MINISTÉRIO PÚBLICO
PORTUGAL
PROCURADORIA-GERAL DA REPÚBLICA
GABINETE CIBERCRIME

Gabinete Cibercrime

PLANO DE AÇÃO

2017

gabinete cibercrime
cibercrime@pgr.pt

23 de fevereiro de 2017

http://cibercrime.ministeriopublico.pt/

PLANO DE AÇÃO

CIBERCRIME 2017

Enquadramento

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

2. 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*".

3. 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*".

4. No despacho de definição de objetivos estratégicos para 2016-2017, a Procuradora-Geral da

República, definindo o cibercrime e a prova digital como áreas prioritárias, fixou como objetivos estratégicos:
- "*capacitar os magistrados do Ministério Público e reforçar a cooperação com órgãos de polícia criminal na obtenção de prova digital e no combate ao cibercrime*" e
- "*continuar a dinamizar a rede de pontos de contacto de magistrados especializados em cibercrime*".
Diz-se ainda neste despacho que, "*para além do cumprimento dos objetivos estratégicos anuais agora estabelecidos, as diversas estruturas do Ministério Público podem e devem propor outras vertentes que entendam justificar especial investimento face aos resultados do ano anterior e às especificidades das suas funções, sem nunca perder de vista os objetivos estratégicos trianuais*".

Objetivos gerais

Com este plano de ação pretende continuar a desenvolver-se o conhecimento dos fenómenos de natureza criminal ocorridos nas redes de comunicações ou cometidos por via delas, no contexto nacional. Pretende, por via deste conhecimento, continuar a dotar-se o Ministério Público de condições de maior eficácia no tratamento destes mesmos fenómenos, sensibilizando os magistrados para as problemáticas que os envolvem.
É ainda objetivo geral deste plano de ação dar continuidade ao plano de formação específica, nesta área, dos magistrados do Ministério Público, designadamente sobre a obtenção de prova digital.
Por último, pretende ainda dar-se continuidade ao fomento da especialização prática de magistrados nesta temática, em cada uma das comarcas, para isso se contando com a rede de pontos de contacto existente.

Linhas de ação a desenvolver

1. Dinamização da rede de pontos de contacto do Cibercrime

A rede de pontos de contacto carece de dinamização.

O Gabinete Cibercrime criou (e tem mantido) uma rede de pontos de contacto em todas as comarcas. Tais pontos focais têm recolhido informação sobre a cibercriminalidade, que têm vindo a ser discutidas nas reuniões de pontos de contacto, sendo o resultado da discussão partilhado com os restantes colegas da comarca.
Porém, mais recentemente, os pontos de contacto têm vindo a assumir vertentes mais práticas e consequentes ao nível local, assumindo verdadeiras funções de magistrados especializados, a eles sendo, em muitos casos, especificamente distribuídos os inquéritos em que se investiguem crimes relacionados com estas temáticas.
A manutenção da rede supõe a sua dinamização, sobretudo no sentido da consolidação da especialização na distribuição de processos nesta área, que muitas das comarcas já implementaram.

2. Realização de sessões de trabalho/formativas nas comarcas

***Há necessidade de dar continuidade às sessões de trabalho formativas na área do cibercrime e da prova digital, mesmo em comarcas onde no passado recente se realizaram sessões*.**

Na execução do Plano de Ação para 2015/2016, foram realizadas sessões de coordenação nas comarcas do território nacional continental, nas quais participaram 313 magistrados do Ministério Público. A avaliação dessas sessões permitiu concluir que os magistrados acharam as mesmas muito importantes e úteis, por se realizarem na comarca e por incidirem em questões práticas (as quais foi possível discutir por terem sido apresentadas a pequenos grupos de participantes).
Muitos dos magistrados expressaram a necessidade de que tais sessões se repetissem com regularidade, de forma a manter atualização, numa área de evolução tão constante e tão rápida.

3. Desenvolvimento de iniciativas específicas dirigidas a práticas criminosas específicas

***Importa dar continuidade ao processo, em desenvolvimento, de constituição de um registo de processos em que se investiguem crimes de burla* online.**

De facto, uma das manifestações criminais que mais significativamente tem chegado ao Ministério Público é a das burlas em vendas *online*, suscetíveis de atingir um número muito significativo de vítimas, em todo o território nacional. O mesmo sucede com o uso abusivo de dados de cartões de crédito e o *phishing* bancário. Todos estes fenómenos têm dado origem a um número muito expressivo de queixas.
Entre muitos destes processos existirá até conexão processual. Importa continuar a desenvolver esforços no sentido de criar mecanismos de coordenação, que permitam aos magistrados titulares de processos desta natureza aperceber se um determinado processo de inquérito está em relação, designadamente de conexão, com outros também pendentes.

