



**MINISTÉRIO PÚBLICO  
PORTUGAL**

**PROCURADORIA-GERAL DA REPÚBLICA**

**GABINETE CIBERCRIME**

**Gabinete Cibercrime**

**PLANO DE ATIVIDADES**

**2018**



## PLANO DE ATIVIDADES

### CIBERCRIME 2018

#### 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 para o Ano Judicial 2018*, o cibercrime e a prova digital foram apontados como *área prioritária*. Neste documento fixam-se, como objetivos estratégico,:

- "capacitar os magistrados do Ministério Público e reforçar a cooperação com os órgãos de polícia criminal na obtenção de prova digital e no combate ao cibercrime.
- continuar a dinamizar a rede de pontos de contacto de magistrados especializados em cibercrime.
- continuar a promover a articulação com as redes internacionais de combate ao cibercrime, em especial no âmbito da Rede Ibero-Americana de Cooperação Jurídica Internacional (IBerRed) e o Fórum Lusófono sobre Cibercrime e Prova Digital."

**3.** A Lei 96/2017, de 23 de agosto, que define os objetivos, prioridades e orientações de política criminal para o biénio de 2017-2019 estabelece que a cibercriminalidade é um fenómeno criminal:

- de *prevenção prioritária* – Artigo 2º, alínea c) e
- de *investigação prioritária* – Artigo 3º, alínea g).

Fundamenta esta determinação a " *utilização da Internet como veículo de comunicação e propaganda associada ao terrorismo e aos crimes de ódio, os atentados contra os sistemas de informação dos Estados, a tendência para o aumento de casos de extorsão e de furto de credenciais de serviço de armazenamento em nuvem, a deslocação de formas de crime tradicional — em particular dos tráficos — para o ambiente digital, a incidência de crimes contra a liberdade e autodeterminação sexual praticados através da Internet*", que são indicados como " *fatores que apontam no sentido da necessidade de manutenção de esforços na prevenção e repressão do cibercrime (...)*".

**4.** Na Diretiva nº 1/2017 da Procuradora-Geral da República, que fixa *Diretivas e Instruções Genéricas para Execução da Lei de Política Criminal para o Biénio 2017/2019*, em matéria de cibercriminalidade, determina-se que " *deverá ser dado particular relevo aos crimes previstos na Lei*

*do Cibercrime (Lei nº 109/2009, de 15 de setembro) e aos crimes praticados com recurso à Internet que afetem uma elevada pluralidade de vítimas".*

## Objetivos gerais

Com este plano de atividades, dando-se continuidade aos planos de ação de anos anteriores, pretende continuar a dotar-se o Ministério Público de maior eficácia no tratamento dos fenómenos criminais no ciberespaço, sensibilizando os magistrados para as problemáticas que os envolvem.

Com esse propósito, dar-se-á continuidade ao plano de formação específica dos magistrados do Ministério Público nesta área, designadamente quanto à obtenção de prova digital. Mas além disso, pretende ainda dar-se continuidade ao propósito de especialização de magistrados nesta temática, nas comarcas, articulando-se a mesma com a rede de pontos de contacto já existente.

## Linhas de ação a desenvolver

### **1. Dinamização e robustecimento da rede de pontos de contacto do Cibercrime**

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, antevê-se como vantajoso que os pontos de contacto assumam papéis mais práticos e consequentes ao nível local, tornando-se magistrados especializados, a quem possam, por exemplo, ser especificamente distribuídos os inquéritos em que se investiguem crimes relacionados com estas temáticas. Importa, pois, dinamizar esta rede, no sentido da consolidação da especialização.

### **2. Realização de sessões de trabalho/formativas nas comarcas**

Ao longo dos últimos anos, o Gabinete Cibercrime tem vindo a desenvolver sessões formativas e de coordenação nas diversas comarcas do território nacional. De forma consistente e persistente, a avaliação dessas sessões permitiu concluir que os magistrados acharam as mesmas muito importantes e úteis. Detetou-se que assim foi, por um lado, por tais sessões terem lugar nas comarcas, não exigindo aos magistrados deslocação para fora do seu local habitual de trabalho. Mas também por privilegiarem uma abordagem prática das questões, em grupos pequenos, o que facilitou o diálogo e a troca de experiências.

Foi recorrente, por parte dos magistrados das comarcas, a expressão de vontade de que estas sessões se repetissem com regularidade, de forma a manter atualização, numa área de evolução tão constante e tão rápida.

Por outro lado, em exercícios anteriores tem vindo a ser manifestada a necessidade de sensibilizar os magistrados judiciais nas comarcas (que em alguns casos assistiram às reuniões promovidas pelo Gabinete Cibercrime), para a especificidade da cibercriminalidade e da prova digital, bem como para a complexidade da realidade do ciberespaço. Paralelamente, sente-se a necessidade de apoiar os magistrados do Ministério

Público na formulação de solicitações ao juiz de instrução, por forma a que as mesmas sejam mais facilmente perceptíveis e atendidas.

### **3. Desenvolvimento de iniciativas específicas dirigidas a práticas criminosas específicas**

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**

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 portuguesas 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**

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.

Desde 2016 que a Procuradoria-Geral da República participa nas atividades da *European Judicial Cybercrime Network*, ou Rede Judicial Europeia para matérias do Cibercrime. Por outro lado, a Procuradoria-Geral da República, por via do Gabinete Cibercrime, esteve na origem da proposta de criação, no seio da Associação Ibero Americana de Ministérios 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**

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 se determinasse, em planos de ação anteriores, a exploração de mecanismos que permitissem dar seguimento a denúncias criminais recebidas por correio eletrónico.

Importa dar continuidade a esses mecanismos experimentais, avaliando a experiência realizada a este propósito, retirando-se desta avaliação conclusões sobre eventuais soluções de futuro. Mas importa também 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**

Uma das vertentes mais importantes da atividade do Gabinete Cybercrime é a do diálogo com entidades públicas responsáveis pela segurança informática. Tem-se, sobretudo, em vista propiciar coordenação, 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. O mesmo sucede com a Unidade Nacional de Combate ao Cybercrime e à Criminalidade Tecnológica da Polícia Judiciária.

### **Enquadramento temporal**

2018