónicas só podem ser autorizadas durante o inquérito, se houver razões para crer que a diligência é indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter, por despacho fundamentado do juiz de instrução e mediante requerimento do Ministério Público, quanto a crimes:

a) Puníveis com pena de prisão superior, no seu máximo, a 3 anos;
b) Relativos ao tráfico de estupefacientes;
c) De detenção de arma proibida e de tráfico de armas;
d) De contrabando;
e) De injúria, de ameaça, de coacção, de devassa da vida privada e perturbação da paz e do sossego, quando cometidos através de telefone;
f) De ameaça com prática de crime ou de abuso e simulação de sinais de perigo; ou
g) De evasão, quando o arguido haja sido condenado por algum dos crimes previstos nas alíneas anteriores.

2 - A autorização a que alude o número anterior pode ser solicitada ao juiz dos lugares onde eventualmente se puder efectivar a conversação ou comunicação telefónica ou da sede da entidade competente para a investigação criminal, tratando-se dos seguintes crimes:

a) Terrorismo, criminalidade violenta ou altamente organizada;
b) Sequestro, rapto e tomada de reféns;
c) Contra a identidade cultural e integridade pessoal, previstos no título iii do livro ii do Código Penal e previstos na Lei Penal Relativa às Violações do Direito Internacional Humanitário;
d) Contra a segurança do Estado previstos no capítulo i do título v do livro ii do Código Penal;
e) Falsificação de moeda ou títulos equiparados a moeda prevista nos artigos 262º, 264º, na parte em que remete para o artigo 262º, e 267º, na parte em que remete para os artigos 262º e 264º, do Código Penal;
f) Abrangidos por convenção sobre segurança da navegação aérea ou marítima.

3 - Nos casos previstos no número anterior, a autorização é levada, no prazo máximo de setenta e duas horas, ao conhecimento do juiz do processo, a quem cabe praticar os actos jurisdicionais subsequentes.

4 - A intercepção e a gravação previstas nos números anteriores só podem ser autorizadas, independentemente da titularidade do meio de comunicação utilizado, contra:

a) Suspeito ou arguido;
b) Pessoa que sirva de intermediário, relativamente à qual haja fundadas razões para crer que recebe ou transmite mensagens destinadas ou provenientes de suspeito ou arguido; ou
c) Vítima de crime, mediante o respectivo consentimento, efectivo ou presumido.

5 - É proibida a intercepção e a gravação de conversações ou comunicações entre o arguido e o seu defensor, salvo se o juiz tiver fundadas razões para crer que elas constituem objecto ou elemento de crime.

6 - A intercepção e a gravação de conversações ou comunicações são autorizadas pelo prazo máximo de três meses, renovável por períodos sujeitos ao mesmo limite, desde que se verifiquem os respectivos requisitos de admissibilidade.

7 - Sem prejuízo do disposto no artigo 248º, a gravação de conversações ou comunicações só pode ser utilizada em outro processo, em curso ou a instaurar, se tiver resultado de intercepção de meio de comunicação utilizado por pessoa referida no n.º 4 e na medida em que for indispensável à prova de crime previsto no nº 1.

8 - Nos casos previstos no número anterior, os suportes técnicos das conversações ou comunicações e os despachos que fundamentaram as respectivas intercepções são juntos, mediante despacho do juiz, ao processo em que devam ser usados como meio de prova, sendo extraídas, se necessário, cópias para o efeito.

Artigo 189º
Extensão

1 - O disposto nos artigos 187º e 188º é correspondentemente aplicável às conversações ou comunicações transmitidas por qualquer meio técnico diferente do telefone, designadamente correio electrónico ou outras formas de transmissão de dados por via telemática, mesmo que se encontrem guardadas em suporte digital, e à intercepção das comunicações entre presentes.

2 - A obtenção e junção aos autos de dados sobre a localização celular ou de registos da realização de conversações ou comunicações só podem ser ordenadas ou autorizadas, em qualquer fase do processo, por despacho do juiz, quanto a crimes previstos no nº 1 do artigo 187º e em relação às pessoas referidas no nº 4 do mesmo artigo.

Lei nº 23/96, de 26 de Julho
Lei dos Serviços Públicos

Artigo 1º
Objecto e âmbito

1 - A presente lei consagra regras a que deve obedecer a prestação de serviços públicos essenciais em ordem à protecção do utente.
2 - São os seguintes os serviços públicos abrangidos:
…
d) Serviço de comunicações electrónicas;
…

Artigo 10º
Prescrição e caducidade

1 - O direito ao recebimento do preço do serviço prestado prescreve no prazo de seis meses após a sua prestação.
2 - Se, por qualquer motivo, incluindo o erro do prestador do serviço, tiver sido paga importância inferior à que corresponde ao consumo efectuado, o direito do prestador ao recebimento da diferença caduca dentro de seis meses após aquele pagamento.
3 - A exigência de pagamento por serviços prestados é comunicada ao utente, por escrito, com uma antecedência mínima de 10 dias úteis relativamente à data-limite fixada para efectuar o pagamento.
4 - O prazo para a propositura da acção ou da injunção pelo prestador de serviços é de seis meses, contados após a prestação do serviço ou do pagamento inicial, consoante os casos.
5 - O disposto no presente artigo não se aplica ao fornecimento de energia eléctrica em alta tensão.

Lei nº 41/2004, de 18 de Agosto
Lei da Proteção de Dados Pessoais e Privacidade nas Telecomunicações

Artigo 4º
Inviolabilidade das comunicações eletrónicas

1 - As empresas que oferecem redes e ou serviços de comunicações eletrónicas devem garantir a inviolabilidade das comunicações e respetivos dados de tráfego realizadas através de redes públicas de comunicações e de serviços de comunicações eletrónicas acessíveis ao público.
2 - É proibida a escuta, a instalação de dispositivos de escuta, o armazenamento ou outros meios de interceção ou vigilância de comunicações e dos respetivos dados de tráfego por terceiros sem o consentimento prévio e expresso dos utilizadores, com exceção dos casos previstos na lei.
3 - O disposto no presente artigo não impede as gravações legalmente autorizadas de comunicações e dos respetivos dados de tráfego, quando realizadas no âmbito de práticas comerciais lícitas, para o efeito de prova de uma transação comercial nem de qualquer outra comunicação feita no âmbito de uma relação contratual, desde que o titular dos dados tenha sido disso informado e dado o seu consentimento.
4 - São autorizadas as gravações de comunicações de e para serviços públicos destinados a prover situações de emergência de qualquer natureza.

Artigo 6º
Dados de tráfego

1 - Sem prejuízo do disposto nos números seguintes, os dados de tráfego relativos aos assinantes e utilizadores tratados e armazenados pelas empresas que oferecem redes e ou serviços de comunicações eletrónicas devem ser eliminados ou tornados anónimos quando deixem de ser necessários para efeitos da transmissão da comunicação.
2 - É permitido o tratamento de dados de tráfego necessários à faturação dos assinantes e ao pagamento de interligações, designadamente:
a) Número ou identificação, endereço e tipo de posto do assinante;
b) Número total de unidades a cobrar para o período de contagem, bem como o tipo, hora de início e duração das chamadas efetuadas ou o volume de dados transmitidos;
c) Data da chamada ou serviço e número chamado;
d) Outras informações relativas a pagamentos, tais como pagamentos adiantados, pagamentos a prestações, cortes de ligação e avisos.
3 - O tratamento referido no número anterior apenas é lícito até final do período durante o qual a fatura pode ser legalmente contestada ou o pagamento reclamado.
4 - As empresas que oferecem serviços de comunicações eletrónicas só podem tratar os dados referidos no nº 1 se o assinante ou utilizador a quem os dados digam respeito tiver dado o seu consentimento prévio e expresso, que pode ser retirado a qualquer momento, e apenas na medida do necessário e pelo tempo necessário à comercialização de serviços de comunicações eletrónicas ou à prestação de serviços de valor acrescentado.
5 - Nos casos previstos no nº 2 e, antes de ser obtido o consentimento dos assinantes ou utilizadores, nos casos previstos no n.º 4, as empresas que oferecem serviços de comunicações eletrónicas devem fornecer-lhes informações exatas e completas sobre o tipo de dados que são tratados, os fins e a duração desse tratamento, bem como sobre a sua eventual disponibilização a terceiros para efeitos da prestação de serviços de valor acrescentado.
6 - O tratamento dos dados de tráfego deve ser limitado aos trabalhadores e colaboradores das empresas que oferecem redes e ou serviços de comunicações eletrónicas acessíveis ao público encarregados da faturação ou da gestão do tráfego, das informações a clientes, da deteção de fraudes, da comercialização dos serviços de comunicações eletrónicas acessíveis ao público, ou da prestação de serviços de valor acrescentado, restringindo-se ao necessário para efeitos das referidas atividades.

7 - O disposto nos números anteriores não prejudica o direito de os tribunais e as demais autoridades competentes obterem informações relativas aos dados de tráfego, nos termos da legislação aplicável, com vista à resolução de litígios, em especial daqueles relativos a interligações ou à faturação.

Lei nº 32/2008, de 17 de Julho
Lei da Conservação de Dados Gerados ou Tratados no Contexto de Oferta de Serviços de Comunicações Eletrónicas

Artigo 1º
Objecto

1 - A presente lei regula a conservação e a transmissão dos dados de tráfego e de localização relativos a pessoas singulares e a pessoas colectivas, bem como dos dados conexos necessários para identificar o assinante ou o utilizador registado, para fins de investigação, detecção e repressão de crimes graves por parte das autoridades competentes, transpondo para a ordem jurídica interna a Directiva nº 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de Março, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações, e que altera a Directiva nº 2002/58/CE, do Parlamento Europeu e do Conselho, de 12 de Junho, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas.

2 - A conservação de dados que revelem o conteúdo das comunicações é proibida, sem prejuízo do disposto na Lei nº 41/2004, de 18 de Agosto, e na legislação processual penal relativamente à intercepção e gravação de comunicações.

Artigo 2º
Definições

1 - Para efeitos da presente lei, entende-se por:

…

g) «Crime grave», crimes de terrorismo, criminalidade violenta, criminalidade altamente organizada, sequestro, rapto e tomada de reféns, crimes contra a identidade cultural e integridade pessoal, contra a segurança do Estado, falsificação de moeda ou títulos equiparados a moeda e crimes abrangidos por convenção sobre segurança da navegação aérea ou marítima.

…

Artigo 3º
Finalidade do tratamento

1 - A conservação e a transmissão dos dados têm por finalidade exclusiva a investigação, detecção e repressão de crimes graves por parte das autoridades competentes.

2 - A transmissão dos dados às autoridades competentes só pode ser ordenada ou autorizada por despacho fundamentado do juiz, nos termos do artigo 9º.

3 - Os ficheiros destinados à conservação de dados no âmbito da presente lei têm que, obrigatoriamente, estar separados de quaisquer outros ficheiros para outros fins.

4 - O titular dos dados não pode opor-se à respectiva conservação e transmissão.

Artigo 9º
Transmissão dos dados

1 - A transmissão dos dados referentes às categorias previstas no artigo 4º só pode ser autorizada, por despacho fundamentado do juiz de instrução, se houver razões para crer que a diligência é indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter no âmbito da investigação, detecção e repressão de crimes graves.

2 - A autorização prevista no número anterior só pode ser requerida pelo Ministério Público ou pela autoridade de polícia criminal competente.

3 - Só pode ser autorizada a transmissão de dados relativos:

a) Ao suspeito ou arguido;

b) A pessoa que sirva de intermediário, relativamente à qual haja fundadas razões para crer que recebe ou transmite mensagens destinadas ou provenientes de suspeito ou arguido; ou

c) A vítima de crime, mediante o respectivo consentimento, efectivo ou presumido.

4 - A decisão judicial de transmitir os dados deve respeitar os princípios da adequação, necessidade e proporcionalidade, designadamente no que se refere à definição das categorias de dados a transmitir e das autoridades competentes com acesso aos dados e à protecção do segredo profissional, nos termos legalmente previstos.

5 - O disposto nos números anteriores não prejudica a obtenção de dados sobre a localização celular necessários para afastar perigo para a vida ou de ofensa à integridade física grave, nos termos do artigo 252º-A do Código de Processo Penal.

6 - As entidades referidas no nº 1 do artigo 4º devem elaborar registos da extracção dos dados transmitidos às autoridades competentes e enviá-los trimestralmente à CNPD.

Lei do Cibercrime - Lei nº 109/2009 de 15 de Setembro

Artigo 11º
Âmbito de aplicação das disposições processuais

1 - Com excepção do disposto nos artigos 18º e 19º, as disposições processuais previstas no presente capítulo aplicam-se a processos relativos a crimes:

a) Previstos na presente lei;

b) Cometidos por meio de um sistema informático; ou

c) Em relação aos quais seja necessário proceder à recolha de prova em suporte electrónico.

2 - As disposições processuais previstas no presente capítulo não prejudicam o regime da Lei nº 32/2008, de 17 de Julho.

Artigo 12º
Preservação expedita de dados

1 - Se no decurso do processo for necessário à produção de prova, tendo em vista a descoberta da verdade, obter dados informáticos específicos armazenados num sistema informático, incluindo dados de tráfego, em relação aos quais haja receio de que possam perder -se, alterar -se ou deixar de estar disponíveis, a autoridade judiciária competente ordena a quem tenha disponibilidade ou controlo desses dados, designadamente a fornecedor de serviço, que preserve os dados em causa.

2 - A preservação pode também ser ordenada pelo órgão de polícia criminal mediante autorização da autoridade judiciária competente ou quando haja urgência ou perigo na demora, devendo aquele, neste último caso, dar notícia imediata do facto à autoridade judiciária e transmitir -lhe o relatório previsto no artigo 253º do Código de Processo Penal.

3 - A ordem de preservação discrimina, sob pena de nulidade:

a) A natureza dos dados;

b) A sua origem e destino, se forem conhecidos; e

c) O período de tempo pelo qual deverão ser preservados,

até um máximo de três meses.

4 - Em cumprimento de ordem de preservação que lhe seja dirigida, quem tenha disponibilidade ou controlo sobre esses dados, designadamente o fornecedor de serviço, preserva de imediato os dados em causa, protegendo e conservando a sua integridade pelo tempo fixado, de modo a permitir à autoridade judiciária competente a sua obtenção, e fica obrigado a assegurar a confidencialidade da aplicação da medida processual.

5 - A autoridade judiciária competente pode ordenar a renovação da medida por períodos sujeitos ao limite previsto na alínea c) do n.º 3, desde que se verifiquem os respectivos requisitos de admissibilidade, até ao limite máximo de um ano.

Artigo 14º
Injunção para apresentação ou concessão do acesso a dados

1 - Se no decurso do processo se tornar necessário à produção de prova, tendo em vista a descoberta da verdade, obter dados informáticos específicos e determinados, armazenados num determinado sistema informático, a autoridade judiciária competente ordena a quem tenha disponibilidade ou controlo desses dados que os comunique ao processo ou que permita o acesso aos mesmos, sob pena de punição por desobediência.

2 - A ordem referida no número anterior identifica os dados em causa.

3 - Em cumprimento da ordem descrita nos nºs 1 e 2, quem tenha disponibilidade ou controlo desses dados comunica esses dados à autoridade judiciária competente ou permite, sob pena de punição por desobediência, o acesso ao sistema informático onde os mesmos estão armazenados.

4 - O disposto no presente artigo é aplicável a fornecedores de serviço, a quem pode ser ordenado que comuniquem ao processo dados relativos aos seus clientes ou assinantes, neles se incluindo qualquer informação diferente dos dados relativos ao tráfego ou ao conteúdo, contida sob a forma de dados informáticos ou sob qualquer outra forma, detida pelo fornecedor de serviços, e que permita determinar:

a) O tipo de serviço de comunicação utilizado, as medidas técnicas tomadas a esse respeito e o período de serviço;

b) A identidade, a morada postal ou geográfica e o número de telefone do assinante, e qualquer outro número de acesso, os dados respeitantes à facturação e ao pagamento, disponíveis com base num contrato ou acordo de serviços; ou

c) Qualquer outra informação sobre a localização do equipamento de comunicação, disponível com base num contrato ou acordo de serviços.

5 - A injunção prevista no presente artigo não pode ser dirigida a suspeito ou arguido nesse processo.

6 - Não pode igualmente fazer -se uso da injunção prevista neste artigo quanto a sistemas informáticos utilizados para o exercício da advocacia, das actividades médica e bancária e da profissão de jornalista.

7 - O regime de segredo profissional ou de funcionário e de segredo de Estado previsto no artigo 182º do Código de Processo Penal é aplicável com as necessárias adaptações.

ANEXO 3

Plano de Ação Cibercrime 2015-2016

CIBERCRIME

Plano de Ação do Ministério Público
2015 – 2016

Enquadramento

1. No documento de definição de *Objetivos Estratégicos trianuais e anuais do Ministério Público para 2015-2018*, o cibercrime e a prova digital foram apontados como *área prioritária*. Neste documento afirma-se que "*os crimes contra infraestruturas tecnológicas (contra a confidencialidade, integridade e disponibilidade de sistemas e dados) têm registado um significativo crescimento, pondo em causa o funcionamento de diversas instituições, públicas e privadas. Por outro lado, o recurso frequente a meios informáticos pelos agentes do crime, em especial o acesso à internet, tem criado particulares desafios à investigação criminal. Por via das redes de comunicação os criminosos têm possibilidade de agir à distância e de atingir um grande número de vítimas, dissimulando pelo ciberespaço os vestígios dessa atividade, em localizações e formatos que dificultam a respetiva deteção, abrangendo tais dificuldades todos os fenómenos criminais. A necessidade de obter elementos de prova em ambiente digital é partilhada por todas as jurisdições, com maior ênfase nas áreas criminais e de família e menores. Assim, o cibercrime e a obtenção de prova digital serão áreas estratégicas do Ministério Público para o próximo triénio*".

2. A Lei 72/2015, de 20 de Julho, que define os objetivos, prioridades e orientações de política criminal para o biénio de 2015-2017 estabelece que a cibercriminalidade é um fenómeno criminal:

- de prevenção prioritária (Artigo 2º, alínea m)) e
- de investigação prioritária (Artigo 3º, alínea h)).

Esta determinação é fundamentada pelo "*aumento do número de crimes informáticos e de crimes cometidos com recurso a meios informáticos, ocorrido na última década, que acompanhou a crescente utilização da informática no estabelecer de relações profissionais, pessoais e comerciais*".

3. No documento de definição de objetivos estratégicos para o triénio judicial 2015-2018 e para o ano judicial 2015-2016 (Artigo 90º da Lei da Organização do Sistema Judiciário), emitido pelo Presidente do Conselho Superior da Magistratura, pela Procuradora-Geral da República e pela Ministra da Justiça, diz-se serem objetivos estratégicos "*melhorar o tempo de resolução dos processos*" e "*racionalizar, padronizar e simplificar procedimentos e rotinas*", passando estes objetivos pela qualificação de "*recursos humanos dos tribunais*".

4. A expansão e ampla difusão de utilização da Internet atingiram toda a população portuguesa. Em particular, o acesso por dispositivos móveis e telefones de última geração (*smartphones*) permite a conectividade permanente às redes. Esta permanente ligação veio criar uma exposição acrescida a riscos e a actuações prejudiciais (e criminosas), que importa conhecer, prevenir e, quando revelem actuações ilícitas, punir.

A lei penal portuguesa (Lei do Cibercrime – Lei nº 109/2009) incrimina diversas atuações, com utilização das redes de comunicações. Portugal ratificou a Convenção do Conselho da Europa sobre Cibercrime (Convenção de Budapeste, em vigor em Portugal desde 2010).

Objetivos gerais

Com este plano de ação pretende-se dotar o Ministério Público de mais eficácia no tratamento de todos os fenómenos de natureza criminal ocorridos nas redes de comunicações ou cometidos por via delas.

Pretendem ainda vir-se a atingir os seguintes objectivos gerais:

- desenvolver o conhecimento do fenómeno, no contexto nacional;
- sensibilizar os magistrados para as problemáticas que o envolvem;
- facultar formação específica nesta área a magistrados do Ministério Público, designadamente sobre a obtenção de prova digital;
- criar especialização nesta temática nas comarcas;
- promover e facilitar a articulação entre as fases processuais de investigação e julgamento e
- padronizar procedimentos e promover boas práticas processuais.

Linhas de ação a desenvolver

1. **Reformulação da rede de pontos de contacto do Cibercrime.**
   Desde a sua criação, em Dezembro de 2011, o Gabinete Cibercrime criou e manteve uma rede de pontos de contacto em todos os círculos judiciais. A tais pontos focais foi dada a missão de recolher informação sobre as problemáticas da realidade processual na área da cibercriminalidade, para introduzir à discussão nas reuniões de pontos de contacto. Era suposto que as conclusões destas mesmas reuniões fossem depois transmitidas aos colegas da circunscrição, pelos pontos de contacto.
   Entretanto, a orgânica judiciária foi alterada e os círculos judiciais deixaram existir. Por outro lado, a atividade dos pontos de contacto, muitíssimo dinâmica em muitos casos foi, num ou noutro, menos consequente ao nível da circunscrição, tendo-se notado casos de menor sucesso nas suas funções.
   Importaria agora, em colaboração com os Magistrados Coordenadores das Comarcas, por um lado, redefinir a rede de pontos de contacto, conciliando-a com a nova orgânica judiciária.
   Por outro lado, importaria também que esta rede tivesse mais consequências práticas ao nível local e ao nível da partilha de informação (no SIMP). Seria desejável que os pontos de contacto da rede fossem magistrados especializados, a quem pudessem ser privilegiadamente distribuídos inquéritos destas temáticas. Desta forma, o ponto (ou pontos, consoante a dimensão da Comarca) será o embrião de uma futura especialização na distribuição de processos nesta área (sendo certo que algumas Comarcas deram já passos nesse sentido).

2. **Realização de sessões de trabalho/formativas nas comarcas.**
   A criminalidade tem vindo a expandir-se, de forma galopante, nas redes de comunicação. Além dos fenómenos de cibercriminalidade, têm-se multiplicado a ocorrência de crimes, chamados tradicionais, onde são utilizadas as redes ou meios informáticos.

É pois importante que a generalidade dos magistrados do Ministério Público com funções de investigação criminal tenha preparação para dirigir a investigação em casos com esta envolvência.
A regular movimentação de magistrados, por um lado, e a constante evolução técnica, por outro, torna necessária a realização de sessões de trabalho formativas neta área, mesmo em Comarcas onde no passado se realizaram já sessões.

3. **Desenvolver iniciativas específicas dirigidas a práticas criminosas específicas.**
Tem sido detetado que alguns dos fenómenos criminógenos nas redes de comunicações atingem um número muito significativo de vítimas, em todo o território nacional. É, por exemplo, o caso das vendas fraudulentas de produtos na Internet: o agente dos factos põe à venda um produto, que vende a múltiplas pessoas, recebendo o respetivo preço, sem nunca o entregar a nenhuma delas. Muitas delas acabam por apresentar queixa na comarca onde residem, dando-se assim origem a múltiplos processos de inquérito em que a vítima é diferente mas o agente do crime e a sua ação criminosa são a mesma.
Entre muitos destes processos existirá conexão processual.
Além disso, proceder a uma investigação isolada em cada um destes casos, multiplicando-se o mesmo tipo de diligências (quando poderia proceder-se a uma só investigação, concentrando vários casos em conexão) constitui um inglório esforço de investigação e um desnecessário consumo de recursos processuais.
Importa pois criar mecanismos operacionais que permitam aos magistrados titulares de processos desta natureza perceber se um determinado processo de inquérito está em relação, designadamente de conexão, com outros também pendentes.
Este propósito poderá atingir-se criando uma ferramenta de registo centralizado de inquéritos, onde se especifiquem campos que permitam, por via de cruzamento de informação (não pessoal), detetar processos concretos em conexão.
Este registo poderá também ser uma interessante ferramenta de conhecimento do fenómeno e, por essa via, de prevenção criminal. Será viável a constituição, com o referido propósito, de um registo de dados de processos (não pessoais), no SIMP, em conjugação com o Gabinete de Coordenação dos Sistemas de Informação da PGR.

4. **Potenciar a cooperação com os órgãos de polícia criminal na obtenção de prova digital.**
O mecanismo rotineiro de delegação de competência para investigação nos órgãos de polícia criminal supõe, em geral, algum percurso burocrático, de troca de expediente entre o Ministério Público e o OPC. Nesta rotina, de remessa física do processo ao OPC, após despacho de delegação de competência pelo Ministério Público, decorre um lapso de tempo significativo, durante o qual não é realizado qualquer ato de investigação criminal.
Nos casos em que, logo no início da investigação, se torna necessária a recolha de prova digital – sobretudo de registo de comunicações (em especial referente a endereços IP) –, pertencendo em exclusivo à autoridade judiciária a competência para esta diligência de prova, aquele percurso burocrático acaba por ser infrutífero, porque o processo tem que ser, de novo, levado a despacho ao Ministério Público. Nestes trâmites esgota-se tempo que, muitas vezes, torna inviável a obtenção daquela prova, por já ter sido destruída.
É certo que o Ministério Público pode, logo aquando do despacho inicial, providenciar no sentido da obtenção daquela prova. Porém, os mecanismos instituídos, de prolação de despacho de delegação de competência em cópia de apenas uma pequena parte do processo, nem sempre permitem alcançar a necessidade daquela diligência.
Noutra vertente, é cada vez mais corrente a necessidade de, em inquérito, proceder à apreensão de dispositivos de comunicação móveis (telemóveis, *smartphones*, *tablets*, etc). O regime de apreensão e de obtenção da eventual prova nele contida é complexo – por exemplo, em certas situações pode ser necessária a intervenção do juiz de instrução (será, por exemplo o caso de ser necessária a apreensão de mensagens eletrónicas ou dados suscetíveis de pôr em risco o respeito pela privacidade do visado).

Porém, a investigação nem sempre tem clara perceção destas estritas regras, sendo certo que a sua violação tem como consequência a nulidade da eventual prova obtida.
Por último, tem sido notado que não tem chegado aos OPC suficiente conhecimento dos novos métodos de investigação e de obtenção de prova, implementados pelo Ministério Público (por exemplo, sobre os procedimentos expeditos para solicitação de informação aos operadores de comunicações portugueses e internacionais, ou sobre as novas possibilidades de realização de perícias, com recurso às universidades).
Importaria pois desenvolver, em conjunto com os OPC, modelos ou formulários de apreensão de elementos de prova. Importaria ainda promover sessões formativas e de partilha de boas práticas, com a participação de oficiais com funções na área da investigação criminal, dos diversos órgãos de polícia criminal.