4. Cooperação com os órgãos de polícia criminal na obtenção de prova digital

Importa discutir com os órgãos de polícia criminal as linhas de evolução e iniciativas futuras neste domínio, do cibercrime e, sobretudo, da obtenção de prova digital.

A investigação de cibercriminalidade, bem como a de outros crimes que suponham a obtenção de prova digital é sofisticada e exige o recurso a novas e complexas provas. Os OPC têm vindo a referir que nem sempre lhes tem chegado suficiente conhecimento destes novos métodos de investigação e de obtenção de prova, sobretudo daqueles que têm sido 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).
Por outro lado, importa discutir com os órgãos de polícia criminal boas práticas, que podem por exemplo passar pelo desenvolvimento conjunto de modelos ou formulários de apreensão de elementos de prova.

5. Intensificar a cooperação internacional e a troca de experiências e de boas práticas

Importa cooperar nas atividades da* European Judicial Cybercrime Network. *Por outro lado, tendo sido acometida à Procuradoria-Geral da República de Portugal a tarefa de impulsionar, quer a CiberRede /* CiberRed*, quer o Fórum Lusófono sobre Cibercrime e Prova Digital, importa dinamizar a efetiva operacionalização destes grupos de trabalho.

A cibercriminalidade é, mais que outros fenómenos criminógenos, pela sua própria natureza, transnacional. Desta característica resulta que a cooperação internacional é crucial em quase todas as investigações concretas. Mas resulta também que é essencial o intercâmbio internacional de experiências e boas práticas. É, pois, determinante, tirar o melhor partido das vantagens de todos os canais e instrumentos de cooperação internacional disponíveis.
No decurso de 2016, a Procuradoria-Geral da República participou na fundação da *European Judicial Cybercrime Network*, ou Rede Judicial Europeia para matérias do Cibercrime. Por outro lado, esteve na origem da proposta de criação, no seio da Associação Ibero Americana de Ministério Públicos, da CiberRede / *CiberRed*, Rede Ibero Americana de Ministérios Públicos na área do Cibercrime. Por último, foi também da Procuradoria-Geral da República a proposta, aprovada pelos Procuradores-Gerais da CPLP, de constituição de um Fórum Lusófono sobre Cibercrime e Prova Digital.

6. Considerar e ponderar os desafios colocados ao direito penal e ao processo penal pelas tecnologias da informação e comunicação

É prioritário impulsionar a reflexão, na comunidade jurídica, das necessidades de ajustamento do processo penal à era digital.

Na era da Internet, a vida e as rotinas alteraram-se de forma muitíssimo significativa, por exemplo, pela massificação de vias e modos de comunicação informais e desmaterializados.
Estas circunstâncias levaram a que, no Plano de Ação 2015-2016, se determinasse a exploração de mecanismos que permitissem dar seguimento a denúncias criminais recebidas por correio eletrónico.
Entre outras, importa avaliar a experiência realizada a este propósito, retirando-se desta avaliação conclusões sobre eventuais soluções de futuro. Mas importa mais: importa avaliar a necessidade de introdução de alterações, por exemplo legislativas, ou às rotinas processuais, impostas por estes novos mecanismos que, à revelia das normas e das práticas estabelecidas, acabam por arrastar para o processo penal as informalidades das vias de comunicação modernas.

7. Articulação do Ministério Público com outras entidades

O rápido conhecimento da notícia do crime do crime e a realização de diligências urgentes de obtenção de prova são condições de sucesso na investigação de crimes no ambiente digital.

O Plano de Ação 2015-2016 definia como prioridade o desenvolvimento da articulação e cooperação com entidades responsáveis pela segurança informática. Tinha-se em vista desenvolver formas de coordenação com entidades públicas e outros atores (em causa estava então, sobretudo, o Centro Nacional de Cibersegurança), com o propósito de vir a permitir, de forma expedita, o recebimento da notícia do crime e a remessa das participações

ao serviço do Ministério Público competente.
Com a recente criação e instalação da Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica, na Polícia Judiciária, esta necessidade de articulação externa do Ministério Público, em situação urgente, torna-se ainda mais premente.

8. Interação com a comunidade, sobretudo em contexto de risco

É necessário fazer chegar a preocupação de prevenção a contextos de risco (escolas, por exemplo), dando a conhecer a competência e a ação do Ministério Público nesta área específica.

Assim é porque, entre muitas outras características específicas, a cibercriminalidade e demais ilícitos praticados nas redes, caracteriza-se pela sua difusão metástica, podendo atingir vítimas em qualquer local e em qualquer contexto, desde que tenham acesso a redes de comunicações.

Enquadramento temporal
2017