



**MINISTÉRIO PÚBLICO
PORTUGAL**

PROCURADORIA-GERAL DA REPÚBLICA

GABINETE CIBERCRIME

Gabinete Cibercrime

PLANO DE ATIVIDADES

2019

PLANO DE ATIVIDADES

CIBERCRIME 2019

Objetivos Gerais e Estratégicos

Dando-se continuidade aos planos de ação de anos anteriores, o Gabinete Cibercrime pretende contribuir para dotar 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.

Além disso, pretende 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. Por outro lado, é assumido como objetivo estratégico intensificar o diálogo com os órgãos de polícia criminal especificamente sobre a obtenção de prova digital, de forma a agilizar e tornar mais eficiente a cooperação no combate ao cibercrime.

Por último, é propósito primordial do Gabinete Cibercrime reforçar a cooperação e articulação com as redes internacionais especializadas de combate ao cibercrime (em especial a CiberRede/CiberRed – Rede Ibero-Americana de Cooperação na Área do Cibercrime e o Fórum Lusófono sobre Cibercrime e Prova Digital, mas também a *European Judicial Cybercrime Network*).

Linhas de Ação

1. Reforço da rede de pontos de contacto, como células de especialização

O Gabinete Cibercrime mantém uma rede de pontos de contacto em todas as comarcas, composta por magistrados especializados que, apesar da mobilidade própria da função, têm vindo a acumular conhecimento e experiência acrescida nas temáticas da prova digital e do cibercrime.

Será vantajoso reforçar a sua intervenção prática e processual, para que a estes magistrados especializados 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

O Gabinete Cibercrime tem vindo a desenvolver, de forma cíclica, sessões formativas e de coordenação nas diversas comarcas do território nacional.

A avaliação dessas sessões permitiu concluir que, de forma consistente e persistente, os magistrados acharam as mesmas muito importantes e úteis. Detetou-se que assim foi, por um lado, por tais sessões se realizaram nas próprias 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.

De igual modo, tem sido recorrente o interesse manifestado pelos magistrados na repetição regular das sessões, tendo em vista ir mantendo alguma atualização - necessária, mais que noutras, nesta área de evolução tão constante e tão rápida.

3. Avaliação de mecanismos implementados

Em execução de planos de ação de anos anteriores, o Gabinete Cibercrime desenvolveu novos métodos e procedimentos. Por exemplo, introduziu mecanismos experimentais que permitem dar seguimento a denúncias criminais recebidas por correio eletrónico. Também por exemplo, espoletou a celebração de protocolos com instituições universitárias, tendo em vista a obtenção de peritos informáticos. Ou ainda, dinamizou cooperação específica com operadores de comunicações.

Importa avaliar o funcionamento desses mecanismos experimentais, retirando desta avaliação conclusões sobre eventuais soluções de futuro.

4. Cooperação específica com os órgãos de polícia criminal

A investigação de cibercriminalidade e a obtenção de prova digital foram, no passado, uma área de trabalho específica da Polícia Judiciária. A prática veio desconstruir este modelo, disseminando por todos os órgãos de polícia criminal processos concretos que tocam aspetos “digitais”.

Importa articular o Ministério Público com os vários órgãos de polícia criminal, tendo em conta tornar eficiente o modelo de cooperação funcional e a efetiva direção do inquérito.

A obtenção de prova digital é sofisticada e exige o recurso a novos e complexos métodos e procedimentos. Os diversos órgãos de polícia criminal têm referenciado a sua própria insuficiência a este respeito.

Importa pois explorar a definição de boas práticas, as quais podem, por exemplo, passar pelo desenvolvimento conjunto de modelos ou formulários de obtenção de prova.

5. Desenvolvimento de iniciativas específicas dirigidas a práticas criminosas específicas

Uma das manifestações criminais *digitais* 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 e de inquéritos.

Entre muitos destes processos existirá 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, de conexão com outros também pendentes.

Importa finalizar o processo em curso de estabelecimento de uma base de dados de apoio à investigação de crimes de burla, se ocorridos *online*.

6. Identificação de desafios colocados ao direito penal e ao direito processo penal pelas tecnologias da informação e comunicação

Importa identificar novos fenómenos crimínógenos e a forma de os investigar e contrariar, de modo a melhor adequar a resposta do Ministério Público aos mesmos.

Mas importa também identificar eventuais necessidades de ajustamento legislativo, sobretudo em sede de prova digital.

7. Intensificação da troca de experiências e de boas práticas

A cibercriminalidade é, mais que outros fenómenos crimínógenos, 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. Importa consolidar a participação nesta rede de cooperação.

Por outro lado, a Procuradoria-Geral da República, por via do Gabinete Cibercrime, coordena a CiberRede / *CiberRed* - Rede Ibero Americana de Ministérios Públicos na área do Cibercrime. Do mesmo modo, a Procuradoria-Geral da República coordena o Fórum Lusófono sobre Cibercrime e Prova Digital (que inclui os Ministérios Públicos dos países membros da CPLP).

Importa reforçar a liderança destas redes especializadas, dinamizando-as e intensificando a troca de experiências.

8. Articulação do Ministério Público com outras entidades

Uma das vertentes mais importantes da atividade do Gabinete Cibercrime 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.

Mas têm-se também em vista a perspetiva mais institucional, de coordenação de nível superior. Neste campo, é determinante a interação com o Conselho Superior de Segurança do Ciberespaço e com a Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica da Polícia Judiciária.

Enquadramento temporal

2019

Iniciativas

1. Reforço da rede de pontos de contacto, como células de especialização

- a. Diálogo com as comarcas, sobre especialização
- b. Dinamização da Rede de Pontos de Contacto
- c. Dinamização do Grupo Técnico de Apoio

2. Realização de sessões de trabalho/formativas nas comarcas

- a. Desenvolvimento de sessões nas comarcas do território nacional.

3. Avaliação de mecanismos implementados

- a. Perícias nas universidades
- b. Procedimento de encaminhamento de denúncias
- c. Cooperação com operadores de comunicações

4. Cooperação específica com os órgãos de polícia criminal

- a. Coordenação com a Polícia Judiciária, quanto a critérios materiais de delegação de competência para investigação
- b. Dinamização de novos procedimentos, por exemplo no recebimento de queixas relacionadas com crimes que supõem prova digital

5. Desenvolvimento de iniciativas específicas dirigidas a práticas criminosas específicas

- a. Plataforma de registo de burlas *online*
- b. Resposta 24/7

6. Identificação desafios colocados ao direito penal e ao processo penal pelas tecnologias da informação e comunicação

- a. Darkweb
- b. Fake news
- c. Legislação sobre prova digital

7. Intensificação da troca de experiências e de boas práticas

- a. Dinamização das redes

8. Articulação do Ministério Público com outras entidades

- a. UNC3CT
- b. CNCS