5. **Explorar mecanismos que permitam dar seguimento a denúncias recebidas por correio eletrónico.**
São recebidas, com crescente regularidade, por via do endereço eletrónico do Gabinete Cibercrime, queixas criminais, algumas das quais descrevem com algum detalhe situações de facto que, a serem verdadeiras consubstanciariam efetivamente crime. Nem sempre provêm de pessoas que se identificam mas, apercebe-se com frequência, nos casos relatados, haver alguma urgência na recolha de prova que, a não ser de imediato recolhida, poderá deixar de existir.
Importaria explorar a possibilidade de criar canais expeditos que permitissem encaminhar para os serviços do Ministério Público competentes estas denúncias, de forma a, por um lado, serem praticados eventuais atos urgentes de recolha de prova e por outro, serem desenvolvidas diligências no sentido do preenchimento de eventuais condições formais em falta na denúncia (por exemplo, a cabal identificação do denunciante).

6. **Desenvolver a articulação e a cooperação com entidades responsáveis pela segurança informática**
A ocorrência de atos contra estruturas de comunicação e informação – por exemplo, os ataques informáticos – consubstancia, em geral, a prática de crimes (designadamente de sabotagem informática e de acesso ilegítimo, o primeiro dos quais tem sempre natureza pública). A sua deteção é frequentemente feita por estruturas privadas (CERTs de entidades privadas: universidades, operadores de comunicações ou bancos) e também por estruturas públicas (Centro Nacional de Cibersegurança ou CERT-PT). A apresentação da queixa pelas entidades lesadas ocorre, muitas vezes, bastante tempo depois dos factos, o que torna menos viável a investigação – sendo certo que, havendo notícia do crime, a mesma poderia ter-se iniciado logo a seguir ao mesmo, em virtude da natureza pública do ilícito. Estas circunstâncias prejudicam o sucesso da investigação criminal.
Importa pois desenvolver formas de coordenação com aquela entidade pública e outros atores, tendo em vista, de forma expedita, o recebimento da notícia do crime e, igualmente de forma expedita, a realização de diligências urgentes de obtenção de prova, e a remessa das participações ao serviço do Ministério Público competente.

Enquadramento temporal

Setembro de 2015 a Julho de 2016

ANEXO 5

Agenda

MINISTÉRIO PÚBLICO
PORTUGAL
EM DEFESA DA LEGALIDADE DEMOCRÁTICA
gabinete CIBERCRIME

Reunião dos pontos de contacto do Gabinete Cibercrime

23 de Fevereiro de 2016

Procuradoria-Geral da República

10:30

Abertura (Procuradora-Geral da República)

10:35

O gabinete Cibercrime e os Pontos de Contacto

- Investigação criminal: algumas propostas práticas do Gabinete Cibercrime
- Breve ponto de situação quanto aos fenómenos criminógenos e quanto às questões problemáticas mais significativos nas comarcas – intervenção dos pontos de contacto

12:45

Pausa para almoço

14:15

Novos projectos

- Pornografia infantil nas redes – apresentação (Marta Viegas - DCIAP)
- Linguística forense
- Articulação do Ministério Público com os OPC na área do cibercrime e da obtenção de prova digital
- Iniciativa na área das burlas *online*

16:00 - Encerramento

ANEXO 7

Agenda da Conferência *Darkweb*

MINISTÉRIO PÚBLICO
PORTUGAL
EM DEFESA DA LEGALIDADE DEMOCRÁTICA
gabinete CIBERCRIME

Os Desafios da Criminalidade na Darkweb

Conferência

Procuradoria-Geral da República

11 de Março de 2016

10:00

Abertura (Procuradora-Geral da República)

10:15

Os desafios da criminalidade na *darkweb* - ***Gabinete Cibercrime***

10:30

O que é a *darkweb*? – ***Lino Santos, Centro Nacional de CiberSegurança***

11:00

A experiência prática na Europa - ***Carlos Nunes, Inspetor da Polícia Judiciária***

11:45

O quadro legal português e a *darkweb*: obstáculos legais à obtenção de prova - ***David Silva Ramalho, Advogado***

12:30

Debate

13:00

Encerramento

ANEXO 11

Crimes de pornografia infantil

MINISTÉRIO PÚBLICO
PORTUGAL
gabinete CIBERCRIME

NOTA

(interna)

INQUÉRITOS REFERENTES A PORNOGRAFIA INFANTIL

Janeiro a junho de 2016

SUMÁRIO

PROPÓSITO DA PRESENTE NOTA

1. Com esta nota pretende dar-se conhecimento do Relatório 1/2016 do DCIAP, referente à cooperação desenvolvida com o *National Center For Missing & Exploited Children* (NCMEC), dos Estados Unidos da América, visando a participação e investigação de crimes de pornografia infantil. Junta-se esse relatório, da autoria da Sra. Dra. Marta Viegas, como Anexo 1.

A COOPERAÇÃO COM O NCMEC

2. Recorda-se que, na sequência de contactos desenvolvidos com o *Immigration and Customs Enforcement* (ICE) do *Department of Homeland Security* dos Estados Unidos da América, foi estabelecido um protocolo informal de cooperação com o *National Center for Missing and Exploited Childre*n (NCMEC).

3. O NCMEC é uma organização não-governamental, mas tutelada pelo Congresso dos Estados Unidos, que tem como propósito recolher, com vista à sua transmissão às autoridades policiais e judiciais territorialmente

competentes, quer dentro dos Estados Unidos, quer noutros países, a informação que encontre disponível sobre crianças desaparecidas e sobre crianças exploradas sexualmente. Em especial, a sua atuação tem incidido sobre eventuais utilizadores de *sites* na Internet onde se divulgue pornografia infantil, bem como de canais de assédio a crianças para a prática de atos sexuais ou de prostituição.

4. 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 atos sexuais) com ligação a Portugal – ou seja, cujo eventual responsável utilizou, para aceder à Internet, um endereço de IP pertencente a um operador de comunicações português. Estas situações foram no passado transmitidas a autoridades policiais portuguesas. Porém, na sua generalidade, foram inconsequentes em termos processuais.

5. Sobre esta matéria foi emitida a Diretiva nº 4/2013 da Procuradoria-Geral da República, que atribuiu ao DCIAP competência para, de forma centralizada, 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.
Em consequência destas determinações, as autoridades norte-americanas passaram a remeter direta e exclusivamente ao DCIAP as suas participações, contendo imagens (fotografias ou vídeos) de pornografia infantil.

O PROCEDIMENTO NO DCIAP

6. Quando são recebidas tais participações, o DCIAP analisa sumariamente as mesmas, tendo em vista apurar da concreta suscetibilidade – ou não –, de a denúncia ter relevância criminal. Em mais de metade dos casos, a denúncia é arquivada liminarmente. Nos restantes, é determinada a abertura de inquérito.

7. Procede-se ao arquivamento liminar, por exemplo, quando a participação não contém nenhuma imagem identificável como de pornografia infantil, ou quando há dúvida sobre a idade da pessoa retratada. Também se arquiva liminarmente quando não é legalmente permitido obter informação de localização do agente do crime (por exemplo, porque os eventuais factos decorreram há mais que um ano, ou o servidor Internet está baseado no estrangeiro e é não cooperante), ou ainda quando a participação não identifica o endereço de IP utilizado pelo agente do crime, ou a data e hora em que o fez.

8. Nos casos em que se procede à abertura de inquérito, realizam-se diligências (sobretudo solicitando referências de utilização de endereços IP aos operadores de comunicações), com vista a apurar qual a identidade e local de residência do autor dos factos. Logo que se apuram referências de eventual identidade e morada, o inquérito é remetido à comarca territorialmente competente, para realização das ulterioras diligências de inquérito.

BALANÇO

9. A Circular nº 02/2013 da Procuradoria-Geral da República determina que os Senhores Magistrados comuniquem ao DCIAP o resultado final destes inquéritos, remetidos às diversas comarcas. A verdade, porém, é que o DCIAP tem manifestado que apenas tem tido conhecimento de um número reduzido de despachos finais. Por isso, a informação disponível pode não ser completa.

10. Inquéritos instaurados. Como consta do relatório do DCIAP, no primeiro semestre de 2016 (janeiro a junho) foram remetidas pelo NCMEC 669 participações. Delas, apenas 319 deram origem a abertura de inquérito (as restantes 350 foram arquivadas liminarmente, por alguma das razões a que acima se aludiu).
Do mesmo relatório consta que, desde outubro de 2013 (e até junho de 2016), se procedeu à abertura de 1350 inquéritos, de entre as 2880 participações recebidas do NCMEC no mesmo período.

11. Muitos destes inquéritos foram arquivados ainda no DCIAP. Com efeito, destes 1350 inquéritos, apenas foram remetidos para as comarcas 601 deles.
Desde logo, 41 inquéritos eram duplicação de outros, ou estavam em conexão com outros, e foram incorporados nos mesmos. Por outro lado, 634 dos inquéritos foram arquivados no DCIAP, logo após as primeiras diligências.
A maior parte deles foi logo arquivada porque os operadores de comunicações já não detinham informação sobre o utilizador do IP a partir do qual foi feito o *upload* das imagens ou vídeos. Ou ainda por ter sido usado um IP público. Em todos estes casos, não é tecnicamente possível reunir prova que permita apurar a identidade dos suspeitos.

12. Também muitos arquivamentos nas comarcas. Dos 601 inquéritos remetidos para as comarcas desde outubro de 2013, 173 deles foram já arquivados com fundamento no artigo 277º, nºs 1 e 2 do Código de

Processo Penal (por inexistir prova de crime ou prova da identidade do seu autor, ou por ser legalmente inadmissível o procedimento ou, ainda, por não ter sido possível obter indícios suficientes da verificação de crime ou de quem foram os agentes).

13. Suspensões provisórias do processo. Segundo as comunicações efetuadas ao DCIAP, foi aplicada a suspensão provisória do processo em 17 inquéritos destes inquéritos. À data do relatório do DCIAP referente ao primeiro semestre de 2016, 9 destes inquéritos já tinham sido arquivados por o prazo da suspensão estar já findo.

14. Acusações. Até ao final de janeiro de 2016, o DCIAP foi informado de que tinha sido proferida acusação em apenas 3 dos processos remetidos às comarcas. É o que resulta do relatório do DCIAP referente ao segundo semestre de 2015, que se junta como Anexo 2. Por, na altura, se aperceber que este número de acusações poderia não corresponder à realidade, foi solicitada a colaboração dos pontos de contacto do Gabinete Cibercrime para, nas comarcas, averiguarem o verdadeiro estado dos processos e, também, da eventual prolação de mais despachos de acusação.
Em resultado desta iniciativa informal veio a apurar-se que, até ao fim de junho de 2016, tinham afinal sido proferidas, pelo menos, 20 acusações – que são as acima referidas.

15. Condenações. O relatório do DCIAP não o refere, porque não podia referi-lo, mas metade destas acusações foram já encaminhadas para julgamento e os respetivos arguidos condenados. Tal informação resulta de trabalho adicional de pesquisa realizado pelo Sr. Dr. Raúl Farias, do Gabinete da Senhora Procuradora-Geral da República, com referência a 31 de outubro de 2016, o qual se junta como Anexo 3.
Da análise efetuada, verifica-se que, em 10 dos 20 processos em que foram proferidas acusações, foram, entretanto, realizados os respetivos julgamentos e proferidas sentenças de condenação. Anota-se que de nenhum dos julgamentos realizados resultou decisão de absolvição.
Por outro lado, quanto aos restantes 10 processos, 8 deles estão já em fase de julgamento, ou aguardam julgamento, ou ainda marcação da respetiva data. Num outro deles, após a acusação, em fase de instrução, foi decretada a suspensão provisória do processo e quanto ao último, está ainda pendente (foi usada a forma de processo sumaríssimo).

16. Repercussão social. A instauração destes processos deu origem a um grande número de buscas domiciliárias, de constituições de arguidos e de aplicação de medidas de coação – nelas se incluindo medidas

de prisão preventiva. Pela natureza da dinâmica processual, não é possível, no contexto desta nota, contabilizar o número de arguidos constituídos, ou o número de buscas, ou o número de prisões preventivas impostas.

Em todo o caso, o acompanhamento do eco público destes processos, na comunicação social, permitiu concluir que os mesmos tiveram enorme repercussão (sobretudo por ter havido diversas detenções). Juntam-se, no Anexo 4, algumas das notícias publicadas a este respeito, entre junho de 2015 e outubro de 2016.

Afigura-se que esta difusão, pelos *media*, de intervenções policiais e judiciárias a este respeito, tem a virtualidade de criar efeito de prevenção geral, profilático, que ultrapassará em muito o mero efeito processual endógeno. Anota-se este resultado como muito positivo.

SÍNTESE CONCLUSIVA

17. Ficou dito acima que, desde 2013, foram remetidos às diversas comarcas do país 601 inquéritos, sendo em 20 deles proferida acusação por crimes relacionados com pornografia infantil. Deduzidos aqueles em relação aos quais se optou por suspensão provisória do processo (que foram 17), estarão pendentes nas comarcas 420 inquéritos, ainda em investigação. Por outro lado, em todos os processos deste conjunto já julgados, houve decisão de condenação.

18. Apesar da aparente desproporção, entre o número de inquéritos e o número de acusações, o balanço é muito positivo. Na verdade, a investigação neste tipo de inquéritos é muito difícil e complexa, costumando ser demorada. O respetivo resultado tarda sempre em ser atingido. Por outro lado, todos estes processos supõem a realização de perícia informática, a qual é quase sempre um imprescindível meio probatório. É sabido que as perícias, em regra a cargo da Polícia Judiciária, estão a ser realizadas com um enormíssima demora e atraso – que anda pelos três anos.

Tendo todo este procedimento sido introduzido no terceiro trimestre de 2013 é, pois, natural que seja ainda pouco expressivo o número de inquéritos em que tenha sido deduzida acusação. Em todo o caso, espera-se que em breve o número de acusações deduzidas venha a aumentar muito, consoante forem sendo concluídos os inquéritos.

19. Por outro lado, o número de condenações tem também um significado claro: nos processos em que foi já realizado o julgamento, não houve absolvições, em todos eles havendo sentença condenatória.

20. Como ficou bem expresso, todo este procedimento era, antes de 2013, inexistente. As eventuais notícias de crimes eram comunicadas e dissipadas pelas várias comarcas, onde se diluíam na massa dos restantes

inquéritos, sem que se atendesse a que, neste caso, uma intervenção rápida do Ministério Público, sobretudo na fase inicial, é crucial para o sucesso da investigação. Ou seja, antes da introdução desta abordagem inicial concentrada no DCIAP, não tinha sido possível obter resultados positivos neste tipo de processos. A intervenção do DCIAP foi assim um elemento diferenciador da eficácia da intervenção do Ministério Público.

21. Pode, pois, concluir-se que o estabelecimento deste mecanismo veio permitir a investigação de processos que anteriormente não tinha sido possível investigar. Antes, neste tipo de casos, os processos eram generalizadamente arquivados, por falta de capacidade para lidar com os mesmos, sobretudo na sua fase inicial. Este mecanismo procedimental veio alterar a situação e os resultados são já visíveis. Na fase processual dependente do Ministério Público foram deduzidas muitas acusações e determinadas um número significativo de suspensões provisórias do processo. Quanto à fase de julgamento, começaram a surgir as primeiras condenações por crimes desta natureza.

Tendo em conta o tipo específico de criminalidade em causa (difusão de pornografia infantil), estas observações afiguram-se muito satisfatórias.

Lisboa, 3 de novembro de 2016

ANEXO 14

Alerta Cibercrime 7 de dezembro de 2015

MINISTÉRIO PÚBLICO
PORTUGAL
EM DEFESA DA LEGALIDADE DEMOCRÁTICA
gabinete CIBERCRIME

ALERTA CIBERCRIME

7 de Dezembro de 2015

Chamadas fraudulentas em nome da Microsoft

1.

Está em curso uma campanha de chamadas fraudulentas em que, de forma enganosa, é invocado o apoio técnico da Microsoft tendo como alvo utilizadores do território nacional.

2.

Nesta actividade criminosa, os "atacantes" contactam os alvos selecionados por telefone, fazendo-se passar pela equipa de Assistência Técnica da Microsoft. No contacto, a vítima é informada de que tem um problema no seu computador (normalmente um vírus) para o qual o assistente tem resolução.

A vítima é depois "conduzida" a instalar *software* que lhe é remetido e que resolverá o suposto problema. O *software* instalado é de origem maliciosa e, entre as várias ações, poderá danificar, roubar dados, cifrar (ransomware) ou até mesmo inutilizar o sistema.

3.

É recomendável que, tal como acontece nos casos de "*phishing*" por correio eletrónico, os utilizadores avaliem cautelosamente as comunicações que recebam, nunca fornecendo informações pessoais e não instalando qualquer tipo de *software* que lhe seja indicado telefonicamente.

ANEXO 15

Alerta Cibercrime 17 de dezembro de 2015

MINISTÉRIO PÚBLICO
PORTUGAL
EM DEFESA DA LEGALIDADE DEMOCRÁTICA
gabinete CIBERCRIME

ALERTA CIBERCRIME

17 de Dezembro de 2015

'Phishing' dirigido a clientes do Montepio Geral

1.

Está em curso uma campanha de "*phishing*" dirigido a clientes do Montepio Geral.

2.

Como habitual nestes casos, o processo começou com a expedição, para muitos destinatários, de mensagens fraudulentas de correio eletrónico. A primeira destas mensagens a ser sinalizada pelo Gabinete Cibercrime, datava de 16 de Dezembro de 2015, às 02:01 UTC. Na mensagem, o seu autor anunciou que o destinatário tem a conta bancária bloqueada até que proceda a atualizações na mesma. Remete um *link*, que diz ser do Montepio Geral, mas que na realidade aponta para um *site* Internet onde se copiam todos os conteúdos disponibilizados pelo site autêntico do Montepio, mas não é a verdadeira página web daquele banco: https://net24-monteepio.websiteseguro.com. Ou seja, é uma falsa página - a página autêntica está alojada em https://www.montepio.pt.

3.

A página fraudulenta é muitíssimo parecida, praticamente igual, em aparência, aos olhos do utilizador comum, à autêntica página do Montepio Geral. Está alojada num servidor no Uruguai. Se a vítima aceder a ela e nela introduzir a informação que se lhe solicita, fornecerá aos autores destes factos todos os dados necessários a proceder a todos os movimentos bancários.

ANEXO 16

Alerta Cibercrime 18 de fevereiro de 2016

MINISTÉRIO PÚBLICO
PORTUGAL
EM DEFESA DA LEGALIDADE DEMOCRÁTICA
gabinete CIBERCRIME

ALERTA CIBERCRIME

18 de Fevereiro de 2016

'Phishing' dirigido a clientes do Montepio Geral

1.

Está em curso mais uma campanha de "*phishing*" dirigido a clientes do Montepio Geral, que repete os procedimentos de duas outras, anteriores, detetadas a 17 de Dezembro de 2015 e a 25 de Janeiro de 2016.

2.

Como habitual nestes casos, o processo começou com a expedição, para muitos destinatários, de mensagens fraudulentas de correio eletrónico. A primeira destas mensagens desta nova campanha sinalizada pelo Gabinete Cibercrime data de 18 de Fevereiro de 2016, às 03:47 UTC. Na mensagem anuncia-se ser necessário proceder a atualização de dados, no site do Montepio Geral, para garantir o acesso aos respetivos serviços, devendo essa atualização, sob pena de bloqueio do serviço, ser feita mediante introdução dos códigos de acesso e do *Cartão de Matriz*.

3.

As mensagens sinalizadas indicavam provir de endereços de IP pertencentes a dois fornecedores de *cloud services*, que foram concretamente identificados, estando ambos baseados na Suíça.

4.

As mensagens contêm *links*, que dizem ser de acesso à página *web* do Montepio Geral. Tais *links* conduzem a *sites* Internet onde se reproduzem, de forma muitíssimo fiel, todos os conteúdos disponibilizados no *site* autêntico do Montepio, mas não são geridos por aquele banco nem por ele autorizados.

Foram identificadas pelo menos duas páginas falsas, clonadas da página do Montepio Geral, com os seguintes URL: https://seg-montepio.websiteseguro.com e

https://net24montactulizacao.websiteseguro.com. Em Janeiro haviam sido identificadas também as seguintes páginas "falsas", entretanto inactivas: https://actualizacaomontepio.websiteseguro.com e https://actualizacaodesegura.websiteseguro.com. Todas elas são páginas *falsas*, já que a autêntica página está alojada em https://www.montepio.pt.

Tais páginas *falsas* – todas elas –, estão fisicamente alojadas num servidor localizado no Uruguai, o qual é administrado por um fornecedor de *cloud services* com sede no Brasil.

5.

Estas páginas fraudulentas são muitíssimo parecidas, praticamente iguais em aparência, aos olhos do utilizador comum, à autêntica página do Montepio Geral. Se a vítima aceder a elas e nelas introduzir a informação que se lhe solicita, fornecerá aos autores destes factos todos os dados necessários ao acesso, no legítimo *site* do Montepio Geral, à sua conta bancária. E assim, permitirá que terceiros procedam a todos os movimentos bancários permitidos por esta via.

ANEXO 18

Relatório Eurojust - 25 de novembro de 2015

gabinete CIBERCRIME

NOTA

Eurojust Meeting on Cybercrime

Towards a Judicial Cybercrime Network

Haia, 25 de Novembro de 2015

1.

Decorreu, no dia 25 de Novembro de 2015, nas instalações da Eurojust, na Haia o "*Eurojust Meeting on Cybercrime - Towards a Judicial Cybercrime Network*", no qual participou o Gabinete Cibercrime, em representação da Procuradoria-Geral da República.

Esta reunião destinava-se a discutir os possíveis caminhos na criação formal de uma rede judiciária na área do cibercrime. Era propósito da Eurojust e da representação da Holanda abordar eventuais vertentes práticas e concretas.

Junta-se a agenda como Anexo 1.

2.

Em momento prévio ao da reunião, tinha sido solicitada a contribuição escrita dos participantes, pelo preenchimento de um questionário que respondesse aos seguintes pontos: a estrutura da rede, os seus membros, as suas tarefas (e expetativas) e, por último, a vantagem de ser apoiada por uma página *web*.

Junta-se, como Anexo 2, o formulário respondido por Portugal

3.

Participaram na reunião membros nacionais na Eurojust (entre eles, a Presidente da Eurojust e membro nacional da Bélgica, Michèle Coninsx, Daniela Buruiana, membro nacional da Roménia e Presidente da *Task Force on Cybercrime*, Koen Hermans, Vice-Presidente da *Task Force on Cybercrime* e membro adjunto da Roménia e José Eduardo Guerra, membro adjunto de Portugal e igualmente membro da *Task Force on Cybercrime*.

Participaram também representantes da Holanda, que vai liderar o processo de constituição da rede, durante a Presidência holandesa do Conselho da União Europeia, no primeiro semestre de 2016 (designadamente Erik Planken, do Ministério da Segurança e Justiça e Lodewijk van Zwieten, Procurador Holandês destacado como perito em Cibercrime na Eurojust).

Participaram ainda representantes do Departamento de Justiça dos Estados Unidos da América (Cristina Posa) e do Conselho da Europa (Alexander Seger).

Por último, participaram representantes indicados por 23 dos Estados membros, por serem especialistas na área da cibercriminalidade.

4.

No decurso da reunião foi esclarecido que o cibercrime e a cibersegurança serão uma das prioridades da presidência holandesa do Conselho da União Europeia, que ocorrerá no primeiro semestre de 2016, em trio com a Eslovénia e Malta. Neste contexto, merecerão especial atenção os dossiês da proteção de dados e da retenção de dados de tráfego.

Em particular quanto à investigação de cibercriminalidade, será propósito holandês o de reforçar a efetividade na atuação das autoridade públicas (promovendo o uso dos instrumentos existentes e explorando possíveis falhas nos instrumento existentes). Por outro lado, foi igualmente definido como objetivo o de abordar vertentes menos exploradas: a do recurso ao acesso direito a fornecedores de serviços na Internet estrangeiros, o acesso transfronteiriço a dados e a definição mais rigorosa de princípios de jurisdição no ciberespaço.

Neste contexto, a criação efetiva e formal de uma rede de procuradores na área do cibercrime assume um papel importante, ao permitir contruir ligações mais fáceis e sólidas entre quem tem que dirigir a investigação nos vários Estados Membros da União Europeia, abrindo canais para a partilha de boas práticas, novidades legislativas ou jurisprudência.

Planeia a Holanda vir a lançar formalmente a rede em Maio ou Junho de 2016.

5.

Da discussão resultaram ideias ainda por purificar, a propósito da rede.

Assumiu-se que deverá ser autónoma da Eurojust, embora possa ter o seu apoio de secretariado. Deverá promover reuniões duas vezes por ano, para permitir a criação de laços entre os seus membros. Ganhará, se puder dispor de uma plataforma segura de comunicações e de um *site web* seguro.

Por outro lado, foi vincado que uma rede desta natureza deverá ser orientada para a ação e os casos concretos, permitindo facilitar a ultrapassagem de eventuais dificuldades na cooperação internacional, por exemplo.

Poderá igualmente ser uma sua mais-valia a monitorização de decisões judiciais ou a partilha de atualizações sobre tendências criminógenas.

6.

Anotaram-se alguns pormenores a carecer de discussão futura, por exemplo quanto à representação da Irlanda ou do Reino Unido, onde o Ministério Público apenas intervém numa fase final da investigação (a qual é quase

integralmente assegurada pela polícia). Noutros Estados Membros poderá haver necessidade de mobilizar juízes de investigação (ou de *instrução*).

Por outro lado, embora se tenha referido a vantagem da eventual presença de países terceiros à União Europeia (como a Suíça, a Noruega ou os Estados Unidos), não foi possível encontrar um critério para essa presença.

7.

Ficou a Eurojust, com a futura presidência holandesa do Conselho da União Europeia, com o encargo de convocar uma nova reunião, de afinação dos pormenores da rede e de lançamento da mesma.

