gabinete CIBERCRIME

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