A Eurojust anunciou que, quando tal reunião ocorrer, por razões formais e de eficácia, irá convocar diretamente os representantes dos Estados Membros que agora compareceram, a menos que venha a haver indicação em contrário das respetivas procuradorias-gerais.

Lisboa, 2 de Dezembro de 2015

(Pedro Verdelho)

ANEXO 20

Relatório *Strategic Seminar*

NOTA

STRATEGIC SEMINAR **"**KEYS TO CYBERSPACE**"**

A Haia, 2 de Junho de 2016

1.

Decorreu, no dia 2 de Junho de 2016, na Haia o *Strategic Seminar* "Keys to Cyberspace", no qual participou o Gabinete Cibercrime, em representação da Procuradoria-Geral da República. Esta reunião destinou-se a congregar representantes dos Estados Membros da União Europeia, com experiência prática em cibercrime, com o objetivo de identificar e encontrar possíveis soluções para os desafios da investigação e prossecução de casos de cibercrime.

Os temas genéricos incluíram a jurisdição no ciberespaço, em especial em relação com os fenómenos da chamada *cloud*, a cooperação com fornecedores de serviço Internet sedeados nos Estados Unidos da América e a encriptação de dados. Uma sessão especial focou-se na criação do *EU Judicial Cybercrime Network*, ou Rede Judicial Europeia para matérias do Cibercrime.

Foi propósito deste seminário que as suas conclusões fossem apresentadas no *11th Meeting of the Consultative Forum of Prosecutors General and Directors of Public Prosecutions of the Member States of the European Union*, a realizar a 3 de Junho de 2016.

Junta-se a agenda como Anexo 1.

2.

As discussões travadas durante todo o seminário incidiram sobre um documento previamente distribuído, que se junta como Anexo 2. Por outro lado, foi previamente solicitada opinião escrita sobre as conclusões a remeter ao *11th Meeting of the Consultative Forum*, em particular quanto à criação do *EU Judicial Cybercrime Network*. A este propósito foi a seu tempo remetido o documento que se junta como Anexo 3.

3.

Participaram na reunião membros nacionais na Eurojust (entre eles, o Vice-Presidente da Eurojust e membro nacional de Espanha, Francisco Jiménez-Villarejo, Daniela Buruiana, membro nacional da Roménia e Presidente da *Task Force on Cybercrime*, Koen Hermans, Vice-Presidente da *Task Force on Cybercrime* e

membro adjunto da Roménia e José Eduardo Guerra, membro adjunto de Portugal e igualmente membro da *Task Force on Cybercrime*). Participaram também diversos representantes da Holanda, que tem liderado o processo de constituição da *EU Judicial Cybercrime Network*. Participaram ainda representantes do Departamento de Justiça dos Estados Unidos da América, da Suíça e da Noruega. Por último, participaram representantes especificamente indicados pelos Estados Membros da União Europeia, por serem especialistas na área da cibercriminalidade.

4.

Como informação de fundo, foi referida na reunião a conferência, organizada pela Presidência holandesa da União Europeia, "*Crossing borders: Jurisdiction in Cyberspace*" a qual teve lugar a 7 e 8 de Março de 2016, em Amesterdão. Anote-se que o Ministério Público esteve presente e teve intervenção nesta conferência, moderando um dos workshops.

Desta conferência resultaram várias propostas, tendo em vista tornar mais expedita a cooperação internacional e a cooperação com fornecedores de serviço (como a criação de um portal *online*, pontos únicos de contacto, traduções automáticas, adoção de procedimentos para situações de emergência e um regime simplificado de pedidos de auxílio mútuo para as chamadas informações de assinante, ou *subscriber information*).

5.

Quanto à temática da jurisdição no ciberespaço, em especial em relação com os fenómenos da chamada *cloud*, a ideia principal em discussão foi a da necessidade de, em investigação criminal, se poder aceder a informação alojada noutro local – que não a do agente que investiga. Este acesso pode supor a obtenção de dados fisicamente alojados num país diferente da entidade investigante.

O subscritor interveio a este propósito, para descrever o mecanismo do Artigo 15º, nº 5 da Lei do Cibercrime, que prevê a extensão da pesquisa informática a sistemas remotos, mesmo que localizados no estrangeiro. Representantes de outros países aludiram a mecanismos de igual teor, nos respetivos sistemas legais.

6.

No que respeita à cooperação com fornecedores de serviço Internet sedeados nos Estados Unidos da América, foi feita uma apresentação por Aaron R. Cooper, do Departamento de Justiça dos Estados Unidos. Seguiu-se um *tour de table* sobre as experiências nacionais de cada Estado Membro a este propósito.

O subscritor relatou brevemente, a este respeito, a cooperação que tem sido desenvolvida com ISP globais (a Google, a Microsoft e a Facebook). Sublinhou-se estar a haver eficácia neste diálogo, mas evidenciou-se também subsistirem sérias deficiências. Assim acontece, por exemplo, por esta cooperação depender da boa

vontade dos operadores, que são livres de cooperar ou não. Por isso, há muitos importantes operadores que não são "cooperantes". Não existe um quadro normativo onde esta prática de cooperação possa encontrar referência. Desta falta de referência legal resulta, por exemplo, que todos os operadores europeus estejam impedidos de cooperar com autoridades de outros Estados, sem recurso aos mecanismos da cooperação judiciária formal.

7.

A propósito da encriptação de dados, foram feitas duas apresentações: uma delas, por Aaron R. Cooper, do Departamento de Justiça dos Estados Unidos, sobre o caso que opôs o Ministério Público americano à Apple Inc; a outra, por Eirik Tronnes Hansen, procurador na Noruega, sobre a experiência do seu país.

O tema é extremamente relevante, já que um número crescente de prestadores de serviços eletrónicos tem vindo a implementar a criptografia nos seus serviços, de onde resulta que, frequentemente, as autoridades deixam de conseguir aceder a dados, mesmo que apreendam fisicamente os dispositivos onde os mesmos estão armazenados.

O subscritor interveio para salientar que a Convenção de Budapeste (ratificada por 25 dos 28 Estados Membros da União Europeia e já assinada pelo 3 restantes) prevê um instrumento legal, no Artigo 18º, nº 1, que enquadra juridicamente o tema. Na lei portuguesa, esta norma tem plena equivalência no Artigo 14º, nº 1, da Lei do Cibercrime. Nesta última prevê-se que, "*se no decurso do processo se tornar necessário à produção de prova, tendo em vista a descoberta da verdade, obter dados informáticos específicos e determinados, armazenados num determinado sistema informático, a autoridade judiciária competente ordena a quem tenha disponibilidade ou controlo desses dados que os comunique ao processo ou que permita o acesso aos mesmos, sob pena de punição por desobediência*".

Durante a sessão discutiu-se ainda a possibilidade de impor coativamente a obrigação de fornecer a chave de abertura da encriptação a suspeitos e a utilização coerciva de dados biométricos (por exemplo, impressões digitais).

8.

A reunião terminou com uma sessão mais informativa, em que foi feito o ponto da situação quanto a criação do *EU Judicial Cybercrime Network*. Tal atualização foi feita por Erik Planken, do Ministério da Segurança e Justiça da Holanda, em representação da Presidência Holandesa da União Europeia e por Daniela Buruiana, membro nacional da Roménia e Presidente da *Task Force on Cybercrime*.

A criação da rede está agora pendente de aprovação no Conselho de Ministros das áreas Justiça e Administração Interna (JAI) da União Europeia, a realizar a 9 e 10 de Junho: será presente ao mesmo um projeto de resolução que a aprovará.

No entretanto, foi apresentado um primeiro "produto" dessa rede embrionária: o nº 1 do *Cybercrime Judicial Monitor*, uma publicação que virá no futuro a divulgar atualizações legais nos Estados Membros, análises de decisões judiciais e ainda abordagem de tópicos especiais de interesse.

Foi ainda apresentado um projeto de site web de acesso restrito, que sirva de apoio à rede.

9.

Por constrangimento do horário do voo de regresso a Portugal, não foi possível ao subscritor assistir à sessão de encerramento do seminário.

Lisboa, 2 de Junho de 2016

(Pedro Verdelho)

ANEXO 22

Questionário – Portugal

EUROJUST
The European Union's Judicial Cooperation Unit
P.O. Box 16183 – 2500 BD The Hague • The Netherlands

Dear participant,

The idea of a judicial cybercrime network of prosecutors and judges has already been mentioned several times at different fora. In November 2014, in the margins of the Eurojust seminar on cybercrime, a brainstorming session for practitioners was held in order to discuss the possibility to set up a network at EU level, which would enable experts to share expertise and knowledge. The national authorities present agreed on the need to establish such a network and discussed in general terms the activities which it should cover.

Also during the Eurojust tactical meeting on cybercrime, held on 1 July 2015, the participants reiterated the need to set up a judicial cybercrime network. It was concluded that the network should be used as a platform to facilitate direct contact in order to share and discuss difficulties and best practices in cybercrime investigations and prosecutions. An online secure restricted area would facilitate the sharing of sensitive information.

The aim of the meeting on 25 November is to concretely discuss and find agreement between the representatives of the EU Member States upon the several aspects of a judicial cybercrime network.

In view of this discussion, could you kindly provide your input on each of the following points:

- Structure of the network
  In our opinion, the network should be based on a list of contact points, of prosecutors – one or two prosecutor from each country.
  A coordinator of the network should be assigned, in view of taking the lead of the eventual future meetings/discussions. This coordinator should be one of the national contact points and should have the support of Eurojust, both in substantial and administrative issues.

- Members of the network
  One or two prosecutors should be assigned by the Prosecutor-General of each Member State. In case a Member States decides to appoint a more extended number (it is envisaged that it can for example the case of countries with more than one Prosecutor-General), a national coordinator of all the contact points will be also appointed.

- Tasks of the network/expectations
  The network can be an interesting forum for sharing trends of the evolving cybercriminal acts and of new emerging difficulties on real investigations.
  It can also be a good place for discussion of new problems and new solutions, in view of combating cybercrime.
  Finally, the network can facilitate investigations with international links: it can facilitate preparing and sending international MLA requests and it can make easier eventual coordination between authorities from different Member States.
  It can be considered the use of the network to transfer requests, in an expedited manner.

- Website
  For the purposes of sharing information and transfer of requests of international cooperation, a web secure platform can be a very useful tool.

Kindly send your replies to cyber@eurojust.europa.eu by 3 November 2015.

Thank you very much in advance for your cooperation.

Country: *Portugal*

Name: *Pedro Verdelho*

ANEXO 23

Portuguese Contribution

Portuguese Contribution,

regarding the Point for Discussion, on the

BACKGROUND PAPER SESSION I

II. POINTS FOR DISCUSSION

In view of the above-mentioned developments, the Chairs of the Forum would welcome the views of its Members on the following questions:

1. Would you agree to a Forum conclusion supporting the initiative of the Netherlands' Presidency in setting up the European Judicial Cybercrime Network using the following draft suggestion:

"The Consultative Forum took note of the Netherlands Presidency initiative aiming at establishing the European Judicial Cybercrime Network. The Consultative Forum supports such initiative, as a way to foster contacts among cybercrime judicial practitioners in the EU Member States and increase efficiency of investigations and prosecutions of cybercrime cases."

The response to Question 1 is "yes".

In fact, it should be supported the idea of creation of a European network of prosecutors working on cybercrime. Such a network will facilitate cooperation among prosecutors in the European space, both on concrete cases and in general knowledge on cybercrime and electronic evidence issues.

Regarding the cooperation in concrete cases, this network, as a specialised group of experts, will potentiate the role of Eurojust, where it will be based.

But it is referring to the generic cooperation that the advantages seem to be more obvious. Cybercrime and digital evidence are evolving very fast. Each day new criminal techniques are discovered, all over the globe. This continuous novelty is a challenge to prosecutors working in this area. Thus, sharing of experience will only be a great benefit. As said, this network will open channels for sharing good practice, law or jurisprudence news.

The effective and formal creation of a network of prosecutors in cybercrime plays thus an important role in helping to build easier and stronger links between those who have to direct criminal investigations the Member States of the European Union

ANEXO 24

Programa do Seminário

gabinete CIBERCRIME

aecid CENTRO DE FORMACIÓN

FISCALIA GENERAL DEL ESTADO

Asociación Ibero Americana de Ministerios Públicos

Red Iberoamericana de Cooperación Jurídica Internacional

Seminário sobre *CIBERCRIME E PROVA DIGITAL*	Seminario sobre CIBERDELINCUENCIA Y PRUEBA DIGITAL
5 a 9 de Outubro de 2015 Santa Cruz de la Sierra, Bolívia	5 a 9 de Octubre de 2015 Santa Cruz de la Sierra, Bolivia

AGENDA	AGENDA
5 de Outubro de 2015 9:30 – Receção dos participantes 10:00 – Sessão de abertura 10:30 – Pausa 11:00 - *Conferência inaugural: Desafios da luta contra o cibercrime no quadro do Estado de Direito* – Pedro Verdelho - Portugal 13:00 – Almoço 14:30 – *O enquadramento legislativo internacional - A harmonização normativa com base na Convenção de Budapeste* – Pedro Verdelho - Portugal 6 de Outubro de 2015 9:30 – *A articulação dos tipos penais perante as novas formas de atuação delitiva: em particular a luta contra a pornografia infantil na Internet* – Daniela Hernandez Lopez – México 11:00 – Pausa 11:30 - *A articulação dos tipos penais perante as novas formas de atuação delitiva: em particular os ataques a sistemas de informação* – Jorge Luis San Lucas González - Equador 13:00 – Almoço 14:30 - *A articulação dos tipos penais perante as novas formas de atuação delitiva: em particular as burlas através da Internet* – Horacio Azzolin - Argentina 16:00 - *A articulação dos tipos penais perante as novas formas de atuação delitiva: em particular os direitos da propriedade intelectual* - Ricarte Donato González - Panamá 7 de Outubro de 2015 9:30 - *A articulação dos tipos penais perante as novas formas de atuação delitiva: em particular a radicalização*	5 de Octubre de 2015 9:30 – Acreditaciones 10:00 - Inauguración 10:30 – Pausa 11:00 - *Conferencia inaugural: Desafíos en la lucha contra la ciberdelincuencia en el marco del Estado de Derecho* - Pedro Verdelho - Portugal 13:00 – Almuerzo 14:30 – *El marco legislativo internacional - La armonización normativa sobre la base del Convenio de Budapest* - Pedro Verdelho - Portugal 6 de Octubre de 2015 9:30 - *La articulación de tipos penales ante las nuevas formas de actuación delictiva; en particular la lucha contra la pornografía infantil en la red* – Daniela Hernandez Lopez – México 11:00 – Pausa 11:30 - *La articulación de tipos penales ante las nuevas formas de actuación delictiva: en particular los ataques a los sistemas de información* – Jorge Luis San Lucas González - Ecuador 13:00 – Almuerzo 14:30 - *La articulación de tipos penales ante las nuevas formas de actuación delictiva; en particular la defraudación a través de la red* - Horacio Azzolin - Argentina 16:00 - *La articulación de tipos penales ante las nuevas formas de actuación delictiva; en particular los derechos de propiedad intelectual* - Ricarte Donato González - Panamá 7 de Octubre de 2015 9:30 - *La articulación de tipos penales ante las nuevas formas de actuación delictiva: en particular la*

através da Internet: crimes de ódio e terrorismo – Elvira Tejada - Espanha 11:00 – Pausa 11:30 – *A cooperação internacional como mecanismo essencial na luta contra o cibercrime: Instrumentos disponíveis no quadro da Convenção de Budapeste* - Pedro Verdelho - Portugal 13:00 – Almoço 14:30 - *A cooperação internacional como mecanismo essencial na luta contra o cibercrime: implementação de instrumentos e canais existentes no contexto ibero-americano* - Ana Maria Martín - Espanha 16:00 – *O Reforço da coordenação entre os Ministérios Públicos dos países ibero-americanos: pistas para a criação de um grupo de trabalho de âmbito ibero-americano* - Ana María Martin - Espanha 8 de Outubro de 2015 9:30 - *O desafio da investigação tecnológica: novos métodos de investigação criminal; a salvaguarda dos direitos e liberdades das personas - em particular, conservação de dados e proteção da privacidade* –Elvira Tejada - Espanha 11:00 – Pausa 11:30 - *Mesa Redonda: Análise de mecanismos concretos de investigação:* Apresentação Introdutória - Carlos Bruno Ferreira da Silva - Brasil 13:00 – Almoço 14:30 - *A especialização do Ministério Público como forma de atuar frente à delinquência* - Argentina, Brasil, Espanha e Portugal 9 de Outubro de 2015 9:30 – Elaboração e aprovação de conclusões 11:00 – Pausa 12:30 – Sessão de Encerramento	*radicalización a través de la red: crímenes de odio y terrorismo* – Elvira Tejada - España 11:00 – Pausa 11:30 – *La cooperación internacional como mecanismo esencial en la lucha contra el cibercrimen: instrumentos disponibles en el marco del Convenio de Budapest* - Pedro Verdelho - Portugal 13:00 – Almuerzo 14:30 - *La cooperación internacional como mecanismo esencial en la lucha contra el cibercrimen: instrumentos y canales existentes en el contexto iberoamericano* - Ana María Martín España 16:00 - *Reforzamiento de la coordinación entre los Ministerios Públicos de los países Ibero americanos: apuntes para la creación de un grupo de trabajo en el ámbito iberoamericano* - Ana María Martin - España 8 de Octubre de 2015 9:30 - *El desafío de la investigación tecnológica: nuevos métodos de investigación criminal; la salvaguarda de los derechos y libertades de las personas - en particular, conservación de datos y protección de la privacidad* – Elvira Tejada - España 11:00 – Pausa 11:30 - *Mesa Redonda: Análisis de mecanismos concretos de investigación:* Ponencia introdutória - Carlos Bruno Ferreira da Silva - Brasil 13:00 – Almuerzo 14:30 - *La especialización del Ministerio Fiscal como forma de actuar frente a la delincuencia:* Argentina, Brasil, España y Portugal 9 de Octubre de 2015 9:30 - Elaboración y aprobación de conclusiones 11:00 – Pausa 12:30 – Sesión de Clausura

ANEXO 25

Conclusões do Seminário

FISCALIA GENERAL DEL ESTADO

Seminário sobre
CIBERCRIME E PROVA DIGITAL
5 a 9 de outubro de 2015, Santa Cruz de la Sierra, Bolívia

Por ocasião do Seminário Internacional sobre "*CIBERCRIME E PROVA DIGITAL*", organizado no âmbito da AIAMP e realizado no Centro de Formação da AECID de Santa Cruz de La Sierra – Bolívia, entre os dias 5 a 9 de outubro de 2015, em concretização de deliberação da XXII Assembleia Geral da AIAMP (Montevideu), os assistentes, representantes dos Ministérios Públicos e *Fiscalias* da Argentina, Brasil, Bolívia, Cuba, Equador, Espanha, Honduras, México, Panamá, Paraguai e Portugal, alcançaram as seguintes

CONCLUSÕES

Primeira

Num tempo em que a Internet é uma realidade omnipresente, é de suma importância considerar que o desenvolvimento das tecnologias de informação e comunicação deu lugar a um contexto no qual, com facilidade, se produz uma multiplicação exponencial dos fenómenos criminais cujo objeto ou meio de cometimento são as próprias tecnologias de informação e comunicação.

Acresce que estas novas actividades se projetam numa dimensão espacial que supera os limites territoriais dos Estados. As atividades nas redes são alheias aos conceitos de nacionalidade ou de

jurisdição; não conhecem fronteiras e podem ser cometidas a partir de qualquer parte do mundo e produzir efeitos simultâneos ou sucessivamente em espaços territoriais diferentes e distantes.

Pelo que, a luta contra estes fenómenos criminais deve enfrentar-se necessariamente tendo em conta este caráter supranacional.

Segunda

A cooperação internacional é essencial ao efetivo combate destes fenómenos criminais, mas por si só não é suficiente. A harmonização da legislação penal substantiva e da legislação processual dos vários países constitui, para estes efeitos, um pressuposto básico necessário para tornar possível essa cooperação internacional.

Tanto no âmbito da cooperação internacional como no âmbito da harmonização legislativa, a Convenção de Budapeste sobre Cibercrime, do Conselho da Europa constitui um documento de referência, dada a sua relevância e vocação de universalidade, sendo, por isso, conveniente a adesão à mesma por parte de todos os Estados. Isso sem prejuízo da importância de outros tratados internacionais como a *Convenção Iberoamericana sobre investigação, asseguramento e obtenção de prova em matéria de cibercriminalidade* (pendente de entrar em vigor), assim como a Recomendação da COMJIB relativa à tipificação e punição da cibercriminalidade, ambos os instrumentos assinados em Madrid no ano de 2014. Em relação a estes últimos documentos é de assinalar que na Declaração de Santo Domingo, no marco da última reunião plenária da COMJIB, se instou os Estados à sua adesão e/ou ratificação.

Terceira

O intercâmbio de experiências acerca das principais tendências criminais e dos problemas mais relevantes que surgem no decurso da investigação e prossecução penal da cibercriminalidade torna-se necessário para aumentar a eficácia da resposta penal a estas condutas. Mediante a partilha de

experiências e boas práticas é possível melhorar a capacidade de obtenção, preservação e uso de provas digitais nos processos penais, criar condições que favoreçam a cooperação prática e operativa em casos específicos, detetar eventuais lacunas legais e identificar as necessárias reformas legislativas que as colmatem, e adaptar, efectivamente, as legislações nacionais aos padrões internacionais acordados neste campo.

Quarta

Por ocasião deste Seminário, celebrado em Santa Cruz de la Sierra, organizaram-se diversos painéis temáticos orientados para o intercâmbio de experiências. Isso permitiu aos assistentes expor a regulamentação legal existente nos respetivos países relativamente a alguns dos tipos penais enquadráveis no âmbito da cibercriminalidade, como é o caso dos crimes de pornografia infantil, ataques aos sistemas de informação, fraude através da Internet, violação de direitos de propriedade intelectual e do fenómeno de radicalização através da Internet (crimes de ódio e de terrorismo).

Os painéis, que se estruturaram numa exposição introdutória seguida de debate aberto entre todos os assistentes, tornaram possível conhecer o desenvolvimento penal substantivo dos ordenamentos jurídicos dos diferentes países e a experiência adquirida na aplicação prática dos mesmos.

Igualmente se considerou de interesse partilhar os desafios que se colocam na investigação tecnológica, em particular quanto ao modo de compaginar a utilização eficaz dos novos métodos de investigação criminal com a salvaguarda dos direitos e liberdades das pessoas. Neste âmbito, mais do que na área do direito penal substantivo, constataram-se importantes lacunas nos ordenamentos jurídicos internos de alguns Estados. Em relação a essa matéria evidenciou-se a necessidade de abordar reformas específicas, devidamente harmonizadas com os *standards* internacionais, de modo a que seja possível que as provas digitais se obtenham e conservem nos diferentes países com as condições e garantias necessárias à sua utilização em processos penais que correm noutros Estados.

Quinta

No decurso do Seminário constatou-se claramente que a enorme complexidade técnica e a evolução constante das novas tecnologias exigem uma intervenção especializada por parte do Ministério Público. Para tanto será imprescindível a capacitação específica e permanente de quem tenha de atuar contra esta forma de criminalidade.

Não obstante, dada a crescente necessidade de recorrer a provas digitais na generalidade das investigações por qualquer tipo de crime, a capacitação nesta matéria deverá também envolver, pelo menos nos aspetos básicos, todos os membros das *Fiscalias*/Ministérios Públicos que tenham a seu cargo a investigação e prossecução penal.

Sexta

A complexidade técnica e jurídica que carateriza a investigação tecnológica, e a experiência adquirida nalguns países, tornam aconselhável a criação de unidades especializadas nas *Fiscalias* ou Ministérios Públicos, já que somente por esta via se logrará incrementar a eficácia e a capacidade de atuação contra este fenómeno criminal e, ao mesmo tempo, melhorar a coordenação – nacional e internacional – das investigações por factos desta natureza.

Sétima

1. As especiais conotações da cibercriminalidade, a sua natureza transnacional e a diversidade das suas manifestações ilícitas incrementam a complexidade destas investigações, especialmente no que concerne ao procedimento de obtenção e conservação de provas, devido à sua volatilidade, o que, com frequência, coloca dúvidas quanto à sua validade e eficácia para o exercício da ação penal, dificultando a prossecução e punição destes crimes.

As lacunas legislativas, a insuficiente ou inexistente especialização do Ministério Público e dos demais intervenientes no processo, assim como as deficiências na cooperação institucional e judiciária, dificultam a atuação dos responsáveis pela investigação e incrementam o risco de impunidade, favorecendo os autores desses factos ilícitos.

Neste contexto,

a) Afigura-se essencial que as *Fiscalias*/Ministérios Públicos dos diferentes Estados iberoamericanos estabeleçam vias de comunicação para intercambiar experiências práticas e informação atualizada dos sistemas penais substantivos e processuais de cada país.
b) Afigura-se também fundamental fortalecer os instrumentos internacionais, judiciários e de cooperação interinstitucional – formais e informais – para poder transmitir e solicitar com agilidade a informação necessária às investigações.

2. Os assistentes ao Seminário, conscientes de que só com uma atuação especializada, coordenada, articulada e ágil se poderão alcançar resultados efetivos na luta contra a cibercriminalidade, consideram oportuna a criação de uma Rede ou Sistema articulado de pontos de contacto especializados em cibercriminalidade, integrada por membros de todas e cada uma das *Fiscalias* e Ministérios Públicos Iberoamericanos.

O objetivo deste projeto é o de promover e melhorar a informação disponível sobre os diferentes sistemas jurídicos iberoamericanos no âmbito da cibercriminalidade, potenciar o intercâmbio de experiências e conhecimentos necessários para solucionar os múltiplos problemas que se colocam nesta área, criar e difundir boas práticas entre os seus integrantes e optimizar e agilizar a cooperação institucional e a tramitação, pelos seus canais regulamentares, das solicitações de assistência internacional relacionadas com os crimes informáticos entre os países.

3. No entendimento de que estes objetivos da Rede coincidem com os pretendidos pela AIAMP, em particular os constantes das alíneas f), g), i), j) y k) do artigo 3º dos seus Estatutos, assim como com a

aspiração e os objetivos da IberRed (artigo 4º do seu Regulamento), os participantes no Seminário propõem que este entramado de pontos de contacto especializados contra a cibercriminalidade das *Fiscalias*/Ministérios Públicos Iberoamericanos se integre na IberRed, servindo-se de toda a sua estrutura administrativa e organizativa, incluindo a plataforma Iber@, já que a mesma dispõe da configuração e dos meios adequados para tornar possível a relação permanente, num espaço próprio, entre os pontos de contacto e utilizadores.

4. Para início de implementação deste projeto é imprescindível que em cada uma das *Fiscalias*/Ministérios Públicos Iberoamericanos se designe pelo menos um *Fiscal* / Magistrado do Ministério Público que atue como ponto de contacto, sem prejuízo de, tendo em conta as caraterísticas da Instituição em causa, se poder designar um número superior de contactos. Neste último caso, será conveniente que em cada *Fiscalia* ou Ministério Público se designe um coordenador nacional nessa matéria, que atue como intermediário com a Secretaria Geral da IberRed e com as restantes *Fiscalias* ou Ministérios Públicos.

Também se considera conveniente que a Rede, no seu conjunto, se articule em torno de um coordenador geral, encarregado da sua dinamização e demais funções que, em momento próprio, se determinem.

5. A fim de tornar efetivo este projeto, os assistentes ao Seminário acordaram em elevar esta iniciativa à próxima Assembleia-Geral da AIAMP, expondo a conveniência do imediato início de funcionamento de uma Rede ou Sistema articulado de pontos de contacto, fazendo chegar a esta Instituição a necessidade de constituir um grupo de trabalho com o objetivo de definir as linhas essenciais para o seu desenvolvimento. Esse grupo de trabalho poderia ser integrado pelos próprios pontos de contacto que vão sendo designados pelos respetivos *Fiscales Generales* / Procuradores-Gerais.

É por isso que, se aprovada esta proposta, se solicita à AIAMP que demande aos *Fiscais*/Procuradores-Gerais a nomeação, com a maior brevidade, de um ponto de contacto para esta Rede, com a finalidade

de que se integre no grupo de trabalho. Igualmente importa que aquele organismo inste da IberRed os recursos necessários para efectivar este projeto.

Tendo em vista o início de funcionamento deste projeto, sugere-se a possibilidade de a AIAMP atribuir a uma das *Fiscalias*/Ministérios Públicos Iberoamericanos a responsabilidade de impulsionar as atividades dirigidas a esse fim.

Estas conclusões serão feitas chegar à próxima Assembleia-Geral da Associação Iberoamericana de Ministérios Públicos, que terá lugar em Santa Cruz de la Sierra (Bolívia) nos dias 28 e 29 de outubro de 2015.

Santa Cruz de la Sierra, 9 de outubro de 2015

Anexo I - Lista de participantes

Argentina	Horacio Azzolin	Procuración General de la Nación Cibercrimen
Bolivia	Eliana Tejerina Rocha	Ministerio Público de Bolivia
Brasil	Carlos Bruno Ferreira da Silva	Procuradoria-Geral da República
Cuba	Eugenio Raul Martinez González	Fiscalía General de la República Cuba
Ecuador	Jorge San Lucas	Fiscalía General del Estado Ecuador
Ecuador	Alain Luna	Fiscalía General del Estado Ecuador
España	María Elvira Tejada de la Fuente	Coordinadora Nacional contra la Criminalidad Informática Fiscalía General del Estado España
España	Ana María Martin Martín	Fiscalía General del Estado España
Honduras	Yeymy Sugey Palacios Pereira	Ministerio Público Honduras
México	Daniela Hernández López	Procuraduría General de la República- Policía Federal Ministerial
Panamá	Ricaurte Donato González Torres	Procuraduría General de la Nación Panamá
Paraguay	Alfirio González Sandoval	Fiscalía General del Estado

		Paraguay
Portugal	Maria de Lurdes Lopes	Procuradoria-Geral da República
Portugal	Pedro Verdelho	Procuradoria-Geral da República, Gabinete Cibercrime

gabinete CIBERCRIME

aecid CENTRO DE FORMACIÓN

FISCALIA GENERAL DEL ESTADO

Asociación Ibero Americana de Ministerios Públicos

Red Iberoamericana de Cooperación Jurídica Internacional

Anexo II – Agenda

Seminário sobre *CIBERCRIME E PROVA DIGITAL*	Seminario sobre CIBERDELINCUENCIA Y PRUEBA DIGITAL
5 a 9 de Outubro de 2015 **Santa Cruz de la Sierra, Bolívia**	**5 a 9 de Octubre de 2015** **Santa Cruz de la Sierra, Bolivia**

AGENDA	AGENDA
5 de Outubro de 2015 **9:30** – Receção dos participantes **10:00** – Sessão de abertura **10:30** – Pausa **11:00** - *Conferência inaugural: Desafios da luta contra o cibercrime no quadro do Estado de Direito* – Pedro Verdelho - Portugal **13:00** – Almoço **14:30** – *O enquadramento legislativo internacional - A harmonização normativa com base na Convenção de Budapeste* – Pedro Verdelho - Portugal **6 de Outubro de 2015** **9:30** – *A articulação dos tipos penais perante as novas formas de atuação delitiva: em particular a luta contra a pornografia infantil na Internet* – Daniela Hernandez Lopez – México **11:00** – Pausa **11:30** - *A articulação dos tipos penais perante as novas formas de atuação delitiva: em particular os ataques a sistemas de informação* – Jorge Luis San Lucas González - Equador **13:00** – Almoço **14:30** - *A articulação dos tipos penais perante as novas formas de atuação delitiva: em particular as burlas através da Internet* – Horacio Azzolin - Argentina **16:00** - *A articulação dos tipos penais perante as novas formas de atuação delitiva: em particular os direitos da propriedade intelectual* - Ricarte Donato González - Panamá	**5 de Octubre de 2015** **9:30** – Acreditaciones **10:00** - Inauguración **10:30** – Pausa **11:00** - *Conferencia inaugural: Desafíos en la lucha contra la ciberdelincuencia en el marco del Estado de Derecho* - Pedro Verdelho - Portugal **13:00** – Almuerzo **14:30** – *El marco legislativo internacional - La armonización normativa sobre la base del Convenio de Budapest* - Pedro Verdelho - Portugal **6 de Octubre de 2015** **9:30** - *La articulación de tipos penales ante las nuevas formas de actuación delictiva; en particular la lucha contra la pornografía infantil en la red* – Daniela Hernandez Lopez – México **11:00** – Pausa **11:30** - *La articulación de tipos penales ante las nuevas formas de actuación delictiva: en particular los ataques a los sistemas de información* – Jorge Luis San Lucas González - Ecuador **13:00** – Almuerzo **14:30** - *La articulación de tipos penales ante las nuevas formas de actuación delictiva; en particular la defraudación a través de la red* - Horacio Azzolin - Argentina **16:00** - *La articulación de tipos penales ante las nuevas formas de actuación delictiva; en particular los derechos de propiedad intelectual* - Ricarte Donato González - Panamá

gabinete CIBERCRIME

aecid CENTRO DE FORMACIÓN

FISCALIA GENERAL DEL ESTADO

Asociación Ibero Americana de Ministerios Públicos

Red Iberoamericana de Cooperación Jurídica Internacional

7 de Outubro de 2015 **9:30** - *A articulação dos tipos penais perante as novas formas de atuação delitiva: em particular a radicalização através da Internet: crimes de ódio e terrorismo* – Elvira Tejada - Espanha **11:00** – Pausa **11:30** – *A cooperação internacional como mecanismo essencial na luta contra o cibercrime: Instrumentos disponíveis no quadro da Convenção de Budapeste* **-** Pedro Verdelho - Portugal **13:00** – Almoço **14:30** - *A cooperação internacional como mecanismo essencial na luta contra o cibercrime: implementação de instrumentos e canais existentes no contexto ibero-americano* - Ana Maria Martín - Espanha **16:00** – *O Reforço da coordenação entre os Ministérios Públicos dos países ibero-americanos: pistas para a criação de um grupo de trabalho de âmbito ibero-americano* - Ana María Martin - Espanha	**7 de Octubre de 2015** **9:30** - *La articulación de tipos penales ante las nuevas formas de actuación delictiva: en particular la radicalización a través de la red: crímenes de odio y terrorismo* – Elvira Tejada - España **11:00** – Pausa **11:30** – *La cooperación internacional como mecanismo esencial en la lucha contra el cibercrimen: instrumentos disponibles en el marco del Convenio de Budapest* - Pedro Verdelho - Portugal **13:00** – Almuerzo **14:30** - *La cooperación internacional como mecanismo esencial en la lucha contra el cibercrimen: instrumentos y canales existentes en el contexto iberoamericano* - Ana María Martín España **16:00** - *Reforzamiento de la coordinación entre los Ministerios Públicos de los países Ibero americanos: apuntes para la creación de un grupo de trabajo en el ámbito iberoamericano* - Ana María Martin - España
8 de Outubro de 2015 **9:30** - *O desafio da investigação tecnológica: novos métodos de investigação criminal; a salvaguarda dos direitos e liberdades das personas - em particular, conservação de dados e proteção da privacidade* – Elvira Tejada - Espanha **11:00** – Pausa **11:30** - *Mesa Redonda: Análise de mecanismos concretos de investigação:* Apresentação Introdutória - Carlos Bruno Ferreira da Silva - Brasil **13:00** – Almoço **14:30** - *A especialização do Ministério Público como forma de atuar frente à delinquência* - Argentina, Brasil, Espanha e Portugal	**8 de Octubre de 2015** **9:30** - *El desafío de la investigación tecnológica: nuevos métodos de investigación criminal; la salvaguarda de los derechos y libertades de las personas - en particular, conservación de datos y protección de la privacidad* – Elvira Tejada - España **11:00** – Pausa **11:30** - *Mesa Redonda: Análisis de mecanismos concretos de investigación:* Ponencia introdutória - Carlos Bruno Ferreira da Silva - Brasil **13:00** – Almuerzo **14:30** - *La especialización del Ministerio Fiscal como forma de actuar frente a la delincuencia:* Argentina, Brasil, España y Portugal
9 de Outubro de 2015 **9:30** – Elaboração e aprovação de conclusões **11:00** – Pausa **12:30** – Sessão de Encerramento	**9 de Octubre de 2015** **9:30** - Elaboración y aprobación de conclusiones **11:00** – Pausa **12:30** – Sesión de Clausura

gabinete CIBERCRIME

aecid CENTRO DE FORMACIÓN

FISCALIA GENERAL DEL ESTADO

Asociación Ibero Americana de Ministerios Públicos

Red Iberoamericana de Cooperación Jurídica Internacional

ANEXO 26

Despacho da Sra. PGR

MINISTÉRIO PÚBLICO
PORTUGAL
EM DEFESA DA LEGALIDADE DEMOCRÁTICA

Despacho

A XXIII Assembleia-Geral da Associação Iberoamericana de Ministérios Públicos (AIAMP), realizada em outubro de 2015, em Santa Cruz de la Sierra, Bolivia, aprovou a proposta do Ministério Público de Portugal para constituição de uma Rede Ibero-americana de Fiscales e Procuradores Especializados em Cibercriminalidade, integrada por todos os membros da AIAMP, tendo designado o Ministério Público português como coordenador da Rede.

Mais foi aprovado que o Ministério Público português se articule com a Secretaria-Geral da AIAMP para a constituição de um Grupo de Trabalho que inclua pontos de contacto de diversos membros da AIAMP, com o objetivo de dinamizar e definir as linhas essenciais para o desenvolvimento, implementação e funcionamento da rede.

Assim, com vista à concretização do mandato da Assembleia-Geral da AIAMP, designo o Senhor Procurador da República, Dr. Pedro Verdelho, Coordenador do Gabinete CiberCrime da Procuradoria-Geral da República, para, em articulação, em tudo o que se revelar necessário, com a Senhora Procuradora da República, Dra. Joana Ferreira, da Divisão de Cooperação Judiciária Internacional da PGR, e com a Senhora Procuradora da República, Dra. Maria de Lurdes Lopes, do Gabinete da Procuradora-Geral:

a. Desenvolver, tendo em conta as linhas de trabalho enunciadas, todas as diligências necessárias à constituição do Grupo de Trabalho aprovado pela XXIII Assembleia-Geral da AIAMP;
b. Impulsionar e coordenar os trabalhos de criação da Rede, com vista à sua apresentação, para aprovação, na XXIV Assembleia-Geral da AIAMP, a realizar nos dias 10 e 11 de outubro de 2016, em Lisboa.

Comunique:

Ao Senhor Secretário da Procuradoria-Geral da República

Ao Senhor Procurador da República, Dr. Pedro Verdelho e às Senhoras Procuradoras da República, Dra. Joana Ferreira e Dra. Maria de Lurdes Lopes.

Lisboa, 28 de junho de 2016

A Procuradora-Geral da República

(Joana Marques Vidal)

ANEXO 27

CiberRede - documento de conceito

MINISTÉRIO PÚBLICO
PORTUGAL
PROCURADORIA-GERAL DA REPÚBLICA

AIAMP
Asociación Ibero Americana de Ministerios Públicos

CiberRede / *CiberRed*

REDE IBERO-AMERICANA DE MINISTÉRIOS PÚBLICOS ESPECIALIZADOS EM CIBERCRIME

RED IBEROAMERICANA DE FISCALES ESPECIALIZADOS EN CIBERDELINCUENCIA

Documento de Conceito

Documento Conceptual

Contexto	*Contexto*
No decurso do Seminário Internacional sobre "Cibercrime e Prova Digital", organizado no âmbito da AIAMP e realizado no Centro de Formação da AECID de Santa Cruz de La Sierra (Bolívia), entre os dias 5 a 9 de Outubro de 2015, em concretização de deliberação da XXII Assembleia Geral da AIAMP (Montevideu), os assistentes, representantes dos Ministérios Públicos e *Fiscalias* da Argentina, Brasil, Bolívia, Cuba, Equador, Espanha, Honduras, México, Panamá, Paraguai e Portugal, concluíram que só com uma atuação especializada, coordenada, articulada e ágil se poderão alcançar resultados efetivos na luta contra a cibercriminalidade. Por essa razão, consideraram oportuna a criação de uma rede ou sistema articulado de pontos de contacto especializados em cibercriminalidade, integrada por membros de todas as *Fiscalias* e Ministérios Públicos Ibero-americanos. O objetivo de uma tal rede seria o de promover e melhorar a informação disponível sobre os diferentes sistemas jurídicos ibero-americanos no âmbito da cibercriminalidade, potenciar o intercâmbio de experiências e conhecimentos necessários para	*Durante el Seminario Internacional sobre "Cibercrimen y Prueba Digital", organizado en el marco de la AIAMP y celebrado en el Centro de Formación de la AECID, en Santa Cruz de la Sierra (Bolivia), los 5-9 octubre de 2015, en aplicación de la resolución de la XXII Asamblea General de la AIAMP (Montevideo), asistentes, representantes de los Ministerios Públicos y de las Fiscalías de Argentina, Brasil, Bolivia, Cuba, Ecuador, España, Honduras, México, Panamá, Paraguay y Portugal, llegaron a la conclusión de que solamente con una actuación especializada coordinada, articulada y ágil, se podrán lograr resultados eficaces en la lucha contra el cibercrimen. Por esta razón, han considerado oportuna la creación de una red o sistema articulado de puntos de contacto especializados en cibercrimen, integrada por miembros de todas las Fiscalías y Ministerios Públicos iberoamericanos.* *El objetivo de dicha red sería el de promover y mejorar la información disponible sobre los diferentes sistemas jurídicos iberoamericanos en el ámbito de la criminalidad cibernética, mejorar el intercambio de experiencias y conocimientos necesarios para*

solucionar os múltiplos problemas que se colocam nesta área, criar e difundir boas práticas entre os seus integrantes e otimizar e agilizar a cooperação institucional e a tramitação, pelos seus canais regulamentares, das solicitações de cooperação judiciária internacional, relacionadas com os crimes informáticos, entre os países. Esta rede de magistrados especializados em cibercriminalidade das *Fiscalias* e Ministérios Públicos ibero-americanos será mais eficaz se se integrar na IberRed, servindo-se de toda a sua estrutura administrativa e organizativa, incluindo a plataforma Iber@, já que a mesma dispõe da configuração e dos meios adequados para tornar possível a relação permanente, num espaço próprio, entre os pontos de contacto e utilizadores. A XXIII Assembleia Geral da AIAMP (Santa Cruz de la Sierra) deliberou a constituição desta rede, apontando as respetivas conclusões no sentido de que Portugal se articule com a Secretaria Geral da AIAMP tendo em vista a constituição de um grupo de trabalho, constituído por diversos membros da AIAMP, que dinamize e defina as linhas essenciais para o desenvolvimento, implementação e funcionamento da rede.	*solucionar los muchos problemas que se plantean en este ámbito, crear y difundir buenas prácticas entre sus miembros y optimizar y agilizar la cooperación institucional y los trámites procesales, por sus canales reglamentarios, de las solicitudes de cooperación judicial internacional relacionados con la delincuencia informática entre los países.* *Dicha red de fiscales especializados en ciberdelincuencia de las Fiscalías y Ministerios Públicos iberoamericanos será más eficaz si se integra en IberRed, haciendo uso de toda su estructura administrativa y organizativa, incluyendo la plataforma Iber@, ya que la misma dispone de la configuración y de los medios adecuados a tornar posible la relación permanente, en un espacio adecuado, entre los puntos de contacto y usuarios.* *La XXIII Asamblea General de AIAMP (Santa Cruz de la Sierra) aprobó la creación de esta red, señalando las conclusiones respectivas en el sentido de que Portugal se articule con la Secretaría General de AIAMP con el propósito de la creación de un grupo de trabajo, integrado por diversos miembros de la AIAMP, que dinamice y establezca las líneas esenciales al desarrollo, implementación y operación de la red.*
Linhas orientadoras	*Líneas de orientación*
Propósito geral • Intensificar o relacionamento entre os Ministérios Públicos na área da cibercriminalidade e da prova digital. • Permitir a troca de experiências e de boas práticas. • Facilitar a cooperação no caso concreto. Objetivos	*Propósito general* • *Intensificar la relación entre las Fiscalías y los Ministerios Públicos en el ámbito de la delincuencia cibernética y la prueba digital.* • *Permitir el intercambio de experiencias y buenas prácticas.* • *Facilitar la cooperación en el caso concreto.* *Objetivos*

• Ser um fórum permanente, de contacto e intercâmbio. • Propiciar discussão de tendências na cibercriminalidade e na obtenção de prova digital.	• *Ser un foro permanente de contacto y el intercambio.* • *Proporcionar discusión sobre las tendencias de la ciberdelincuencia y la obtención de prueba digital.*
Linhas de Ação	*Líneas de Acción*
1. Rede de pontos de contacto em cada Procuradoria / *Fiscalía* Cada ponto de contacto representará a sua instituição na rede e nas suas reuniões. Providenciará apoio ou assistência a propósito de solicitações de cooperação internacional, na área da cibercriminalidade. (Para a eficaz implementação deste projeto é imprescindível que em cada uma das *Fiscalías* / Procuradorias se designe pelo menos um Fiscal / Magistrado do Ministério Público que atue como ponto de contacto, sem prejuízo de, tendo em conta as caraterísticas da instituição em causa, poder ser designado um número superior de pontos de contacto. Neste último caso, será conveniente que em cada *Fiscalía* ou Procuradoria se designe um coordenador nacional, que atue como intermediário com a Coordenação da Rede e a Secretaria Geral da IberRed e com as restantes *Fiscalías* ou Ministérios Públicos). 2. Reunião anual Destina-se a permitir a partilha de atualizações legislativas e operacionais e também a discussão de novas práticas e métodos. Suporá a abordagem de temáticas estratégicas específicas (ex: especialização de magistrados, harmonização legislativa, adesão a instrumentos internacionais em vigor, necessidades de formação).	*1. Red de puntos de contacto en cada Procuraduría / Fiscalía* *Cada punto de contacto representará a su institución en la red y sus reuniones.* *Proporcionará apoyo o asistencia en relación con las solicitudes de cooperación internacional en materia de delito cibernético.* *(Para la aplicación eficaz de este proyecto es esencial que en cada una de las Fiscalías / Procuradurías se designe al menos un Fiscal / Magistrado del Ministerio Público que funcione como punto de contacto, sin perjuicio de, teniendo en cuenta las características propias de cada institución, poder ser designado un número superior de puntos de contacto. En este último caso, será conveniente que en cada Fiscalía o Ministerio Público, se designe a un coordinador nacional, como intermediario con la Coordinación de la Red y la Secretaría General de IberRed, bien como con las restantes Fiscalías o Ministerios Públicos).* *2. Reunión Anual* *Se destina a permitir compartir actualizaciones legislativas y operativas y también a la discusión de nuevas prácticas y métodos.* *Supondrá un enfoque temático estratégico específico (por ejemplo, especialización de los magistrados, armonización legislativa, adhesión a instrumentos internacionales vigentes o necesidades de formación).*

3. Plataforma *online* de partilha de informação (baseada na plataforma Iber@) Incluirá legislações nacionais, substantivas e processuais. Descreverá as estruturas legais e judiciárias nacionais (para facilitar e agilizar a cooperação). Dará apoio à rede de pontos de contacto.	*3. Plataforma online para compartir información (basada en la plataforma Iber@)* *Incluirá las leyes nacionales, sustantivas y procesales.* *Describirá las estructuras legales y judiciales nacionales (para facilitar y agilizar la cooperación).* *Providenciará apoyo a la red de puntos de contacto.*
Estrutura orgânica	*Estructura orgánica*
Coordenação, exercida pela Procuradoria / *Fiscalía* que for designada para o efeito pela Assembleia Geral. Pontos de Contacto, indicados por cada uma das Procuradorias / *Fiscalías* por período indeterminado (até a respetiva entidade indicar a sua substituição) e ainda, caso seja designado mais que um ponto de contacto, um Coordenador Nacional dos pontos. A Secretaria Geral da IberRed apoiará a Coordenação da Rede na implementação desta e nas suas atividades futuras, bem como assumirá o encargo de integrar a Rede na Iber@.	*Coordinación, ejercida por la Fiscalía / Procuraduría, que sea designada a tal efecto por la Asamblea General.* *Puntos de contacto indicados por cada Fiscalía / Procuraduría, por un período indeterminado (hasta que su entidad indique su reemplazo) y también, si hay más de un punto de contacto designado, un Coordinador Nacional de los puntos.* *La Secretaría General de IberRed apoyará la Red en su implementación e en sus actividades futuras; del mismo modo, asumirá la tarea de integrar la Red en Iber @.*
Reunião fundadora	*Reunión de fundación*
Sendo a rede aprovada no decurso da Assembleia Geral de Outubro de 2016, a realizar em Lisboa, propõe-se a realização de uma reunião fundadora da rede, durante o primeiro trimestre de 2017, com a participação dos pontos de contacto entretanto indicados. Esta reunião teria como propósito abordar a temática estratégica específica do "cibercrime no espaço Ibero-Americano - os fenómenos criminais e a legislação", definir os objetivos estratégicos da CiberRede para o próximo triénio e ainda fixar a temática estratégica específica e o formato da subsequente reunião da rede.	*Una vez aprobada la red, durante la Asamblea General de octubre de 2016, que tendrá lugar en Lisboa, se propone llevar a cabo una reunión de constitución de la red durante el primer trimestre de 2017, con la participación de los puntos de contacto nacionales.* *Esta reunión se destina a abordar el tema estratégico específico de "delito cibernético en el espacio iberoamericano – los fenómenos criminales y la ley", establecer los objetivos estratégicos de CiberRed para los próximos tres años y también determinar la estrategia temática específica y el formato de la subsiguiente reunión de la red.*

ANEXO 28

Programa da visita da delegação turca

MINISTÉRIO PÚBLICO
PORTUGAL
EM DEFESA DA LEGALIDADE DEMOCRÁTICA
gabinete CIBERCRIME

TAIEX Study Visit on the Convention on Cybercrime and computer related crimes

21.01.2016

Rua do Vale de Pereiro, 2, 3º, Lisboa

Turkish Delegation:

- Mr Ekrem Cetinturk,
- Mr Musa Heybet
- Mr Mehmet Okmen

Interpreter:

- Mr Huseyin Yilmaz

Portuguese Prosecutor General's Office – Cybercrime Office
Procuradoria-Geral da República – Gabinete Cibercrime

- Pedro Verdelho

Portuguese Ministry of Justice

- Fernando de Sousa Jr.

AGENDA

Chair : Pedro Verdelho, Coordinator of the Cybercrime Office

10:00	Arrival of the Turkish Delegation
10:05	Meeting and presentation, by the Turkish Delegation, of the scope and objectives of the visit.
10:10	Presentation: The Cybercrime Office
10:30	Coffee break
11:30	Presentation: The Portuguese Cybercrime Law – substantive provisions; discussion
12:30	Lunch break
14:00	Presentation: The Portuguese Cybercrime Law – procedural provisions; discussion
15:30	Coffee break
16:00	Discussion with the Turkish Delegation
17:00	End of the visit

ANEXO 42

Comentários da PGR de Portugal

gabinete CIBERCRIME

Portuguese Contribution,

regarding the Points for Discussion, on the

BACKGROUND PAPER SESSION I

THE CJEU'S ANNULMENT OF THE DATA RETENTION DIRECTIVE:

PRACTICAL IMPLICATIONS FOR INVESTIGATIONS AND PROSECUTIONS

1. The Forum would appreciate being informed of whether, and if so to what extent, in your Member State the annulment of the DRD affected:

1.1. the prevention, detection, investigation and prosecution of serious offences

1.2. judicial cooperation within the EU

The decision of 8 April 2014, so far, did not affect prevention, detection, investigation and prosecution of serious offences or judicial cooperation.

In fact, even if, so far, the question was not submitted to the courts – and it may certainly be in the future -, the common understanding, within both the judicial community and the telecom operators is that the Law which transposed the Directive is in force.

This act, Law 32/2008, besides of transposing the Directive 2006/24EC, introduced a complex framework regulating data retention (for example the rules that have to be observed, the personnel that can access the data, storage conditions and precise rules to access the data). Thus, most of the requirements of the ruling of the ECJ are already considered in the domestic law. For that reason, it is understood that the ruling didn't affect the validity of the national law.

2. In your opinion, how may national data retention laws be aligned to the criteria set forth in the DRD Judgment, in a manner that reconciles the need for procedural safeguards with the demands for efficacy in criminal investigations and the unpredictability of crime?

As said, some of the requirements of the judgment are already covered by the Portuguese law. Thus, other member States can do the same.

For example, the Portuguese law provides conditions to access data, stating that an order from a judge is always required to disclose the data (Article 9, 1 of Law 32/2008). This matches the requirement of the court

when states that the Directive does not provide the *authorisation and or supervision of an independent authority.*

On the other hand, the court states that the Directive does not provide for an obligation to destroy the data after the retention period. The Portuguese law states exactly the opposite, imposing the destruction of the data after the retention period (Article 7, 1, e, of the Law 32/2008).

Regarding maintaining the data, the ECJ also underlined the lack of requirements. Again, the Portuguese law includes rules that have to be observed, including multiple safeguards (for example, who is authorised to access the data, storage conditions and other).

However, some of the conditions described by the ECJ ruling are absolutely unable to fulfil, by its nature.

In fact, the ruling if the European court states that the data retention is indiscriminate and has no linking to fighting serious crime and, on the other hand, the retained data don't refer to suspicious persons.

With all respect, the court is leading the discussion to an inconsistent path: in fact, data retention is needed and useful, as the court recognises, because it is indiscriminate, on one hand, and covers all the citizens, on the other. In fact, if the suspect is already under investigation, then, there are other instruments to perverse the data which refers to him. Data retention, as it is understood, is just useful if the data refer to all the citizens.

This is also the reason why, with all the respect, it does not make any sense the statement of the court saying that the retention should vary according to the persons concerned or the different categories of data.

When data are retained, no one knows that those data will be needed, one day, as evidence of a crime. The retained data can be used as evidence of a crime because they were preserved indiscriminately. The data in case are already preserved when the investigation needs them – not data to preserve, in the future. It does not make sense to require that the retention only refers to already identified criminals – in this case, interception of communications can be eventually an option, but only referring to future crimes.

It is impossible to preserve data for future evidentiary purposes if the data refers to crimes or criminals that are not yet known.

To have, or not to have, data retention is an option. But if it is recognised acknowledge that the retention of data genuinely satisfied an objective of general interest in the fight against serious crime, than, it has to be made indiscriminately referring to all the citizens.

The point is not general retention or limited and oriented retention (that is unfeasible). The point is the complex of safeguards around storage and disclosure of the data. It is also a major point that the data are retained solely to be used in criminal proceedings (for serious crimes) – and not, for example, for the purposes of national security or intelligence.

3. In your view, how could Eurojust further assist national competent authorities in overcoming challenges in judicial cooperation arising from the lack of harmonised national data retention regimes?

The only thing that Eurojust can do, at this respect, is to support the revision of the regulations all over Europe, reintroducing legal frameworks creating the obligation of the retention of data.

4. The Forum would be grateful for the opinion of its members regarding those remedies you consider could be effective in addressing the current fragmented data retention framework amongst Member States and challenges deriving therefrom. In particular, do you believe there to be a need for a solution at EU level?

Yes, indeed.
The ruling of the ECJ affected a European instrument. Even if there is no direct and immediate connexion between the invalidity of that European instrument and the domestic laws of the Member States, in fact, the consequences of that ruling were pretty clear in some Member States, because the direct and immediate source (at least of inspiration…) of their domestic regulations was exactly that instrument. An EU binding instrument, that the Member States had to transpose, mandatorily, was invalidated, with very serious consequences to the domestic legal frameworks.
Thus, the EU should not leave each of the Member States alone, when finding a solution to this problem.

ANEXO 43

Agenda da reunião do grupo apoio

MINISTÉRIO PÚBLICO
PORTUGAL
EM DEFESA DA LEGALIDADE DEMOCRÁTICA
gabinete CIBERCRIME

Reunião do
Grupo Técnico de Apoio ao
Gabinete Cibercrime

(na Procuradoria-Geral da República – Rua do Vale de Pereiro, 2, 3º Andar)

11 de Fevereiro de 2016

10:30 – Abertura e breve introdução dos trabalhos

- O Plano de Ação Cibercrime 2015 – 2016 (referência geral)
    - opções estratégicas
    - reformulação da rede de pontos de contacto
    - sessões nas comarcas

11:00 – Referência a algumas iniciativas pendentes

- Cooperação com o NCMEC
- Linguística forense

11:15 – Novos projetos e novas iniciativas

- eventual estrutura de emergência (24/7) para recolha de participações emergentes e de prova digital urgente – e em particular *online*;

12:45 – Pausa para almoço

14:00 – Novos projetos e novas iniciativas (continuação)

- articulação do Ministério Público com os OPC na área do cibercrime e da obtenção de prova digital (formulário de prova digital; formulário de apreensão de telefones; formulário de queixa por furto de telemóvel);
- iniciativa na área das burlas *online*

16:00 – Encerramento

Lista de participantes

nome	colocação	endereço de email
João Conde Correia	PGD do Porto	joaocondecorreia@gmail.com
José Eduardo Lima	PGD do Porto	ze.limas@gmail.com
Marta Viegas	DCIAP	marta.viegas@pgr.pt
Miguel Rodrigues	DIAP de Leiria	miguel.j.rodrigues@mpublico.org.pt
Nuno Serdoura dos Santos	DIAP do Porto – Matosinhos	nunoserdoura@sapo.pt
Pedro Verdelho	Gabinete Cibercrime	pedro.verdelho@pgr.pt
Raúl Farias	Gabinete da Sra. PGR	raul.farias@pgr.pt
Rui Batista	Gabinete da Sra. PGR	rui.batista@pgr.pt

ANEXO 49

Nota Prática 9

NOTA PRÁTICA nº 9/2016
21 de setembro de 2016

Jurisprudência sobre cibercrime

Pretende-se com esta nota prática referenciar a jurisprudência de tribunais superiores sobre crimes informáticos e crimes cometidos por via de sistemas informáticos, publicada e disponível na Internet. Todos os acórdãos estão também referenciados no SIMP temático Cibercrime.

Não é propósito desta nota fazer a análise dos acórdãos, os quais se referem apenas com um curto sumário, deixando-se ainda muito brevíssimos comentários genéricos, de enquadramento, que somente pretendem dar pistas sobre a extensão e o sentido da jurisprudência.

O período temporal coberto termina na presente data e recua até 2009, ano da publicação da Lei do cibercrime, embora se incluam algumas decisões anteriores, por se manterem pertinentes.

1. Acesso ilegítimo

Das decisões mais antigas conhecidas sobre acesso ilegítimo, uma delas é já muito desatualizada, por ser anterior à Lei do Cibercrime (publicada em 15 de setembro de 2009) e a outra versa sobre a evolução do tipo descrito na lei anterior para o atual. Este último confirma as conclusões que o acórdão mais antigo formula, quanto à essência do tipo de crime, apesar de o tipo de crime de acesso ilegítimo da Lei do Cibercrime (Artigo 6º) ter substanciais alterações em relação ao seu congénere da Lei nº 109/91 (Artigo 7º). Por outro lado, o acórdão mais recente clarifica o intuito do tipo de crime, indo no sentido dos outros dois acórdãos.

Acórdão do Tribunal da Relação de Coimbra de 17 de fevereiro de 2016

- Comete o crime de acesso ilegítimo (Artigo 6º, nºs 1 e 4, al a, da Lei nº 109/2009), o inspetor tributário que, por motivos estritamente pessoais, acede ao sistema informático da Autoridade Tributária, consultando declarações de IRS de outrem. O tipo subjetivo daquele ilícito penal não exige qualquer intenção específica (como seja o prejuízo ou a obtenção de benefício ilegítimo), ficando preenchido com o dolo genérico de intenção de aceder a sistema)

Acórdão da Relação do Porto de 8 de janeiro de 2014

- O crime de acesso ilegítimo, previsto no Artigo 6º da Lei do Cibercrime (Lei nº 109/2009) incrimina exatamente a mesma factualidade que era incriminada pelo crime correspondente (Artigo 7º da Lei nº 109/91). Todavia, na lei nova, não se exige qualquer intenção específica (por exemplo, a de causar prejuízo ou a de obter qualquer benefício ilegítimo), apenas se exigindo dolo genérico. O bem jurídico protegido é a segurança dos sistemas informáticos.

Acórdão da Relação de Coimbra de 15 de outubro de 2008

- O bem jurídico protegido do crime de acesso ilegítimo é a segurança do sistema informático – a proteção ao designado "domicílio informático" algo de semelhante à introdução em casa alheia.

2. Falsidade informática

A generalidade das decisões publicadas sobre o crime de falsidade informática faz uma interpretação estrita e literal dos seus complexos elementos. Noutra vertente, não é pacífico o entendimento jurisprudencial quanto aos interesses jurídicos protegidos pelo tipo de crime.

Também quanto à falsidade informática se anota a virtude, que as decisões de tribunais superiores sempre têm, de discutir a inserção de casos concretos no tipo de crime. Neste caso é particularmente interessante a confrontação do tipo de crime (e de outros correlacionados) com atuações ilícitas relacionadas com cartões bancários.

Acórdão da Relação do Porto de 26 de maio de 2015

- No crime de falsidade informática (Artigo 3º nº 1, da Lei do Cibercrime), os dados informáticos têm de ser alterados com o propósito de desvirtuar a demonstração dos factos que com aqueles dados podem ser comprovados. Comete tal crime quem introduzir no sistema informático de um hospital episódios de cirurgias realizadas em regime de ambulatório como se tivessem sido levadas a cabo em regime de internamento, quando tal não correspondia à realidade. A relação jurídica que com este comportamento se cria não corresponde à verdade, sendo certo que os dados assim vertidos no sistema informático produzem os mesmos efeitos de um documento falsificado, pondo em causa o seu valor probatório e consequentemente a segurança nas relações jurídicas.

Acórdão da Relação de Évora de 19 de maio de 2015

- O tipo objetivo do crime de falsidade informática previsto no nº 1 do Artigo 3º da Lei do Cibercrime supõe que a interferência no tratamento informático de dados produza, como resultado, dados ou documentos não genuínos. O tipo supõe dolo, nas formas gerais e ainda, enquanto elemento subjetivo especial do tipo, a intenção de provocar engano nas relações jurídicas, bem como, relativamente à produção de dados ou documentos não genuínos, a particular intenção do agente de que tais dados ou documentos sejam considerados ou utilizados para finalidades juridicamente relevantes como se fossem genuínos. Este crime visa proteger a segurança das relações jurídicas enquanto interesse público essencial que ao próprio Estado de Direito compete assegurar e não a confidencialidade, integridade e disponibilidade de sistemas informáticos, de redes e de dados informáticos. O uso de documento não genuíno (nº 3 do Artigo 3º) apenas é punido se o for por pessoa distinta da que praticou a "falsificação". A utilização de nome de outrem para criar endereço de correio eletrónico traduz a produção de dados ou documentos não genuínos (mediante a introdução de dados informáticos) e é idóneo a fazer crer que foi a pessoa a quem respeita o nome quem efetivamente criou aquele endereço.

Acórdão da Relação do Porto de 17 de setembro de 2014

- Constitui o crime de contrafação de moeda falsa (Artigos 262º, nº 1 e 267º, nº 1, c) do Código Penal), o fabrico de cartão de crédito falso com inserção de banda magnética clonada de um cartão verdadeiro, por bastar para o preenchimento do tipo a interferência na banda magnética do cartão de crédito clonado. Constitui o crime de falsidade informática (Artigo 3º, nºs 1 e 2 da Lei 109/2009) a captura, em ATM, da informação existente na banda magnética de cartão de crédito.

Acórdão da Relação do Porto de 24 de abril de 2013

- O bem jurídico tutelado pelo crime de falsidade informática (Artigo 3º, nºs 1 e 3 da Lei do Cibercrime), não é o património, mas antes a integridade dos sistemas de informação, através do qual se pretende impedir os atos praticados contra a confidencialidade, integridade e disponibilidade de sistemas informáticos, de redes e dados informáticos, bem como a utilização fraudulenta desses sistemas, redes e dados.

Acórdão da Relação do Porto de 21 de novembro de 2012

- O crime de passagem de moeda falsa e o crime de falsidade informática estão em relação de concurso efetivo, porque protegem interesses diferentes: o primeiro, a fé pública na moeda, a segurança e funcionalidade do tráfego monetário e a integridade do sistema monetário; o crime de falsidade informática visa proteger a integridade dos sistemas de informação e a sua confidencialidade, integridade e disponibilidade.

Acórdão da Relação de Lisboa de 10 de julho de 2012

- O crime de falsidade informática previsto no Artigo 3º da Lei do Cibercrime não veio esvaziar de sentido a alínea c) do nº 1, do Artigo 267º, do Código Penal, continuando este preceito a abranger a conduta que se traduza em adulteração de cartões de crédito, uma vez que no crime de contrafação de moeda o bem jurídico protegido é a integridade ou intangibilidade do sistema monetário legal em si mesmo considerado, aqui representado pelos cartões de crédito por via da sua equiparação àquela.

Acórdão da Relação de Lisboa de 30 de junho de 2011

- O bem jurídico protegido pelo crime de contrafação de moeda é a intangibilidade do sistema monetário, incluindo a segurança e credibilidade do tráfego monetário; o bem jurídico protegido pelo crime de falsificação informática é a integridade dos sistemas de informação. Se a ação consiste em duplicar e utilizar cartões bancários, com acesso a dados que neles se encontravam, produzindo com estes dados documentos não genuínos para os utilizar no levantamento de dinheiro ou pagamento de bens, ocorrem, em concurso efetivo, aqueles dois crimes.

3. Burla informática

Com exceção das situações de facto relacionadas com levantamento de dinheiro em utilização indevida de cartões bancários, a jurisprudência sobre burla informática ainda é escassa. A referência legislativa é o Artigo 221º do Código Penal, introduzido em 1995 e alterado em 1998. Em geral, as decisões conhecidas incidem sobre a essência do tipo de crime, quer na sua generalidade, quer na relação com o tipo de crime de falsidade.

Acórdão do Tribunal da Relação do Porto de 3 de fevereiro de 2016

- A burla informática consiste num erro consciente provocado por intermédio da manipulação de um sistema de dados ou de tratamento informático. Não se exige um qualquer engano ou artifício por parte do agente, mas sim a introdução e utilização abusiva de dados no sistema informático.

Acórdão do Tribunal da Relação de Évora de 19 de novembro 2015

- A manipulação de dados de uma máquina ATM com o propósito de que a mesma, sem motivo legítimo, ejete uma grande quantidade de notas, preenche o tipo de crime de burla informática.

Acórdão da Relação do Porto de 30 de setembro de 2009

- Na burla informática a lesão do património produz-se através da intromissão nos sistemas e da utilização em certos termos de meios informáticos - é um crime de resultado, exigindo-se que seja produzido o prejuízo patrimonial de alguém.

Acórdão da Relação do Porto de 30 de abril de 2008

- Se a burla se realizou mediante a introdução de dados incorretos/falsos no sistema informático da Segurança Social, existe concurso efetivo de burla e falsidade informática.

4. Burla informática – cartões Multibanco

*No final da década de 1990, o Tribunal Constitucional (Acórdão nº 48/99, de 19 de janeiro de 1999) e o Supremo Tribunal de Justiça (Acórdãos de 2 de outubro de 1996 e de 19 de dezembro de 2001) deixaram entender que o levantamento indevido de dinheiro com cartões bancários ilegitimamente obtidos consubstanciava a prática de crime de furto (furto do cartão, primeiro, mas igualmente furto do dinheiro, depois). O "*pin*" do cartão ilegitimamente obtido era assim equiparado à chave de um cofre, que permitia a quem furtasse ou roubasse o cartão, também, furtar dinheiro.*

Na sequência da posição assumida na anotação ao Código Penal de Leal Henriques e Simas Santos, a ulterior jurisprudência das Relações passou a tender para considerar que esta atuação preenche o tipo de crime de burla informática, na medida em que supõe "utilização não autorizada de dados".

A jurisprudência mais recente é quase unânime nesse sentido, havendo, todavia, ainda alguma resistência do Supremo Tribunal de Justiça.

Acórdão da Relação de Évora de 20 de janeiro de 2015

- Quem subtraí um cartão multibanco alheio e, de seguida, levanta quantias em dinheiro de caixa de ATM, comete em concurso efetivo, dois crimes: um de furto e outro de burla informática.

Acórdão da Relação do Porto de 5 de junho de 2013

- Comete o crime de burla informática (Artigo 221º do CP) quem utiliza um cartão bancário de débito para pagamentos, sem autorização do legítimo titular do cartão, ainda que para o efeito não seja necessária a marcação de qualquer código. Este crime tutela a utilização correta dos meios informáticos e também o património de outrem.

Acórdão da Relação de Guimarães de 18 de dezembro de 2012

- O levantamento de dinheiro em caixas ATM com utilização do cartão de outrem e digitação do respetivo código de acesso sem autorização, com intenção de obter enriquecimento ilegítimo, causando a outra pessoa prejuízo patrimonial, integra uma das modalidades da ação típica do crime de burla informática.

Acórdão da Relação de Évora de 26 de junho de 2012

- A burla informática, consiste na manipulação dos sistemas informáticos, ou utilização sem autorização ou abusiva determinando a produção dolosa de prejuízo patrimonial; o tipo pretendeu abranger a utilização indevida de máquinas automáticas de pagamento.

Acórdão da Relação do Porto de 14 de março de 2012

- Uma das modalidades da ação típica do crime de burla informática, é a apropriação de dinheiro através da introdução e utilização no sistema informático das ATM de dados sem autorização (introdução do cartão e digitação do código de acesso), com intenção de obter enriquecimento ilegítimo, causando a outra pessoa prejuízo patrimonial.

Acórdão do Supremo Tribunal de Justiça de 5 de novembro de 2008

- A utilização de um cartão Multibanco obtido por via de violência ou coação, para levantamento de dinheiro é ainda parte da prática do crime de roubo, perdendo qualquer autonomia, ou estando mesmo tipicamente excluída, a integração do crime de burla informática).

Acórdão do Supremo Tribunal de Justiça de 29 de maio de 2008

- Se o agente do crime força a vítima a revelar o código secreto (PIN) do seu cartão de débito ou de crédito que lhe retira, para depois se apoderar dos proventos económicos que a utilização desse cartão

obtém através do sistema bancário, em prejuízo da vítima, há uma consumpção de normas entre os crimes de roubo e os de burla informática.

5. Reprodução ilegítima de programa protegido

Existia rica jurisprudência sobre o crime de reprodução ilegítima de programa protegido ao abrigo da antiga Lei da Criminalidade Informática, atualmente revogada (Lei nº 109/91). Talvez por se terem firmado, nesse tempo, orientações claras e, ainda também, por o tipo de crime não ter sofrido, da versão de 1991 para a de 2009, alteração substancial, é mais diminuta a jurisprudência sobre a lei vigente (a Lei do Cibercrime – Lei nº 109/2009). Os acórdãos referenciados abordam, todavia, três ideias basilares: por um lado, a de que é ilícito, quanto a um programa informático que se comprou licitamente, reproduzi-lo em número superior ao contratualmente previsto; por outro lado, a de que o crime não exige intenção lucrativa; por último, a de que os seus elementos típicos fulcrais (reprodução, divulgação e comunicação ao público) não são cumulativos, bastando-se o tipo de crime com apenas um de entre eles.

Acórdão do Tribunal da Relação de Lisboa de 8 de setembro de 2015

- De acordo com o Decreto-Lei nº 252/04, que criou o direito de autor sobre programas de computador, a autorização de utilização do programa não implica a transmissão dos direitos atribuídos ao autor do programa de computador - designadamente os direitos de reprodução, transformação e colocação em circulação.

Acórdão da Relação de Coimbra de 30 de outubro de 2013

- O tipo de crime de reprodução ilegítima de programa protegido não exige que, cumulativamente, haja reprodução, divulgação e comunicação ao público, bastando-se, por exemplo, com a instalação não autorizada de um programa informático protegido.

Acórdão da Relação de Coimbra de 12 de julho de 2006

- A instalação de um único programa informático licenciado em vários computadores de uma empresa traduz-se numa reprodução de programa não autorizada. O tipo de crime de reprodução de programa protegido não exige intenção de lucro.

6. Usurpação

A discussão jurisprudencial mais recente sobre a violação de direito de autor, na vertente criminal, incide sobre dois aspetos práticos: um deles é o da incriminação, ou não, de agentes que, apesar de terem sido encontrados na posse de com cópias ilegítimas de obras, não venderam as mesmas; o outro respeita à reprodução por sistemas de som (altifalantes), de obras (nomeadamente música), em áreas públicas (sobretudo cafés, bares, esplanadas ou similares). A respeito desta última problemática, a discussão jurisprudencial portuguesa está balizada pelo Acórdão de fixação de Jurisprudência do STJ de novembro de 2013, mas a questão não está encerrada nas instâncias da União Europeia.

Acórdão do Tribunal da Relação de Lisboa de 4 de fevereiro de 2016

- A transmissão de fonogramas através de aparelho de televisão e rádio com amplificador num estabelecimento comercial de café constitui execução pública, a que se refere o artigo 184º do Código do Direito de Autor e dos Direitos Conexos, que necessita de autorização dos respetivos produtores. Não estando autorizada a execução pública dos fonogramas, procede a providência cautelar com a imposição da proibição de continuação da execução e com a condenação de uma sanção pecuniária compulsória, mas já não procede na parte em que é pedido o encerramento do estabelecimento, por ser uma medida desproporcionada e desnecessária, nem a apreensão dos bens em causa e o livre acesso ao estabelecimento para fiscalização, por serem medidas também

desnecessárias, já que se trata de um estabelecimento aberto ao público em que facilmente se controla o cumprimento ou não da medida de proibição decretada.

Acórdão do Tribunal da Relação de Coimbra de 20 de janeiro de 2016
- Constitui mera receção e não reutilização da obra transmitida, a difusão de música ambiente de determinada estação emissora de rádio, através de várias colunas de som. Esta difusão não constitui crime de usurpação (Artigo 195º do Código do Direito de Autor e dos Direitos Conexos) e não carece de autorização dos autores das obras radiodifundidas por aquela estação emissora.

Acórdão do Tribunal da Relação de Guimarães de 11 de janeiro de 2016
- Quem adquire um conjunto de obras contrafeitas com o propósito de as vir a vender, preenche o tipo de crime do Artigo 199º do Código do Direito de Autor e dos Direitos Conexos na forma tentada. Porém, tendo em conta a moldura penal abstratamente aplicável para o crime consumado a prática deste ilícito típico na forma tentada não é punível (Artigos 22º, 23º do Código Penal e 197º nº1 CDADC).

Acórdão da Relação de Évora de 19 de novembro de 2013
- Pratica o crime de usurpação e/ou aproveitamento de obra usurpada quem colocar à venda cópias não autorizadas de fotogramas ou videogramas; mesmo que não tenha sido vendida nenhuma cópia, o crime consuma-se se o agente estava em local de venda, com intenção de venda e na posse de cópias ilegais.

Acórdão de fixação de jurisprudência do Supremo Tribunal de Justiça nº 15/2013, de 13 de novembro de 2013
- A aplicação, a um televisor, de aparelhos de ampliação do som, difundido por canal de televisão, em estabelecimento comercial, não configura uma nova utilização da obra transmitida, pelo que o seu uso não carece de autorização do autor da mesma, não integrando consequentemente essa prática o crime de usurpação (Artigos 149º, 195º e 197º do Código do Direito de Autor e dos Direitos Conexos).

Acórdão da Relação de Évora de 15 de outubro de 2013
- A emissão de programa televisivo, em estabelecimento aberto ao público, através de um televisor ligado a uma box da Cabovisão (e a nenhum outro dispositivo), sem que os titulares dos direitos de autor tivessem concedido uma autorização específica para este efeito, não preenche o tipo de ilícito de usurpação dos Artigos 195º e 197º do Código dos Direitos de Autor e dos Direitos Conexos.

Acórdão da Relação de Coimbra de 30 de março de 2011
- O crime de usurpação (Artigos 195º, 197º e 199º do CDADC) tutela o exclusivo de exploração económica da obra, que a lei reserva ao respetivo autor; o crime verifica-se quando ocorre uma utilização não autorizada, independentemente de o agente se propor obter qualquer vantagem económica; a utilização ou reprodução sem expressa autorização do autor apenas é permitida para fim exclusivamente privado, sem prejuízo para a exploração normal da obra e sem injustificado prejuízo dos interesses legítimos do autor.

7. Phishing

A jurisprudência sobre phishing *disponível é, toda ela, da jurisdição cível e respeita a casos em que aquilo que se discutia era a responsabilização, ou não, da instituição bancária, pela perda resultante de um ato criminoso. É colateral a esta a questão da culpa – e eventual responsabilidade – do "dono" da conta bancária, a qual apenas é reservada para casos de negligência grosseira.*

Acórdão da Relação de Lisboa de 15 de março de 2016

- O *phishing* constitui uma fraude eletrónica cuja consequência é a obtenção ilícita de dados de acesso a contas bancárias e a sua utilização subsequente em proveito do autor da fraude. Apenas há responsabilidade da vítima, se se determinar que ela, com negligência grave, permitiu ao defraudador o acesso às credenciais de acesso. Negligência grave (ou grosseira) corresponde à falta grave e indesculpável, consistente na omissão dos deveres a que se está adstrito, que só uma pessoa especialmente desleixada, descuidada e incauta deixaria de observar. Não se provando como o agente do crime obteve as credenciais, não pode qualificar-se a atuação da vítima como gravemente negligente.

Acórdão do Tribunal da Relação de Coimbra de 2 de fevereiro de 2016

- Não se tendo provado que o cliente forneceu a terceiros as chaves de acesso ao serviço de *homebanking* nem que, ao navegar na Internet, permitiu que outrem tenha capturado as credenciais de acesso e validação, recai sobre o banco a responsabilidade pela movimentação fraudulenta da sua conta bancária, através da internet (por via dos serviços de *homebanking*).

Acórdão da Relação de Évora de 25 de junho de 2015

- No âmbito do *homebanking*, em regra recai sobre o Banco depositário o ónus da prova de que a falta de cumprimento de regras de segurança não procede de culpa sua. Mas o Banco pode elidir aquela presunção, demonstrando a culpa do cliente, por exemplo, provando que o cliente beneficiário violou o contrato, divulgando na internet dados pessoais, secretos e intransmissíveis relativos ao seu acesso, em benefício de *hackers*. Age com culpa o utente que fornece todo o conteúdo do cartão matriz perante uma solicitação numa página idêntica à do Banco, uma vez que contraria toda a lógica do sistema de segurança que não pode ser desconhecida por parte do utilizador.

Acórdão da Relação de Lisboa de 3 de março de 2015

- Não se tendo apurado ter o cliente permitido o acesso de terceiros às suas credenciais, não se pode concluir ser imputável ao mesmo a quebra da confidencialidade dos dispositivos de segurança de acesso à sua conta bancária na Internet.

Acórdão da Relação de Guimarães de 17 de dezembro de 2014

- Num contrato de *homebanking*, o Banco tem a obrigação de assegurar que os dispositivos de segurança personalizados do instrumento de pagamento só sejam acessíveis ao utilizador de serviços de pagamento que tenha direito a utilizar o referido instrumento. O utilizador de serviços de pagamento responde pelas perdas resultantes de operações de pagamento não autorizadas se tiver agido com incumprimento deliberado de uma ou mais das suas obrigações. Pode ainda responder por aquelas perdas se tiver atuado com negligência grave, conceito que se pode definir como "negligência grosseira, erro imperdoável, desatenção inexplicável, incúria indesculpável, vistos em confronto com o comportamento do comum das pessoas, mesmo daquelas que são pouco diligentes".

Acórdão da Relação do Porto de 29 de abril de 2014

- No *homebanking*, incumbe ao Banco ilidir a presunção de culpa pelo perecimento de quantias cujo domínio lhe foi transferido por via contratual, ainda que a causa do perecimento resulte de acessos fraudulentos aos meios de movimentação de contas bancárias que disponibiliza aos seus clientes. Não age com culpa o depositante que por via de uma fraude informática levada a efeito por terceiros, na convicção que estava na página online do banco, introduziu numa página falsa, clonada da página daquele Banco, as suas certificações, pessoais e intransmissíveis, que abusivamente vieram a ser utilizadas no acesso, por terceiros, à conta de que era titular.

Acórdão da Relação de Lisboa de 12 de dezembro de 2013

- No *homebanking* compete ao banco diligenciar pela segurança, de modo a que o seu utilizador não fique privado dos valores nele depositados pelo abusivo acesso de terceiros; ou seja, o cliente tem de poder confiar nesse sistema de acesso à sua conta bancária e respetiva movimentação. Sobre o Banco impende a obrigação de prestar um serviço eficaz e seguro, correndo por sua conta o risco de acessos fraudulentos. Porém, se o cliente fizer uma utilização imprudente, negligente e descuidada desse serviço, revelando a terceiros, na internet, os seus códigos pessoais de acesso ou outros elementos de acesso ao serviço, não é exigível ao Banco o pagamento das quantias por aqueles indevidamente movimentadas.

Acórdão da Relação de Lisboa de 5 de novembro de 2013

- No serviço de *homebanking* é o banco quem tem que diligenciar para que o serviço seja seguro e nele possa o cliente confiar. Ignorando-se como é que os terceiros acederam às chaves ou códigos de acesso, recai sobre o banco o dever de reembolsar os autores dos montantes das operações de pagamento.

Acórdão da Relação do Porto de 29 de outubro de 2013

- Quando ocorre um caso de *phishing*, investe-se o ónus da prova de demonstrar que o computador do cliente defraudado foi infetado com um programa de código malicioso, que abriu uma brecha na respetiva segurança, permitindo a terceiros executar operações bancárias como se fossem os clientes do banco.

8. Pornografia de menores

Ainda é atomística a jurisprudência sobre pornografia de menores. Além disso, incide sobretudo sobre aspetos processuais ou, na parte substantiva, sobre aspetos de pormenor. Não obstante, nem por isso deixam de ser relevantes. É significativa a decisão que diz ser prescindível a concreta determinação da idade do menor/vítima. Já quanto à qualificação como crime do mero download *de ficheiros de pornografia infantil, instalou-se a discussão na jurisprudência.*

Acórdão do Tribunal da Relação de Évora de 2 de fevereiro de 2016

- As medidas de coação de "detenção na habitação com vigilância eletrónica" e "proibição de utilização de equipamentos informáticos e de acesso à internet", esta última sem possibilidade efetiva de fiscalização e controlo, revelam-se medidas insuficientes para acautelar o perigo de continuação da atividade criminosa relativamente a arguido acusado da autoria de 977 crimes de pornografia de menores cometidos no domicílio, justificando-se a aplicação de prisão preventiva.

Acórdão da Relação de Lisboa de 15 de dezembro de 2015

- Se não se provar intenção de partilha, fazer *download* de pornografia infantil constitui a prática de crime de aquisição ou detenção de pornografia de menores (Artigo 176°, n° 4, alínea d), do Código Penal). O *download* não constitui "importação de pornografia de menores" (crime previsto e punido pelo Artigo 176°, n ° 1 alínea c) do Código Penal).

Acórdão da Relação de Évora de 17 de março de 2015

- Tendo os filmes de carácter pornográfico sido objeto de perícia, a sua exibição/visualização em audiência torna-se tarefa sem utilidade detetável. A concreta identificação de vítimas não constitui elemento do tipo de pornografia de menores, previsto no artigo 176º, nº 1, als. c) e d) do Código Penal.

Acórdão da Relação do Porto de 3 de dezembro de 2014
- Fazer *download* de dados de pornografia de menores, de um servidor para o seu dispositivo informático pessoal, relativos a ficheiros de imagens, integra o conceito de importar previsto na alínea c) do nº1 do Artigo 176º do Código Penal.

Acórdão da Relação de Coimbra de 2 de abril de 2014
- Preenche o crime de pornografia de menores o arguido que guarda no seu computador imagens de crianças do sexo masculino, nuas e em poses de exibição dos órgãos sexuais.

9. Não cumprimento de obrigações relativas a proteção de dados

Os processos em que investigam ou julgam crimes desta natureza não são muito abundantes. Não obstante, as decisões de tribunais superiores sobre a temática são ricas e abordam temas essenciais das mesmas (por exemplo, a sobreposição dos crimes da Lei nº 67/98 com o crime de devassa informática - Artigo 193º do Código Penal –, ou ainda a relação entre os diversos crimes da Lei de Proteção de Dados Pessoais).

Acórdão da Relação do Porto de 22 de abril de 2015
- Preenche objetivamente o tipo de crime de não cumprimento de obrigações relativas à proteção de dados pessoais (Artigo 43º, nº 1, c), da Lei nº 67/98) a conduta de quem utiliza dados pessoais recolhidos pela empresa para quem trabalhou como cabeleireira, para promover o seu próprio negócio, também como cabeleireira.

Acórdão da Relação de Évora de 5 de novembro de 2013
- O Artigo 193º do Código Penal (devassa por meio da informática) foi revogado e substituído pelos crimes da Lei de Proteção de Dados Pessoais. Entre o crime de não cumprimento de obrigações relativas a proteção de dados (Artigo 43º da LPDP) e o crime de violação do dever de sigilo (do seu Artigo 47º) verifica-se uma situação de concurso efetivo. O número de crimes cometidos não se afere pelo número de pessoas constantes do ficheiro de dados pessoais, o qual é irrelevante.

10. Ilícitos em redes sociais

A fácil utilização das redes sociais (entre as outras realidades da chamada web.2) para divulgar conteúdos tem dado origem a discussão sobre a legitimidade/licitude da divulgação de alguns desses conteúdos. As decisões referenciadas focam, em geral, a divulgação de dados ou informação em violação da honra de outrem, da privacidade ou do direito à imagem de terceiros.
Destaca-se um recente acórdão que aborda a divulgação de dados de crianças em redes sociais.

Acórdão da Relação de Évora de 25 de junho de 2015
- Em decisão de regulação de responsabilidades parentais, a imposição aos pais do dever de «abster-se de divulgar fotografias ou informações que permitam identificar a filha nas redes sociais» mostra-se adequada e proporcional à salvaguarda do direito à reserva da intimidade da vida privada e da proteção dos dados pessoais e, sobretudo, da segurança da menor no Ciberespaço.

Acórdão da Relação do Porto de 5 de junho de 2015
- O direito à imagem constitui um bem jurídico-penal tutelado em si e independentemente do ponto de vista da privacidade ou intimidade retratada. Abrange dois direitos autónomos: o direito a não ser fotografado e o direito a não ver divulgada a fotografia. O visado pode autorizar ou consentir que lhe seja tirada uma fotografia e pode não autorizar que essa fotografia seja usada ou divulgada. Contra vontade do visado não pode ser fotografado nem ser usada uma sua fotografia. Quem, contra a

vontade do fotografado, utiliza uma fotografia deste, ainda que licitamente obtida e a publicita no Facebook, comete o tipo legal de crime de gravações e fotografias ilícitas (Artigo 199º nº 2 do Código Penal).

Acórdão da Relação de Guimarães de 18 de março de 2013
- A criação, numa rede social, de um perfil em nome de outra pessoa, com inclusão de características de utilizador ofensivas da honra e consideração do "titular" do perfil, constituem crime de difamação.

Acórdão da Relação de Évora de 14 de fevereiro de 2012
- Estando em causa a prática de crimes contra a honra por meio de comentários publicados num *blog*, o domínio do facto assiste a duas pessoas, cuja intervenção é imprescindível ao cometimento do crime: aquela que inscreve o comentário e aquela que disponibiliza o *blog* para o efeito e consente na respetiva publicação. O administrador do *blog* gere e seleciona os comentários feitos no mesmo, pelo que tem o pleno domínio do facto. O importante não é quem causa o facto, mas quem domina a execução deste.

11. Fotografias Ilícitas

O surgimento de significativos casos de crimes de fotografias ilícitas (incluído filmagens em vídeo), previsto no número 2 do Artigo 199º do Código Penal, pode estar associado à expansão das maquinas fotográficas digitais e, sobretudo, à popularização de telefones que incorporam câmaras. A discussão deste fenómeno na jurisprudência coincidiu com o surgimento de um número expressivo de decisões sobre a admissão deste tipo de imagens como prova, em processo penal. A fronteira entre as duas questões jurídicas nem sempre está clara traçada, já que as duas discussões estão muito relacionadas, como que sendo as duas diferentes faces de uma mesma moeda.

Acórdão da Relação de Évora de 26 de abril de 2016
- Comete o crime de gravações e fotografias ilícitas (Artigo 199º, nº 2 do Código Penal), quem monta e mantém em funcionamento um sistema de videovigilância que procede à gravação sistemática de imagens, nelas se incluindo as do acesso a uma habitação de terceiros que são inevitavelmente filmados sempre que entram ou saem de casa.

Acórdão do Tribunal da Relação do Porto de 14 de outubro de 2015
- É legítimo proceder a uma busca domiciliária com vista à apreensão de fotografias ou filmes que se suspeita estarem nesse domicílio, em computador, telemóvel, câmara ou noutro suporte digital, se houver indícios da prática de um crime de gravações e fotografias ilícitas (Artigo 199º, nº 2, a) do Código Penal).

12. Jogo *online*

A decisão que se inclui em baixo relaciona-se estritamente com a regulamentação do jogo, abordando uma variante muito específica da mesma.

Acórdão do Tribunal da Relação de Guimarães de 2 de novembro de 2015
- Não deve ser considerado como "explorador" de jogos (para efeitos do Artigo 108º, nº 1 do Decreto-Lei nº 422/89), aquele que permite que terceiros acedam à Internet, para jogarem *online* jogos de fortuna e azar, mesmo que cobre dinheiro por esse acesso dos jogadores à Internet.

13. Questões processuais substantivas

O incremento dos crimes *online* trouxe com ele a discussão de questões processuais de implicação substantiva. Para já, foram questionados na jurisprudência dois aspetos: por um lado, a do momento de conhecimento, pela vítima, do crime que a atingiu. A questão é relevante, porque muitos dos crimes *online* são de natureza semipública, dependendo portanto a prossecução criminal de apresentação de queixa, em devido tempo. Por outro, foi discutida na jurisprudência a relevância do local da prática física de factos com consequências à distância. Este aspeto também é relevante, não só por razões de natureza processual, por exemplo de competência do tribunal, mas também pela respetiva implicância substantiva.

Acórdão do Tribunal da Relação de Lisboa de 17 de dezembro de 2015

- O direito de queixa extingue-se no prazo de 6 meses a contar da data em que o ofendido teve efetiva noção de que poderá estar a ser vítima de um crime. Em caso de burla por meio de vendas *online*, só decorrido algum tempo sobre a compra o comprador percebe que caiu num engano ardilosamente montado e que nunca nada irá receber em troca do que pagou.

Acórdão do Tribunal da Relação do Porto de 17 de fevereiro de 2016

- Quando estão em causa factos relacionados com envio de SMS e conversações telefónicas (crimes por via de telemóveis), não é relevante o local onde se encontra o ofendido. Se não for indicado o local onde a ofendida se encontrava quando recebeu cada uma das SMS e cada um dos telefonemas, esse não é fundamento, por desproporcional e excessivo, de rejeição da acusação deduzida.

(O Gabinete Cibercrime fica grato pela indicação, para cibercrime@pgr.pt de outras decisões sobre cibercrime que não tenham sido elencadas)

ANEXO 50

Nota Prática 10

NOTA PRÁTICA nº 10/2016
21 de setembro de 2016

Jurisprudência sobre prova digital

Pretende-se com esta nota prática referenciar a jurisprudência de tribunais superiores sobre prova digital, publicada e disponível na Internet. Todos os acórdãos estão também referenciados no SIMP temático Cibercrime.

Compilaram-se decisões que abrangem a chamada *prova digital* num sentido bastante alargado, cobrindo matérias porventura de franja.
Não é propósito desta nota fazer a análise dos acórdãos, os quais se referem apenas com um curto sumário, deixando-se ainda muito brevíssimos comentários genéricos, de enquadramento, que somente pretendem dar pistas sobre a extensão e o sentido da jurisprudência.

O período temporal coberto termina na presente data e recua até 2009, ano da publicação da Lei do cibercrime, embora se incluam algumas decisões anteriores, por se manterem pertinentes.

1. Interceções telefónicas e de comunicações

A temática das interceções telefónicas tem dado origem a inúmeras decisões de tribunais superiores. Porém, aqui apenas se referenciam decisões que, de alguma forma, possam ser úteis para a compreensão do fenómeno digital, deixando-se por referenciar incontáveis acórdãos, sobre escutas telefónicas, disponibilizados no passado recente.

Acórdão da Relação do Porto de 1 de junho de 2016
- As escutas telefónicas são um meio de obtenção de prova, mas as conversações recolhidas através dessas interceções constituem meio de prova. Depois de transcritas e inseridas no processo, passam a constituir prova documental submetida ao princípio da livre apreciação da prova

Acórdão da Relação de Évora de 12 de abril de 2016
- Não é razoável a interpretação do nº4 do Artigo188º do CPP, segundo a qual o prazo de 48 horas para apresentação ao JIC dos elementos referentes às interceções telefónicas se destina ao magistrado e aos dos serviços do Ministério Público: o prazo é fixado ao agente do Ministério Público e não à simbiose do agente com os respetivos serviços

Acórdão da Relação do Porto de 13 de maio de 2015
- Só podem valer como prova em julgamento as comunicações que o Ministério Público mandar transcrever ao OPC e indicar como meio de prova na acusação. A inobservância das regras do Artigo 188º, do CPP constitui nulidade que impede toda e qualquer utilização do material probatório assim obtido - esta invalidade atinge apenas essas concretas comunicações.

Acórdão da Relação de Évora de 5 de maio de 2015
- A lei não impõe a pré-existência, relativamente às escutas telefónicas, de outras diligências probatórias (inconclusivas) que as abonem ou justifiquem.

Acórdão da Relação de Évora de 17 de março de 2015
- É possível lançar-se mão das escutas telefónicas logo como o primeiro meio de obtenção da prova utilizado, quando - e apenas nesta hipótese - o juiz de instrução se convença, em face dos concretos dados factuais trazidos pelo Ministério Público, que ela é a única diligência capaz de fazer carrear para os autos os elementos probatórios aptos à descoberta da verdade.

Acórdão da Relação de Coimbra de 4 de fevereiro de 2015
- Em inquérito, o pedido ao operador de comunicações do registo de todas as comunicações recebidas (por exemplo SMS, e MMS), num período temporal alargado, na medida em que permitem identificar os utilizadores, o relacionamento direto entre uns e outros através da rede, a localização, a frequência, a data, hora, e a duração das comunicações, deve participar das garantias a que está submetida a utilização do serviço, especialmente tudo quanto respeite ao sigilo das comunicações. Torna-se necessária a autorização do Juiz para a sua obtenção e junção aos autos.

Acórdãos da Relação de Évora de 6 de janeiro de 2015 e de 20 de janeiro de 2015
- O regime processual das comunicações telefónicas previsto nos artigos 187º a 190º do Código de Processo Penal deixou de ser aplicável por extensão às "telecomunicações eletrónicas", "crimes informáticos" e "recolha de prova eletrónica (informática)" desde a entrada em vigor da Lei do Cibercrime. Para a prova eletrónica preservada ou conservada em sistemas informáticos existe um novo sistema processual penal, o previsto nos artigos 11º a 19º da Lei do Cibercrime.

Acórdão da Relação de Évora de 6 de janeiro de 2015
- O regime processual da Lei 32/2008 (designadamente o Artigo 3º, nº 1 e 2 e o Artigo 9º) está revogado e substituído pelo regime processual contido na Lei nº 109/2009 para todos os dados que não estejam especificamente previstos no Artigo 4º, nº 1 daquela lei, ou seja, dados conservados em geral; está em vigor para todos os dados que estejam especificamente previstos naquele Artigo 4º, nº 1 (por exemplo para dados conservados relativos à localização celular).

2. Mensagens de SMS e de correio eletrónico

As mensagens curtas de texto (SMS) têm sido cada vez mais utilizadas como prova. Firmou-se jurisprudência quanto à desnecessidade de intervenção judicial na obtenção e junção ao processo dessas mensagens, se o seu destinatário (normalmente o lesado) der autorização para essa junção – por exemplo quando é ele mesmo quem faculta o telefone para a obtenção das mensagens. Já assim não será se as mensagens estão armazenadas em aparelho de quem não autoriza a obtenção das mensagens: neste caso exige-se intervenção judicial, nos termos do Artigo 17º da Lei do Cibercrime.
Contra esta orientação apenas se encontrou uma decisão (embora sobre correio eletrónico), já mais antiga, de 2011. Não está publicada, desde então, nenhuma outra decisão no sentido deste acórdão, cuja orientação tem vindo a ficar mais isolada.
O regime de apreensão de SMS tem o mesmo enquadramento legal (Artigo 17º da Lei do Cibercrime) do regime da apreensão de mensagens de correio eletrónico ou de comunicações de idêntica natureza. A jurisprudência quanto às primeiras é, pois, aplicável a estas últimas.

Acórdão do Tribunal da Relação do Porto de 20 de janeiro de 2016

- Se o arguido enviou ao ofendido mensagem por SMS, o seu destinatário pode fazer da missiva o uso que entender, nomeadamente apresentá-la às autoridades judiciárias para poder servir como prova de um crime de que é vitima. A mensagem mantida em suporte digital, depois de recebida e lida, tem a mesma proteção da carta em papel que, tendo sido recebida pelo correio e aberta, foi guardada em arquivo pessoal. Sendo um mero documento escrito, aquela mensagem não goza da aplicação do regime de proteção específico da reserva da correspondência e das comunicações previsto no Artigo 189º do CPP. A junção aos autos de transcrição de mensagem escrita guardada em telemóvel não tem de ser autorizada pelo juiz.

Acórdão da Relação de Lisboa de 24 de setembro de 2013

- As mensagens de SMS deixam de ter a essência de uma comunicação em transmissão para passarem a ser uma comunicação já recebida, que terá porventura a mesma essência da correspondência», em nada se distinguindo de uma «carta remetida por correio físico»; o destinatário da correspondência tem sobre a mesma toda a disponibilidade, designadamente para divulgar o seu conteúdo ou autorizar que deste tomassem conhecimento as autoridades policiais.

Acórdão da Relação do Porto de 3 de abril de 2013

- As mensagens de SMS recebidas no telemóvel da ofendida e por ela disponibilizadas de forma espontânea são um meio de prova válido, que não requere qualquer validação judicial, por ter sido fornecido por quem é o seu legítimo detentor.

Acórdão da Relação de Guimarães de 15 de outubro de 2012

- A transcrição de mensagens SMS do telemóvel de um queixoso que espontaneamente as fornece, pode valer como prova, apesar de não ter sido ordenada pelo juiz. Só será necessária a intervenção do JIC quando quem fornece aquelas mensagens não puder dispor delas.

Acórdão da Relação do Porto de 12 de setembro de 2012

- A jurisprudência tem equiparado as mensagens SMS às cartas de correio, distinguindo se ainda estão fechadas ou se foram já abertas pelo destinatário. Porém, a Lei do Cibercrime alterou esta abordagem: a leitura de mensagens guardadas num cartão de telemóvel por um agente policial sem autorização do seu dono ou do JIC é prova proibida, em nada relevando que as mesmas tivessem sido ou não abertas e lidas pelo destinatário pois que a lei não distingue entre essas duas situações.

Acórdão da Relação de Lisboa de 29 de março de 2012

- A junção ao processo da transcrição das mensagens SMS gravadas no telemóvel do queixoso, depois do consentimento deste, não está dependente de autorização do JIC.

Acórdão da Relação de Guimarães de 29 de março de 2011

- A apreensão de mensagens de telemóvel (SMS), mesmo que resultante de uma pesquisa de dados informáticos validamente ordenada pelo Ministério Público, deve depois ser autorizada pelo JIC. Embora o MP deva tomar conhecimento em primeira das mensagens, ordenando a apreensão provisória, deve depois ser o juiz a ordenar a apreensão definitiva - Artigo 17º da Lei do Cibercrime. A lei não estabelece distinção entre mensagens por abrir e abertas.

Acórdão da Relação de Lisboa de 11 de janeiro de 2011

- Quanto à apreensão de mensagens de correio eletrónico ou registos de comunicações de natureza semelhante, a Lei do Cibercrime, ao remeter para o regime geral previsto no Código de Processo Penal, determina a aplicação deste regime na sua totalidade, sem redução do seu âmbito - tais

apreensões têm de ser autorizadas ou determinadas por despacho judicial, devendo ser o juiz a primeira pessoa a tomar conhecimento do conteúdo da correspondência apreendida, sob pena de nulidade.

3. Acesso ao conteúdo de telemóveis

O acórdão referenciado é pioneiro na análise da questão da obtenção de conteúdos gravados em telemóvel, não se incluindo neste conteúdo as mensagens de comunicações. Quanto a todo o restante conteúdo – incluída a lista telefónica ou o registo de chamadas efetuadas e recebidas (e presumivelmente também fotografias ou vídeos do dono do telefone), o acórdão estipula que, tendo este conteúdo a natureza de documentos, a sua apreensão não depende de ordem judicial.

Acórdão da Relação de Évora de 7 de abril de 2015

- O exame pericial a um telemóvel e seu cartão SIM, para identificação da respetiva lista telefónica, dos registos das chamadas recebidas e atendidas, das recebidas e não atendidas e, das chamadas efetuadas, não carece da prévia autorização do Juiz de Instrução. Embora as comunicações por telemóvel tenham uma dinâmica entre a realização da chamada e o termo da mesma que perdura durante determinado lapso de tempo, ultrapassado este, deixa de haver comunicação telefónica - nos termos da lei penal, nomeadamente do Artigo 187º, do Código de Processo Penal - e o registo que delas fica passa a constituir um mero documento demonstrativo dessas mesmas comunicações telefónicas.

4. Conversas telefónicas em *alta voz*

A (não) admissibilidade de testemunho sobre conversas telefónicas que se escutaram no telefone de outrem, em alta voz*, provocou forte discussão jurisprudencial no passado. A orientação da jurisprudência mais recente é serena no sentido da admissibilidade deste tipo de prova, nalgumas circunstâncias.*

Acórdão da Relação de Évora de 25 de novembro de 2014

- A prova por depoimento de testemunha que escutou conversação telefónica por intermédio de sistema alta voz, em geral, não é prova livre, podendo cair nas proibições de prova. Porém, a mesma pode ser admissível, desde que se mostre imprescindível, atentas as circunstâncias do caso concreto, designadamente, ocorrer causa de justificação, consistente numa legítima defesa - obter testemunho do crime praticado pelo arguido para o enfrentar e obstar a que prossiga na agressão - ou num direito de necessidade (probatório) - agir para obter prova para o perseguir criminalmente.

Acórdão da Relação de Coimbra de 10 de julho de 2013

- Quando a vítima é a destinatária da comunicação telefónica (ou outra), considera-se justificada a divulgação do teor da conversa pelo sistema de alta voz, quando essa comunicação é o meio utilizado para cometer um crime de ameaças, ou injúrias, se a vítima consentir na divulgação; como tal não constitui prova proibida.

Acórdão da Relação de Coimbra de 6 de março de 2013

- A divulgação, pelo sistema de alta voz, de uma conversa telefónica, quando essa precisa comunicação telefónica é o meio utilizado para cometer um crime de ameaças ou injúrias é lícita, sendo permitido a quem a escutou testemunhar sobre ela, se a vítima consentir na divulgação, como forma de se proteger de tais ameaças ou injúrias.

5. Endereço de IP

Na nota prática nº 2/2013 (de 3 de abril de 2013) concluía-se que a jurisprudência dominante sustentava que o pedido de identificação do utilizador de um determinado endereço IP, num dado dia e hora, não devia ser submetido ao regime dos dados de tráfego, por se entender que este pedido não se refere a informação sobre o percurso dessa comunicação nem sobre outro eventual tráfego comunicacional da pessoa em causa. Por isso, concluía-se que pertencia ao Ministério Público a competência para pedir, a um operador de comunicações, a identificação do seu cliente que utilizou um determinado endereço IP num determinado dia e hora.

Todos os acórdãos agora referenciados, posteriores à emissão daquela nota prática confirmam esta orientação.

Acórdão da Relação do Porto de 17 de setembro de 2014

- No serviço de telecomunicações a obtenção dos dados de base (isto é, dos dados de conexão à rede, tais como a identidade do titular do telefone o seu número e a sua morada, ainda que cobertos pelo sistema de confidencialidade a solicitação do assinante) não contendem com a privacidade do seu titular pelo que devem ser comunicados a pedido de qualquer autoridade judiciária.

Acórdão da Relação de Lisboa de 19 de junho de 2014

- Estando em causa a obtenção da identificação de um utilizador de um endereço IP ou o número de IP usado por um determinado indivíduo, em circunstâncias temporais determinadas, a competência para a respetiva obtenção é do MP. A identificação de um determinado endereço de IP conjugada com a identidade de quem o utilizou num dado dia e hora não revela informação sobre o percurso da comunicação nem sobre outro eventual tráfego comunicacional da pessoa em causa.

Acórdão da Relação de Évora de 22 de abril de 2014

- A identificação completa, morada e endereço de correio eletrónico do titular de determinado *blog*, Facebook ou outra rede social, bem como o IP de criação dessa rede social e o IP onde foi efetuado determinado *post* constituem dados de base, que embora cobertos pelo sistema de confidencialidade, podem ser comunicados a pedido de uma autoridade judiciária.

Acórdão da Relação de Lisboa de 22 de janeiro de 2013

- A obtenção de um concreto endereço IP que esteve na origem da uma determinada comunicação efetuada é da competência do Ministério Público - e não do juiz.

Acórdão da Relação de Évora de 22 de dezembro de 2012

- Obtenção de endereço IP - legitimidade do MP - embora o objeto da decisão seja outro, este aresto cita despacho de JIC sobre a temática em epígrafe.

Acórdão da Relação de Évora de 7 de dezembro de 2012

- Quando o MP pretende apenas aceder ao IP de origem de uma comunicação não está a querer aceder a dados de tráfego (quer saber apenas a identificação e a morada do utilizador do serviço - isto é, quer saber dados de base).

Acórdão da Relação de Évora de 13 de novembro de 2012

- A identificação completa, morada e endereço de correio eletrónico do titular de determinado blogue, bem como o IP de criação desse blogue e o IP de onde foi efetuado determinado *post*, constituem dados de base - os elementos ou dados funcionais (de tráfego), necessários ou produzidos pelo estabelecimento da ligação (...) são a direção, o destino (*adressage*) e a via, o trajeto (*routage*).

Acórdão da Relação de Coimbra de 3 de outubro de 2012
- O endereço IP é um dado de tráfego, sendo a sua obtenção dependente de autorização do JIC - no despacho recorrido, de JIC, a posição assumida no despacho recorrido era a oposta.

Acórdão da Relação de Évora de 12 de julho de 2012
- A identidade de um cidadão que se liga a determinado blogue ou sítio da Internet não está coberta pelo segredo das conversações ou comunicações regulado pelos Artigos 187º a 190º do CPP. O mesmo sucede com os dados de conexão à rede, elementos necessários ao estabelecimento de uma base para comunicação, aquém da comunicação; são prévios em relação a ela e constituem, na perspetiva dos utilizadores, os elementos necessários ao acesso à rede, designadamente através da ligação individual e para utilização própria do respetivo serviço. A eventual confidencialidade desses dados (por exemplo, por força dos termos do contrato de fornecimento do serviço) traduz um simples interesse pessoal do utilizador, que de modo algum contende com a sua esfera pessoal íntima, podendo ser comunicados a pedido de qualquer autoridade judiciária para fins de investigação criminal.

Acórdão da Relação de Évora de 5 de junho de 2012
- Quando o Ministério Público pretende obter "todos os dados do utilizador de IP" num determinado período de tempo, está-se perante dados de tráfego, dependendo a sua obtenção de autorização judicial e só sendo possível quando a um limitado catálogo de crimes. Estando em causa investigação por crime de difamação através da internet, não é admissível o acesso a dados de tráfego, por via de autorização judicial, dado que tal ilícito não consta, nem do catálogo previsto no Artigo 187º do CPP, nem da definição de crime grave do Artigo 2º da Lei nº 32/2008.

Acórdão da Relação e Évora de 27 de janeiro de 2011
- A mera identificação de um titular de um número fixo ou móvel não pertence ao sigilo das comunicações. Quanto a endereços IP fixos, o acesso à identificação do seu utilizador faz-se sem recurso a dados de tráfego, mas quanto a endereços dinâmicos supõe, simultaneamente, aceder a dados de tráfego e depende de autorização judicial.

Acórdão da Relação de Lisboa de 18 de janeiro de 2011
- A identificação completa, morada e endereço de correio eletrónico do titular de determinado *blog,* bem como o IP de criação desse blog e o IP onde foi efetuado determinado *post*, constituem dados de base.

6. Localização celular

A jurisprudência sobre localização celular incide, na sua maioria, sobre a possibilidade legal, ou não, de se proceder à identificação indiscriminada de todas as comunicações efetuadas por via de uma determinada antena repetidora de sinal de telemóvel, num certo período de tempo, na esperança de se encontrarem eventuais registos de comunicações de autores de crimes. Sem exceção, a jurisprudência pronuncia-se no sentido da inadmissibilidade legal desta medida.

Acórdão da Relação de Lisboa de 22 de junho de 2016
- Solicitar a operadoras de telemóveis todos os dados de tráfego dos cartões SIM que operaram num determinado período de tempo em 19 antenas, mas não estando concretizados alvos determináveis, e atingindo a diligência pretendida um universo ilimitado e indiferenciado de cidadãos que não se integram no conceito jurídico-penal de “suspeitos” é proibido por lei e não respeita os princípios constitucionais da proporcionalidade e da adequação.

Acórdão da Relação de Lisboa de 3 de maio de 2016

- Não é permitido, em inquérito, solicitar às operadoras de comunicações que forneçam todos os números de telefone que num determinado período de tempo, se conectaram a uma determinada antena, sem que, previamente, se determinem previamente os suspeitos o que, em caso de desconhecimento da respetiva identificação, pressupõe a existência de dados factuais tendentes à sua individualização, não sendo admissível que sejam consideradas suspeitas de determinada ação criminosa, todas as pessoas que se encontrassem naquele local e tempo.

Acórdão da Relação de Évora de 19 de maio de 2015

- A falta de suspeito determinado contra quem dirigir as escutas telefónicas, os pedidos de obtenção de dados de tráfego ou os pedidos de localização celular, é obstáculo intransponível à realização deste tipo de meios de obtenção de prova. Recolher informações de pessoas inocentes, na esperança de, de entre estas, se "apanhar" algum suspeito, é desproporcional aos fins visados, sendo, pois, uma compressão inconstitucional e ilícita do direito à privacidade e à inviolabilidade das comunicações.

Acórdão da Relação do Porto de 11 de fevereiro de 2015

- Não é admissível solicitar-se a um operador de comunicações que forneça os dados de localização celular relativos a um número indeterminado de pessoas, uma vez que a obtenção indiscriminada de dados de localização celular afronta o direito à inviolabilidade das telecomunicações.

Acórdão da Relação de Évora de 25 de maio de 2013

- A localização celular não pode ser usada já depois de se ter consumado uma situação de perigo; supõe a séria possibilidade da existência dessa situação de perigo para a vida e a integridade física grave de alguém e supõe que a localização celular possa obviar à concretização desse perigo. Não pode ser autorizada quando está apenas em causa a investigação de perigo que já se consumou.

Acórdão da Relação de Évora de 18 de outubro de 2011

- A obtenção de dados de localização celular de uma determinada área geográfica, sem que haja um suspeito concreto, além de ferir os ditames legais, é desprovida de razoabilidade, desproporcionada e inadequada, não sendo justificada face à devassa intolerável que constituiria.

Acórdão da Relação de Évora de 23 de setembro de 2010

- Não é permitida a obtenção de dados sobre a localização celular ou de registos da realização de comunicações, genericamente relativos a uma determinada área geográfica e a determinado intervalo temporal, porque essa diligência vai necessariamente abranger um leque muito alargado de cidadãos e não visa um suspeito determinado, como exige a lei.

7. Imagens de fotografias e imagens de videovigilância como prova

A consideração, como prova válida, de imagens gravadas por indivíduos (privados), não está expressamente regulada na lei processual penal. Porém, já há alguma jurisprudência a esse propósito, em geral permitindo essa mesma utilização, desde que, na sua origem, não esteja um propósito ilícito. No caso de gravações ocasionais feitas por cidadãos, esta ilicitude tem sido aferida, caso a caso, segundo as suas peculiares circunstâncias. Quanto à gravação por via de sistemas de vigilância, esta licitude (e, portanto, a validade da prova delas resultante), não é beliscada por eventual falta formal ou burocrática, por exemplo, de não submissão prévia de pedido anterior à CNPD. Referenciam-se alguns acórdãos da jurisdição laboral que versam sobre a licitude, ou não, de empregadores usarem meios de vigilância eletrónica sobre os seus trabalhadores.

Acórdão da Relação de Coimbra de 18 de maio de 2016

- São lícitas as imagens obtidas através de câmaras de vigilância, em espaços destinados à vida estritamente privada, como o interior de habitações, pelos legítimos utilizadores de tais espaços, visando a defesa dos seus bens pessoais e patrimoniais. Sendo obtidas imagens da prática de crimes por estranhos ao espaço em causa e que nele se introduziram ilegitimamente, é indiferente que não tenha havido autorização do visado ou aprovação da CNPD, uma vez que, por natureza, no caso, as imagens não podem dizer respeito ao núcleo duro da vida privada e mais sensível daquele visado.

Acórdão da Relação de Lisboa de 10 de maio de 2016

- Imagens captadas em local de acesso público, mesmo na falta de consentimento do visado, não correspondem a qualquer método proibido de prova, por não violarem o núcleo duro da vida privada, avaliado numa ideia de proporcionalidade e por existir uma justa causa na sua obtenção e utilização, que é a prova de uma infração criminal. A falta de parecer prévio favorável da CNPD, só por si, não torna a gravação ilícita, nos termos da lei penal.

Acórdão da Relação de Évora de 29 de março de 2016

- É, em princípio, admissível a valoração das fotografias ou filmes que não tenham sido obtidos de forma penalmente ilícita. Filmar a materialidade de autoria de um crime e de utilizar posteriormente o vídeo como prova do facto, embora possa eventualmente preencher a factualidade típica do crime de gravações e fotografias ilícitas (Artigo 199º do Código Penal), pode ser lícito, por exemplo, se quem filmou agiu ao abrigo do direito de necessidade (Artigo 34º do Código Penal), o que vale tanto para a obtenção do vídeo como para a sua posterior utilização em processo crime, pois esta utilização constitui a concretização daquele mesmo fim.

Acórdão da Relação de Évora de 29 de março de 2016

- É prova válida a gravação de filme, com telemóvel, de situação de conflito na qual vem a ocorrer um crime. Já será prova proibida a que resulta de fotografias tiradas já depois de o crime ter ocorrido, ao autor deste, para demonstrar a respetiva presença no local.

Acórdão do Tribunal da Relação de Coimbra de 24 de fevereiro de 2016

- A captação de imagens por particulares, em locais públicos ou de livre acesso ao público, não estando ferida de qualquer ilegalidade nem violando os direitos de personalidade que compreendem o direito à imagem, é meio admissível de prova. As imagens assim captadas não constituem nenhuma violação do "núcleo duro da vida privada" nem do direito à imagem. Por conseguinte, não é necessário o consentimento do visado para essa filmagem, nos termos exigidos pelo Artigo 79º, nº 2, do Código Civil, porquanto a imagem do suspeito se encontra justificada por razões de justiça, nem tão pouco a referida recolha de imagens integra o crime do Artigo 199º, nº 2, do Código Penal. Os depoimentos que reproduzem as ditas filmagens, não estando afetados por qualquer proibição de prova, devem ser livremente apreciados e valorados pelo tribunal.

Acórdão da Relação do Porto de 25 de fevereiro de 2015

- A obtenção de fotografias ou de filmagens sem o consentimento do visado, sempre que exista justa causa nesse procedimento, nomeadamente quando as mesmas estejam enquadradas em lugares públicos, visem a realização de interesses públicos ou hajam ocorrido publicamente não constitui ilícito típico. Nessas circunstâncias mesmo que haja falta de licenciamento da CNPD podem ser usadas como meio de prova.

Acórdão da Relação de Coimbra de 6 de fevereiro de 2015

- Apesar de o Artigo 20º, nº 1 do Código do Trabalho proibir a utilização de meios de vigilância à distância para controlar de forma dedicada e permanente o desempenho profissional do trabalhador, esta utilização é lícita se cumprir os requisitos de fim e publicidade previstos nos nºs 2 e 3 do mesmo artigo e for obtida a autorização da Comissão Nacional de Proteção de Dados. Neste último caso, os dados obtidos podem servir de meio de prova em procedimento disciplinar e no controlo jurisdicional da licitude da decisão disciplinar.

Acórdão da Relação do Porto de 17 de dezembro de 2014

- Não é admissível como meio de prova, em processo laboral, a captação de imagens por sistema de videovigilância; a consequência legal dessa utilização ilícita dos meios de vigilância à distância é a invalidade da prova obtida para efeitos disciplinares.

Acórdão do Tribunal de Justiça da União Europeia de 11 de dezembro de 2014

- A gravação, por um sistema de videovigilância, de imagens de pessoas, por uma pessoa singular, na sua casa familiar, para proteger os seus bens, a saúde e a vida dos proprietários dessa casa e que vigia igualmente o espaço público, não constitui um tratamento de dados efetuado no exercício de atividades exclusivamente pessoais ou domésticas, na aceção do Artigo 3°, n° 2, da Diretiva 95/46/CE.

Acórdão da Relação de Guimarães de 29 de abril de 2014

- Não constituem provas ilegais, podendo ser valoradas pelo tribunal, as imagens gravadas por particulares em locais públicos ou acessíveis ao público, se se destinarem a documentar uma infração criminal e não disserem respeito ao «núcleo duro da vida privada» da pessoa visionada.

Acórdão da Relação do Porto de 23 de outubro de 2013

- São válidas, não constituindo métodos proibidos de prova e podendo ser valoradas pelo julgador, as imagens gravadas por particular, sendo a gravação direcionada para um local público, particularmente dirigida para o seu veículo automóvel, estacionado na via pública, apenas com vista a apurar quem era o autor dos danos, por neste caso existir justa causa para essa captação de imagens (por não serem atingidos dados sensíveis da pessoa visionada). A imagem captada nas circunstâncias deste caso concreto, por um lado não constitui nenhuma violação do "núcleo duro da vida privada", nem do direito à imagem do visionado.

Acórdão da Relação de Évora de 28 de junho de 2011

- A obtenção das imagens através de sistema, tendo em vista a identificação de autores de crimes, visa documentar infrações e não diz respeito ao «núcleo duro da vida privada» da pessoa visionada; é um meio necessário e apto ao exercício do direito de defesa, pelo que está excluída a ilicitude do mesmo. Não constitui um método proibido de prova, dado que existe uma causa de justificação para a sua obtenção.

Acórdão da Relação de Lisboa de 14 de maio de 2009

- Apesar de o Artigo 199º, nº4, do Código Penal proibir e punir a recolha de imagens, por fotografia ou por filmagem, este direito apenas é reconhecido a quem pode legitimamente ostentá-lo e defendê-lo; não é esse o caso de quem entra num espaço vedado e não livremente acessível ao público e dali retira e faz seus bens que sabe não lhe pertencerem - neste caso, são lícitas e válidas como prova as imagens obtidas por câmara de videovigilância oculta.

8. Localizador de GPS

Tal como acontece com outras tecnologias, a informação providenciada por aparelhos de GPS também tem sido indicada em sede probatória, apesar de não existirem normas que refiram expressamente esta nova tecnologia como prova. Mais que a sua utilização – ou não – têm sido discutidas as condições legais em que essa utilização é permitida. Tal como acontece com o uso de imagens, também a este propósito é relevante considerar jurisprudência da jurisdição laboral, sobre o recurso a meios de vigilância eletrónica sobre trabalhadores.

Acórdão da Relação de Lisboa de 13 de abril de 2016

- O aparelho conhecido como *GPS tracker* permite saber, em tempo real, onde está o mesmo – por exemplo, onde está o veículo onde foi instalado, bem como o respetivo percurso, os tempos e locais de paragem, o período de funcionamento do motor e a velocidade a que o automóvel circula. Este meio de obtenção de prova é diferente da interceção de comunicações e não existe lei que o preveja, bem como aos seus limites e às garantias inerentes à sua aplicação. É um meio oculto de investigação que, por isso mesmo, só poderia ser admitido se existisse lei que o consagrasse como um meio de obtenção de prova legítimo e regulasse todos os aspetos do seu regime. Assim é, porque a utilização destes aparelhos, pelo sistemático e permanente registo de dados que propicia e pela natureza dos mesmos, é suscetível de violar a vida privada dos utilizadores dos veículos em que se encontrem instalados.

Acórdão do Supremo Tribunal de Justiça de 13 de novembro de 2013

- O dispositivo de GPS instalado, pelo empregador, em veículo automóvel utilizado pelo seu trabalhador no exercício das respetivas funções, não pode ser qualificado como meio de vigilância à distância no local de trabalho, porquanto apenas permite a localização do veículo em tempo real, não permitindo saber o que faz o respetivo condutor. Encontrando-se o GPS instalado numa viatura exclusivamente afeta às necessidades do serviço, não permitindo a captação ou registo de imagem ou som, o seu uso não ofende os direitos de personalidade do trabalhador, nomeadamente a reserva da intimidade da sua vida privada e familiar.

Acórdão da Relação do Porto de 21 de março de 2013

- A colocação de um localizador de GPS no veículo de um suspeito está sujeita a autorização judicial
- por aplicação analógica do Artigo 187° do CPP.

9. Uso de correio eletrónico para praticar atos processuais

A legislação processual penal desconhece o correio eletrónico como forma de praticar atos processuais, tendo como referência os documentos em papel. O mesmo não acontece com o processo civil, que vai muito mais adiantado neste tema. Por essa razão, a jurisprudência referenciada é maioritariamente da jurisdição civil; mesmo aquela que se reporta expressamente a processo penal, apela igualmente às normas processuais civis. Uma vez que se trata de matéria vizinha, incluiu-se ainda uma decisão quanto ao Citius.

Acórdão do Tribunal da Relação de Coimbra de 15 de setembro de 2015

- É obrigatória a apresentação a juízo dos atos processuais através do sistema Citius, para os profissionais forenses. Apenas o não será em caso de justo impedimento que, no entanto, tem que ser expressamente invocado.

Acórdão da Relação de Coimbra de 30 de junho de 2015
- Não é admitida a prova testemunhal para demonstração da prática de ato processual por transmissão eletrónica de dados, prova que só é admissível por documento eletrónico - ou através da representação escrita de que é suscetível – i.e., através de uma declaração de validação cronológica, que ateste a data da expedição ou receção do documento eletrónico correspondente. Não integra justo impedimento a avaria do computador do Sr. Advogado subscritor da peça processual, impeditiva da expedição ou remessa da peça processual por transmissão eletrónica de dados.

Acórdão do Supremo Tribunal de Justiça de 21 de janeiro de 2014
- Tendo o ato processual – apresentação de requerimento probatório – sido praticado antes do termo do prazo, mas junto tardiamente aos autos, devido a uma gralha no endereço eletrónico do tribunal, não é justificado o seu desentranhamento e desconsideração, com as gravíssimas consequências ao nível da prova e da decisão do mérito da causa.

Acórdão da Relação de Évora de 26 de novembro de 2013
- É permitida a remessa a juízo de peças processuais por via de correio eletrónico.

Acórdão da Relação de Évora de 19 de março de 2013
- O correio eletrónico pode ser usado para a prática de atos processuais, em processo penal.

10. Necessidade de exibição de provas em julgamento

Os acórdãos referenciados neste ponto, sem se referirem especificamente a prova digital, sublinham uma importante orientação sobre a produção de prova em julgamento (aliás comum na jurisprudência), quando essa prova não está, na sua origem, plasmada em papel. Essa orientação vai no sentido da desnecessidade de ver ou ouvir, em julgamento, elementos de prova não impressos se, de alguma forma, esses elementos de prova estão já documentados em papel no processo.

Acórdão da Relação do Porto de 8 de julho de 2015
- As escutas telefónicas, regularmente efetuadas durante o inquérito, uma vez transcritas em auto, passam a constituir prova documental, que o tribunal de julgamento pode valorar de acordo com as regras da experiência; essa prova documental não carece de ser lida em audiência e, no caso de o tribunal dela se socorrer, não é necessário que tal fique a constar da ata.

Acórdão da Relação de Évora de 17 de março de 2015
- Tendo os filmes de carácter pornográfico sido objeto de perícia, a sua exibição/visualização em audiência torna-se tarefa sem utilidade detetável. A concreta identificação de vítimas não constitui elemento do tipo de pornografia de menores, previsto no artigo 176º, nº 1, alíneas c) e d) do Código Penal.

(O Gabinete Cibercrime fica grato pela indicação, para cibercrime@pgr.pt de outras decisões sobre prova digital que não tenham sido elencadas)

ANEXO 51

Alerta Cibercrime de 5 de setembro de 2016

Alerta Cibercrime
05-09-2016

A Coordenação da Área de Sistema e Redes da PGR alertou para o facto de estar em curso uma campanha de ataques de "ransomware". Tais ataques consistem na expedição de mensagens de correio eletrónico para um grande número de vítimas, contendo um ficheiro anexo que, se for aberto, provoca no computador da vítima encriptação de dados, que ficam assim inacessíveis ao seu dono. Normalmente, o criminoso pede um "resgate" para libertar os dados – os quais em geral nunca mais se recuperam.

Neste caso, as mensagens recebidas indicavam, no assunto, "mortage documents" e o documento anexo tinha uma extensão zip.

Não devem abrir-se este tipo de anexos destas mensagens, que devem ser apagadas.

https://simp.pgr.pt/destaques/des_ficha.php?nid_destaque=5004

ANEXO 52

Alerta Cibercrime de 6 de setembro de 2016

Alerta Cibercrime
***Phishing* por via de telemóveis**
06-09-2016

A Rede de CSIRT alertou que está em curso uma campanha de difusão de *malware* por via de SMS, destinadas a smartphones. As vítimas recebem SMS supostamente provenientes do Banco BIC ou do Banco Santander Totta, solicitando que se aceda um link, para reativar a sua conta bancária, supostamente bloqueada.
Vários dos links encaminhados por estas mensagens (http://bit.ly2bptmXi, http://bit.ly/2bHtGBe ou http://bitly.com/2c01I22) foram referenciados como correspondendo a páginas de *phishing* que foram, entretanto, bloqueadas.

https://simp.pgr.pt/destaques/des_ficha.php?nid_destaque=5005

ANEXO 54

Relatório Eurojust 24 de novembro de 2016

RELATÓRIO

Reunião da *European Judicial Cybercrime Network*

EUROJUST, 24 de novembro de 2016

1.

Decorreu, no dia 24 de novembro de 2016, na EUROJUST, a primeira reunião da *European Judicial Cybercrime Network*, ou rede judicial europeia para matérias do cibercrime. A reunião foi presidida por Daniela Buruiana, membro nacional da Roménia na EUROJUST e Presidente da *Task Force on Cybercrime* da EUROJUST. Nela tomaram parte os pontos de contacto especificamente designados para esta rede por 26 dos Estados Membros da União Europeia. Participaram ainda na reunião, além de outros representantes nacionais na EUROJUST, Koen Hermans, Vice-Presidente da *Task Force on Cybercrime* e membro adjunto da Holanda e José Eduardo Guerra, membro adjunto de Portugal na EUROJUST e igualmente membro da *Task Force on Cybercrime*. Participaram ainda representantes da Suíça e da Noruega, bem como representantes da Comissão Europeia, do Conselho Europeu e da Europol.

O subscritor foi indicado pela Procuradoria-Geral da República como representante do Ministério Público nesta rede.

Junta-se a agenda da reunião como Anexo 1.

2.

A criação formal da *European Judicial Cybercrime Network* resultou das conclusões do Conselho da União Europeia de 9 de junho de 2016. De acordo com este ato, esta rede deve congregar representantes dos Ministérios Públicos (nalguns casos, representantes judiciais) dos Estados Membros da União Europeia, especializados em temas de cibercriminalidade. Tem como propósito geral facilitar o intercâmbio de informação sobre cibercriminalidade e prova digital, constituindo um fórum de partilha de boas práticas, novidades legislativas e jurisprudência. A rede deve constituir também um canal de diálogo disponível para a coordenação de investigações de em casos concretos.

Tendo em vista materializar estes objetivos, a *European Judicial Cybercrime Network* realizará duas reuniões por ano, publicará anualmente o boletim *Cybercrime Judicial Monitor* e manterá uma plataforma de acesso

reservado na Internet, com fins colaborativos. Em cada uma das suas reuniões serão abordados específicos temas de interesse na área da cibercriminalidade e da obtenção da prova digital.

3.

Como temas técnicos específicos desta reunião, foram escolhidos a encriptação e as investigações encobertas. Quanto à encriptação, instrumento técnico absolutamente necessário à manutenção de standards mínimos de cibersegurança, foi anotado ser, por outro lado, um grande obstáculo à investigação criminal. Na verdade, na atualidade, todas as atividades criminosas podem potencialmente utilizar meios de comunicação encriptados para comunicar – WhatsApp, Skype, Telegram são, entre muitos outros recursos, vastamente utilizados por quem pratica crimes. Quanto às investigações encobertas, foi afirmado serem uma ferramenta essencial nas investigações de criminalidade *online*, em particular quanto a crimes cometidos na *darkweb*.

4.

Foi feita uma apresentação a este respeito, pela Europol (EC3), em que se apontou para eventuais soluções técnicas para contornar os limites práticos à investigação colocados pela encriptação (obrigação de divulgação ferramentas de desencriptação, ou criação de *backdoors*, ou obrigação de *disclosure*, porventura sob cominação). Reconheceu, a apresentação, a enorme limitação destas possibilidades.

No decurso da discussão da temática, acabou por concluir-se pela necessidade de reconsiderar este tema numa perspetiva legislativa: ponderação da encriptação como um direito; ponderação das limitações desse direito, sobretudo em confronto com outros direitos e deveres; ponderação das obrigações resultantes do uso de encriptação e consequências para a sua não observância.

5.

A representação da Eslováquia (Estado Membro que exerce neste momento a presidência do Conselho da União Europeia), anunciou que desenvolveu um trabalho de mapeamento da posição dos fornecedores de serviços perante a encriptação, ao nível nacional. Concluiu que uma boa parte dos Estados Membros tem legislação que obriga os fornecedores de serviços de telecomunicações a fornecer às autoridades o conteúdo de comunicações de forma legível. Porém, nenhum Estado permite dirigir uma ordem deste tipo a suspeitos.

É precisamente este o enquadramento legal português: os operadores de comunicações estão obrigados a permitir às autoridades, em condições e sob as garantias fixadas pela Constituição e pela Lei, o acesso a dados das comunicações e a respetiva interceção. Todavia, não existe uma obrigação desta mesma natureza para operadores de base *web* (por exemplo, o Facebook). Ou seja, ainda que os operadores portugueses estejam obrigados a permitir o acesso às comunicações que os seus clientes façam, se estes o fizerem utilizando

serviços *web* encriptados baseados no estrangeiro, não existem mecanismo legal para aceder a essas comunicações encriptadas (será, por exemplo, o caso de comunicações efetuadas por mensagens via Facebook).

Por outro lado, alguns dos Estados Membros estão a desenvolver quadros legislativos que lhes permitam introduzir meios de vigilância oculta em dispositivos, à distância – o que pode vir a contornar as dificuldades de acesso a prova encriptada.

Outra das ideias discutidas foi a da necessidade de considerar de forma separada a encriptação *online* (de comunicações) e a encriptação *offline* (de aparelhos, por exemplo *smartphones*, a cujo conteúdo é necessário aceder).

6.

Quanto a operações encobertas, a representação do Reino Unido partilhou a sua experiência prática e as dificuldades com que se tem deparado na execução das mesmas, em ambiente *web*. Estas operações estão sujeitas a limites legais, mas também áquilo que chamaram limites éticos. Por outro lado, quase sem exceção, têm um âmbito transfronteiriço: nem sempre é fácil, no início de uma ação encoberta, apurar a nacionalidade do suspeito que se procura investigar e, por outro lado, com muita facilidade se identificam suspeitos de outras nacionalidades e, sobretudo, baseados noutras jurisdições. Estas circunstâncias criam necessidade de interagir com autoridades destas outras jurisdições.

7.

Durante a reunião foi apresentado o nº 2 do *Cybercrime Judicial Monitor*, uma publicação da rede que pretende divulgar atualizações legais nos Estados Membros, análises de decisões judiciais e ainda explorar tópicos de especial interesse. No corrente número, o tópico especial abordado é o do acesso remoto a sistemas de computadores. A abordagem deste tópico foca-se, sobretudo, na análise dos regimes legais já consagrados nos diversos Estados Membros. Tal análise foi feita a partir das respostas a um questionário elaborado e distribuído para o efeito. A seu tempo, Portugal respondeu a esse questionário, que atempadamente remeteu – junta-se o mesmo como Anexo 3.

Foi ainda apresentada a versão finalizada do site web de acesso restrito, que serve de apoio à rede (a chamada EU Judicial Cybercrime Network Restricted Area, acessível em https://restricted.EUROJUST.europa.eu/my.policy).

8.

Por último, foram discutidos os diversos aspetos de conformação da rede, os quais foram propostos no documento de conceito que se junta como Anexo 2. Recorda-se que o Ministério Público de Portugal participou na reunião de génese desta rede, a 21 de Novembro de 2014 (junta-se o respetivo relatório como Anexo 4). Por constrangimento do horário do voo de regresso a Portugal, não foi possível ao subscritor assistir à parte final da reunião.

Lisboa, 24 de novembro de 2016

(Pedro Verdelho)

ANEXO 56

Questionário CJM2 – resposta de Portugal

1. Does your domestic applicable legal framework permit the remote access to a (computer) system **within the country's territory** in the context of a criminal investigation? **Yes. According to Article 15, number 5 of the Cybercrime Law (Law 109/2009, from 15 September), when, during a search, there are reasons to believe that the information sought is stored in another computer system, but these data are lawfully accessible from the initial system, the search can be extended by authorization of the competent authority (which is a prosecutor).**

    a. If yes, for which purposes (e.g. preservation, evidence collection) is it permitted? **The text of the law does not specify but, in general, the authorisation of a search includes the possibility to seize evidence. It is open to the jurisprudence (and there is still a limited number a cases) a range of questions, such as if this power includes the possibility to delete (illegal) content or other types of data.**

    b. If yes, is it permitted by virtue of special or general legal provisions (such as, e.g. the general rules on searches and seizures)? **Please, see above.**

        i. Please provide the full text of the relevant provision(s), accompanied by a brief explanation, if possible.

Article 15

Search of computer data

1 – When, during the proceedings, it becomes necessary for the gathering of evidence, in order to ascertain the truth, obtain certain and specific data stored in a given system, the judicial authority authorizes by order, or orders, a search in that computer system, and, where possible, leads the event.

2 - The order of the preceding paragraph has a maximum validity of 30 days, under penalty of nullity.

3 - The criminal police force may execute the search without prior judicial authority, when:

a) it is voluntarily consented by the person who has the availability or control of such data, provided that the consent is given in any documented way;

b) In cases of terrorism, violent or highly organized crime, when there is founded evidence of the imminence of a crime which poses a serious risk to life or health of any person.

4 - When the criminal police force searches a system under the preceding paragraph:

a) in the case of b) the investigation is immediately informed to the competent judicial authority so as it can validate it, with the penalty of nullity;

b) in any case, the report under Article 253 of the Code of Criminal Procedure must be fulfilled and forwarded to the competent judicial authority.

5 – When, during a of search, there are reasons to believe that the information sought is stored in another computer system or in a different part of the previous system, but these data are legally accessible from the initial system, the search can be extended by authorization of the competent authority in accordance with paragraphs 1 and 2.

6 – It will be applied to the searches referred to in this Article, mutatis mutandis, the rules for searches of the Code of Criminal Procedure and the Statute of the Journalist.

2. Is the remote access permitted when:

   a. the location of the data is **unknown**? **Yes. The remote access described above is applicable regardless of the location.**

      i. If yes, for which purposes (e.g. preservation, evidence collection) is it permitted?

      ii. Please provide the full text of the relevant provision(s), accompanied by a brief explanation, if possible.

   b. the data is located **abroad**? **Yes. The remote access described above is applicable regardless of the location – thus can be applicable to data stored abroad.**

      i. If yes, for which purposes (e.g. preservation, evidence collection) is it permitted?

      ii. Please provide the full text of the relevant provision(s), accompanied by a brief explanation, if possible.

3. Can the data gathered by means of remote access to a (computer) system be used as evidence in subsequent judicial proceedings? **The remote access can occur in the context of a search. During a search, seizure of evidence is allowed. Thus, if evidence is seized, it can be used in subsequent proceedings. Seizure of data, as evidence, can be executed, according to Article 16, number 7 of the Cybercrime Law (Law 109/2009, from 15 September), according to whichever is most appropriate and proportionate, taking into account the interests of the case, taking the following forms: seizure of the storage medium, by the production of a copy of the data; by preservation, by technological means, of the integrity of the data, without performing a copy or removing them, or removing in a non-reversing way or blocking the access to the data.**

   a. If yes, what are the conditions for their use?

   b. If yes, please provide the full text of the relevant provision(s), accompanied by a brief explanation, if possible.

Article 16

Seizure of computer data

1 - When, during a computer search or other legitimate access to a computer system, it is found computer data or computer documents that are necessary to gather, as evidence, in order to ascertain the truth, the competent judicial authority authorizes or orders their seizure.

2 - The criminal police force can seize computer data without prior judicial authority in the course of a search lawfully enforced under the previous article, as well as in emergency or when there is danger in delay.

3 – In case of seizure of computer data or computer documents which content is likely to disclose personal or intimate information, that would jeopardize the privacy of its owner or a third party, under penalty of nullity, the data or documents shall be submitted to the judge, who will consider its seizure regarding the concrete interests of the case.

4 - The seizures made by the criminal police force are always subject to validation by the judicial authority within 72 hours.

5 - Seizures related to computer systems used for the practice of legal professions, medical, banking and journalistic activities are subject, mutatis mutandis, the rules and procedures of the Code of Criminal Procedure and the Statute of the Journalist.

6 - The system of secrecy or official and state Secrets under Article 182 of the Code of Criminal Procedure shall apply mutatis mutandis.

7 - The seizure of computer data, whichever is most appropriate and proportionate, taking into account the interests of the case, may in particular take the following forms:

a) seizure of the media where the system is installed or seizure of the media where the computer data are stores, and the necessary devices for their reading;

b) production of a copy of the data on an autonomous media;

c) preservation, by technological means, of the integrity of the data, without performing a copy or removing them, or

d) removing in a non-reversing way or blocking the access to the data.

8 - In the case of seizure under b) above, the copy is made in duplicate, being one of the copies sealed and entrusted to the Clerk of Services where the investigation runs its terms and, if technically possible, the data entered are certified by digital signature.

4. Has your country enacted any legal provisions in the field of cybercrime since 1/1/2016? **NO**
    a. If yes, please provide the full text of the relevant provision(s), accompanied by a brief explanation, if possible.

5. Have your judicial authorities delivered any recent relevant decisions or judgements in cybercrime matters?
    a. If yes, please provide a copy of the full text of the decisions or judgements as well as a short summary of the issues/topics addressed therein, if possible.

THANK YOU VERY MUCH FOR YOUR CONTRIBUTION!

ANEXO 61

Criação do Fórum Lusófono

MINISTÉRIO PÚBLICO
PORTUGAL
gabinete CIBERCRIME

(Proposta de deliberação)

FORUM SOBRE CIBERCRIME E PROVA DIGITAL

Enquadramento

A internet é uma realidade omnipresente: as instituições e os cidadãos socorrem-se amplamente dela, nas suas quotidianas e regulares actividades; da mesma forma, os Estados apoiam-se nela no normal exercício das suas tradicionais funções. Desta enorme expansão da utilização regular dos meios informáticos resultou, além do mais, uma multiplicação exponencial de fenómenos cibercriminosos nas redes.

Estas novas actividades ilícitas trouxeram como grande novidade o respectivo desligamento do conceito territorial: as actividades nas redes são indiferentes aos conceitos de nacionalidade ou jurisdição; desconhecem fronteiras e são perpetradas a partir de qualquer ponto do globo, contra vítimas em qualquer ponto do globo.

Não obstante, a língua sobrevive como um dos motivos que levam os cibercriminosos a escolher e estabelecer contacto com as vítimas dos seus actos: será até, porventura, um dos mais importantes. Por exemplo, nas burlas praticadas com recurso a meios informáticos, a comunidade da língua, entre o criminoso e a vítima, é dos requisitos essenciais.

Este desiderato criou a necessidade de fortalecer a cooperação, nesta matéria, entre países que partilhem a mesma língua.

Objetivos gerais

É bem sabido que, no contexto global, apenas se poderão alcançar resultados efetivos na luta contra a cibercriminalidade com uma atuação especializada, coordenada, articulada e ágil. Porém, é igualmente verdade que estas especialização, coordenação e articulação somente são possíveis em ambientes de confiança e de partilha de informação.

No âmbito dos Ministérios Públicos dos Países Lusófonos, um tal ambiente de partilha de informação pode ser criado por via do estabelecimento de um fórum de magistrados especializados, onde participem representantes de todas as Procuradorias-Gerais.

Constituirá objetivo geral deste fórum a partilha de informação e conhecimento sobre os quadros jurídicos dos diversos países lusófonos, no âmbito da cibercriminalidade, bem como facilitar o intercâmbio de experiências e boas práticas processuais necessárias com vista à ultrapassagem dos múltiplos problemas técnicos e jurídicos com que os magistrados se defrontam nesta área, dos crimes informáticos e cometidos com o auxílio das tecnologias e das redes de informação e comunicação.
Esta partilha terá ainda como propósito criar um ecossistema favorável à agilização das formas e dos canais existentes para a cooperação judiciária internacional, entre as diversas autoridades judiciárias, tendo em vista aumentar a capacidade para combater o cibercrime e aumentar a eficácia na recolha, preservação e utilização de prova digital, em processo penal.

Esta iniciativa pretende ainda:

- sensibilizar o conjunto das Procuradorias-Gerais e os magistrados do Ministério Público do espaço lusófono para a dimensão do cibercrime e para a importância da prova digital na actividade judiciária moderna;
- detectar eventuais lacunas legislativas e, bem assim, identificar a necessidade de adopção de novos diplomas normativos que as colmatem;
- avaliar a conformidade das legislações nacionais com os quadros normativos internacionais e as recomendações de organismos internacionais nesta matéria e
- fomentar e apoiar a formação de magistrados do Ministério Público, nas áreas da cibercriminalidade e da obtenção da prova digital.

Resultados esperados

Em resultado das acções que vierem a ser empreendidas, espera-se que:

- seja melhorada a formação dos magistrados do Ministério Público do espaço lusófono em cibercriminalidade e uso de prova digital;
- os Ministérios Públicos do espaço lusófono contribuam para a avaliação dos seus quadros normativos, tendo em vista auxiliar os competentes órgãos a ponderar a adopção de novas soluções legislativas que supram as lacunas criadas pelas acções criminais modernas com uso de novas tecnologias;
- se ponderem a criação de estruturas especializadas de coordenação na área do cibercrime e da obtenção de prova digital e
- de todas as eventuais iniciativas levadas a cabo, resulte melhoria da capacidade de reacção, legal e operacional, dos Magistrados do Ministério Público do espaço lusófono às novas realidades criminógenas e às novas modalidades de prova, em suporte e ambiente digital.

Acções concretas a desenvolver

1.
Pretende desenvolver-se um fórum permanente, de contacto e intercâmbio, que propicie a partilha de informação e a discussão de tendências na cibercriminalidade e na obtenção de prova digital.
Para o efeito, cada uma das Procuradorias-Gerais indicará um ponto de contacto que a represente no fórum e nas suas reuniões. Tal ponto de contacto providenciará apoio aos restantes membros do fórum, em questões relacionadas com o seu país, na área da cibercriminalidade.

2.
Será realizada uma reunião anual dos pontos de contacto, destinada a permitir a partilha de eventuais atualizações legislativas ou operacionais que tenham ocorrido em cada um dos países e também a discussão de novas práticas e métodos de investigação criminal nesta matéria. Nestas reuniões discutir-se-ão também temas específicos, como a formação e especialização de magistrados, a harmonização legislativa entre os países lusófonos, a adesão a instrumentos internacionais.

3.
O fórum deverá ainda explorar possibilidades de criação de uma plataforma online de partilha de informação (legislativa e jurisprudencial, por exemplo) e de auxílio ao trabalho dos magistrados, na investigação e prossecução criminal nesta área.

4.
O fórum explorará ainda, tendo em vista a prossecução dos objectivos enunciados, o eventual desenvolvimento de outras actividades, como por exemplo *workshops* mais alargados de partilha de experiências e boas práticas, ou ainda debates sobre eventuais necessidades de iniciativas legislativas e de eventual acolhimento das normas internacionais de referência, ou sobre a necessidade e vantagem da instituição, no Ministério Público, de estruturas especializadas de coordenação na área do cibercrime e da obtenção de prova digital.

ANEXO 65

Relatório - III Jornadas Jurídicas do MP de Moçambique

MINISTÉRIO PÚBLICO
PORTUGAL
EM DEFESA DA LEGALIDADE DEMOCRÁTICA
gabinete CIBERCRIME

RELATÓRIO

Participação nas

III JORNADAS JURÍDICAS DO MINISTÉRIO PÚBLICO de MOÇAMBIQUE

19 a 21 de setembro de 2016

21 de setembro de 2016

Pedro Verdelho

Participação nas
III JORNADAS JURÍDICAS DO
MINISTÉRIO PÚBLICO de MOÇAMBIQUE
19 a 21 de setembro de 2016

1.

Decorreram, entre 19 e 21 de setembro de 2016, as III Jornadas Jurídicas do Ministério Público de Moçambique, nas instalações da Procuradoria-Geral da República de Moçambique, em Maputo, submetidas ao tema *Por um Ministério Público mais Eficiente na Defesa da Legalidade*.

Foi o subscritor designado para participar naquelas Jornadas. Junta-se a respetiva agenda como Anexo 1.

2.

Esta participação inseriu-se num contexto de cooperação e troca de experiências entre a PGR e o Ministério Público de Moçambique, que assumiu os custos desta participação. No convite, foi manifestado interesse específico em que se incluísse na agenda das Jornadas uma comunicação sobre a experiência portuguesa na prevenção e combate ao crime informático.

3.

Cumpre salientar, como nota liminar, a cordialidade evidenciada pelos vários magistrados moçambicanos que acompanharam o subscritor durante o evento, incluindo a Senhora Procuradora-Geral da República, Dra. Beatriz da Consolação Buchili.

4.

Quanto às sessões de trabalho desenvolvidas, sublinha-se o que de seguida se indica.

Uma das temáticas privilegiadas pelas jornadas, foi a da jurisdição administrativa, incluindo-se as vertentes fiscal e aduaneira. Foram a esse propósito feitas comunicações por vários magistrados do Ministério Público de Moçambique, sobre o "Regime Jurídico da Impugnação dos Atos Administrativos" (por Taíbo Mucobora), sobre a "Fiscalização prévia e responsabilidade financeira" (por Nazimo Aly Mussá), sobre a "Intervenção do Ministério Público na Jurisdição Aduaneira" (por Irene Afonso) e ainda sobre a "Intervenção do Ministério Público na Jurisdição Fiscal" (por Hermínia da Barca).

5.

Foi também propósito dos organizadores abordar temáticas penais de grande atualidade. Foi esse o contexto em que se inseriu a apresentação solicitada ao Ministério Público de Portugal (junta-se, como Anexo 3, a apresentação utilizada).

Após a apresentação, na fase de debate, os participantes mostraram-se interessados no quadro legislativo português, bem como na estrutura e funções do Gabinete Cibercrime. Suscitou também várias questões dos participantes o resultado das experiências realizadas pela Procuradoria-Geral da República na interação com os fornecedores de serviço Internet globais (Facebook, Google e Microsoft).

Houve ainda interesse dos participantes em detetar lacunas na forma como a legislação moçambicana encara os crimes no ciberespaço. A este propósito, foi referido que está em curso a revisão do Código Penal (já em sede parlamentar) e a do Código de Processo Penal, sendo informalmente solicitada a cooperação da Procuradoria-Geral de Portugal, na eventual formulação de sugestões, ao poder legislativo moçambicano, pela Procuradoria-Geral de Moçambique. Foi manifestada a total disponibilidade para o efeito.

Lateralmente, foi referido no debate que, em Angola, estão em apreciação pública os projetos de revisão do Código Penal e do Código de Processo Penal, neles se incluindo normas relevantes a propósito da cibercriminalidade e da obtenção de prova digital.

6.

A vertente penal das Jornadas foi, sobretudo, abordada por magistrados do Ministério Público estrangeiros. Foram assim abordadas as experiências de Angola (por Maria Teresa Manuela), quanto a prevenção e combate à criminalidade organizada e transnacional, de Macau (por Kong Chi), quanto a prevenção e combate ao crime de branqueamento de capitais e de Cabo Verde e Espanha (por Albertino Silva Mendes e Pedro Perez Enciso, respetivamente), quanto à recuperação de ativos.

7.

Um dos aspetos mais interessantes da abordagem penal foi o da problemática do abate e tráfico de espécies protegidas da fauna bravia. O tema foi introduzido por Carlos Lopes Pereira, Chefe de Departamento de Fiscalização da ANAC (a Administração Nacional de Áreas de Conservação) de Moçambique. Interveio nesta temática Albino Vasco Macamo, magistrado do Ministério Público, diretor do recém-criado Gabinete de Defesa dos Direitos e Interesses Difusos, da Procuradoria-Geral de Moçambique.

Fizeram ainda comunicações a este propósito o Professor Samuel K. Wasse, da Washington University, dos Estados Unidos da América (sobre a perícia a partes de espécies traficadas) e Brito Simango, jornalista da Televisão de Moçambique (sobre o papel da comunicação social na preservação do ambiente).

Este painel revelou-se extremamente interessante, por evidenciar fragilidades do sistema moçambicano que são comuns ao sistema português: as autoridades administrativas de conservação da natureza, presentes no terreno, detetam graves ameaças a espécies selvagens, mas depois as autoridades judiciárias não têm capacidade de resposta, ficando os respetivos responsáveis por punir nas instâncias judiciais.

8.

Lateralmente, foram ainda abordadas as temáticas da responsabilidade médica nos casos de erro e de negligência (por Eugénio Zacarias, Bastonário da Ordem dos Médicos de Moçambique) e da prevenção e combate à corrupção no setor privado.

9.

Anota-se, por fim, que assistiu a parte da reunião a Sra. Dra. Sara Agoas, Primeira Secretária da Embaixada de Portugal em Maputo.

21 de setembro de 2016

(Pedro Verdelho)

ANEXO 69

Relatório *Principles and options for an e-evidence exchange platform*

MINISTÉRIO PÚBLICO
PORTUGAL
gabinete CIBERCRIME

NOTA

"Expert Meeting on Principles and options for an e-evidence exchange platform"

Bruxelas

9 de novembro de 2016

1.

Decorreu em Bruxelas, em instalações da Comissão Europeia (que a convocou e patrocinou), uma reunião de peritos nacionais sobre "*Principles and options for an e-evidence exchange platform*". Tratou-se de uma reunião exploratória, na qual a Comissão pretendia aperceber as sensibilidades dos Estados Membros da União Europeia quanto ao estabelecimento de uma plataforma eletrónica que permita trocar, dentro da União Europeia, pedidos de cooperação judiciária referentes a prova eletrónica, no quadro da futura Decisão Europeia de Investigação.

2.

A participação na reunião de representação da PGR e de Portugal, foi determinada pela Procuradoria-Geral, em resposta a uma solicitação da Direção-Geral da Política de Justiça, do Ministério da Justiça.

3.

A agenda (que se junta como Anexo 1) foi essencialmente preenchida com a discussão de um documento previamente preparado pela Comissão Europeia ("*Principles and options for an e-evidence exchange platform - Discussion paper prepared by DG Justice and Consumers for the Expert Group on e-evidence*"), o qual se junta como Anexo 2.

4.

Em termos substantivos, o ponto mais importante da agenda foi a discussão, entre os Estados Membros, das eventuais respostas a dar às diversas perguntas colocadas pelo *Discussion Paper*.

Uma das primeiras, questionava sobre os potenciais utilizadores deste tipo de plataforma. Discutiu-se se os utilizadores credenciados para a mesma deveriam ser apenas pontos focais, centrais, a designar por cada Estado Membro ou, pelo contrário, todo o possível universo de beneficiários (designadamente, por exemplo, todo o conjunto dos magistrados do Ministério Público dos diversos Estados). Esta última opção recolheu um

alargado consenso. Portugal também se manifestou a favor desta opção, uma vez que a versão dos pontos focais seria um retrocesso – num contexto europeu em que são já permitidos e fomentados os contactos diretos entre magistrados dos diversos países.

Foi menos consensual a resposta à da tipologia de plataforma e ao nível da segurança: o documento em discussão elencava as diversas possibilidades técnicas: a utilização de comunicações por correio eletrónico, ou a de sistemas mais seguros de correio eletrónico, se necessário estruturados de forma específica; em alternativa, a construção de uma nova plataforma, seja centralizada ou descentralizada, de acesso seguro e com este fim específico.

A este respeito, reconheceu-se a vantagem de potenciar a simplicidade de um sistema de correio eletrónico. Porém, da discussão resultou que usar apenas este canal seria limitado, por não permitir o reconhecimento e autenticação de forma fácil. Por outro lado, o uso de uma plataforma centralizada poderá tornar o sistema mais vulnerável a ataques ou a falhas técnicas, acarretando também os riscos resultantes da concentração de toda a informação num só nó comunicacional.

Portugal pronunciou-se no sentido da implementação de um modelo misto, em que autenticação fosse centralizada, numa única plataforma comum a todos os Estados Membros da EU, mas em que fosse possível tirar partido da flexibilidade de comunicações por correio eletrónico, com a ponto, mais fáceis e expeditas, privilegiando o contacto direto entre o magistrado requerente de uma diligência e o magistrado requerido.

Discutiu-se ainda a necessidade que pode vir a haver de impor um limite ao "*tamanho*" da informação trocada por esta via (dada a limitação, a este respeito, das comunicações eletrónicas à distância). É sabido ser limitada a quantidade de informação transferível por correio eletrónico, como é também limitada a quantidade de informação transferível a partir de plataformas online.

Por último, abordou-se a dificuldade que as diferenças linguísticas podem significar e, por isso, a vantagem – ou não –, da implementação de um sistema automatizado de tradução. A tendência geral dos interventores foi no sentido da rejeição deste último, por as experiências havidas serem malsucedidas.

Portugal referiu a enorme vantagem que tem retirado do uso de formulários bilingues (que substituem a tradução) nos pedidos endereçados a fornecedores de serviços Internet globais, baseados fora do território nacional.

5.

Tratando-se de uma reunião exploratória das diversas possibilidades, foi feita uma apresentação de uma experiência piloto desenvolvida na Alemanha, pelo Ministério da Justiça do Estado de Nordrhein-Westfalen com o nome de *e-codex*. Trata-se de um mecanismo técnico que permite autenticar comunicações, que efetua de

forma segura, entre duas autoridades judiciárias de dois Estados diferentes, sem o recurso a a plataforma centralizada, mas com uso de tecnologia que faz a ponte entre ambos os sistemas.

Foi ainda feita uma apresentação do projeto *e-evidence*, mais conceptual que prático, desenvolvido ao nível universitário, pelo *Consiglio Nazionale delle Ricerche* (de Itália).

Lisboa, 9 de novembro de 2016

Carla Botelho

Pedro Verdelho

RELATÓRIO DA ACTIVIDADE

Gabinete Cibercrime

MINISTÉRIO PÚBLICO
PORTUGAL

PROCURADORIA-GERAL DA REPÚBLICA
GABINETE CIBERCRIME