MINISTÉRIO PÚBLICO
PORTUGAL
PROCURADORIA-GERAL DA REPÚBLICA
PROCURADORA-GERAL

Ordem de Serviço Nº 1/19

Cibercrime e outros crimes cometidos em ambiente digital
Rede de magistrados especializada

A eficácia da investigação e da ação penal está cada vez mais dependente de especialização daqueles que a dirigem. Assim acontece, em particular, quanto a crimes cometidos em ambiente digital. Os ilícitos praticados com utilização de redes de comunicações, contra meios tecnológicos ou com recurso às tecnologias traduzem atuações concretas tecnicamente complexas e sofisticadas, cuja interpretação supõe conhecimentos específicos no domínio da informática.

Na estrutura do Ministério Público, a direção da investigação em inquéritos em que esteja em causa criminalidade em ambiente digital não tem sido uniformemente distribuída de forma especializada pelos magistrados. Há, porém, casos de distribuição especializada, por exemplo, nas Comarcas de Lisboa e do Porto.

Na comarca de Lisboa, existe especialização na distribuição de crimes previstos na Lei do Cibercrime, na Lei de Proteção de Dados Pessoais e de crimes de burla informática, incluindo burlas cometidas por via de meios informáticos e de redes de comunicações. Na prática, esta especialização inclui, além dos *cibercrimes*, os processos em que se investigue *phishing*, o uso abusivo de dados de cartões de crédito e a clonagem de cartões bancários. Existe ainda especialização na distribuição de processos respeitantes a crimes de pornografia de menores por via de meios tecnológicos, que são agregados aos restantes crimes contra menores.

Na comarca do Porto, existe especialização na distribuição de processos em que se investiguem crimes genericamente cometidos por via de sistemas informáticos, com exceção dos crimes de burla *online* e dos crimes de pornografia infantil por via de meios tecnológicos (estes, estão agregados aos outros crimes sexuais). Na prática, esta especialização inclui os crimes previstos na Lei do Cibercrime, o *phishing* bancário, o uso abusivo de dados de cartões de crédito e a clonagem de cartões bancários.

Estas experiências de especialização têm sido avaliadas de forma muito positiva, em particular pelos magistrados colocados nas secções em causa - por um lado, porque potenciam a gestão e cruzamento de informação nestas áreas de criminalidade e, por outro, porque permitem concentrar a investigação deste tipo de processos em magistrados com maior vocação e apetência técnica para os mesmos.
Numa perspetiva organizativa, a especialização tem tido a vantagem de rentabilizar o investimento na capacitação e no reforço de competências e capacidades técnicas para lidar com este tipo de criminalidade.

O meio tecnológico ou digital em que é praticada tem definido o elemento diferenciador de alguma da criminalidade moderna, correspondente a fenómenos criminógenos relacionados com as tecnologias ou praticados por via destas.
Embora a expressão *cibercrime* emane da Lei do Cibercrime (Lei nº 109/2009, de 15 de setembro) e se reporte primordialmente aos tipos de ilícito ali descritos, a cibercriminalidade tem-se revelado de muito maior espectro, incluindo muitos outros crimes de natureza diversa praticados com auxílio ou por via das tecnologias. A estes crimes aplicam-se os mesmos métodos e modelos de investigação do cibercrime. Também quanto a eles (tal como acontece com os chamados *cibercrimes em sentido restrito*, descritos na Lei do Cibercrime), é necessário obter prova em formato digital, por vezes por via de perícias. Em relação a todos se requer, de quem os investiga, que tenha compreensão deste meio.
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.

Quanto às exigências investigativas, os processos de inquérito em que se investiga este conjunto de tipos de crime, podem dividir-se em três grupos:

- as investigações respeitantes a crimes previstos na Lei do Cibercrime e na Lei de Proteção de Dados Pessoais;
- as investigações respeitantes a crimes de burla informática, previstos no Artigo 221º do Código Penal, e
- as investigações respeitantes a todos os restantes tipos de crime, em cuja prática são utilizados meios tecnológicos – por exemplo, difamações, ameaças, difusão de pornografia infantil, ou burlas cometidas por via da Internet.

As exigências de especialização são diversas, quanto a cada um destes tipos de investigação.

Há claramente necessidade de especialização quanto aos crimes previstos na Lei do Cibercrime e na Lei de Proteção de Dados Pessoais que supõem, pela sua própria natureza, sofisticação técnica e, consequentemente, exigem de quem investiga conhecimentos técnicos elevados.

Porém, o mesmo não acontece, por exemplo, com a generalidade dos crimes contra a honra ou de violação de privacidade cometidos *online*. A investigação de difamação por via de *email* ou por via de um *post* no Facebook não supõe conhecimentos especiais da tecnologia, uma vez que a respetiva prática também não supõe especial uso da tecnologia. Da mesma forma, por exemplo, a prática de burla por via de uma plataforma de vendas *online* não requer, de quem o pratica, o uso de especiais meios tecnológicos. Em consequência, não se exige de quem investiga este tipo de crimes que reúna conhecimentos técnicos excecionalmente elevados que vão para além dos conhecimentos médios de um utilizador habitual das tecnologias. É suposto que a generalidade dos magistrados do Ministério Público atinja, pelo menos, estes conhecimentos médios de um habitual utilizador das tecnologias.
Estes motivos são aplicáveis à generalidade dos crimes praticados com utilização de meios tecnológicos, se esta utilização se fizer ao nível do utilizador comum.

Já assim não acontecerá com alguns dos inquéritos em que se investigam crimes que, transversalmente a estas categorias, revelam uma utilização de meios tecnológicos revestida de particular sofisticação. Será por exemplo o caso, entre outros, dos processos em que se investigue *phishing* ou manipulação e utilização abusiva de dados de cartões de crédito, bem como o caso de algumas burlas informáticas (Artigo 221º do Código Penal).
Da mesma forma, justifica-se especialização na distribuição de processos que suscitem particulares exigências na obtenção de prova digital, ou em que se investiguem factualidades particularmente complexas praticadas com o uso de tecnologias.

Impõe-se pois que, para a investigação de alguns destes tipos de ilícitos, o Ministério Público adapte a sua estrutura organizativa por forma a responder adequada e cabalmente às exigências apresentadas pelos mesmos o que passa pela afetação dos inquéritos que investiguem aqueles fenómenos criminais a magistrados especializados, sempre que as especificidades dos DIAP e das Comarcas o consintam.
Desta forma se logrará melhorar a eficácia na investigação nestes tipos de crimes, contribuindo para a correta qualificação jurídica e aperfeiçoando a qualidade das respostas do Ministério Público no cumprimento das suas competências.

No contexto das atividades do Gabinete Cibercrime da Procuradoria-Geral da República (em atividade desde 2011), foi constituída uma rede informal de pontos de contacto que integra magistrados do Ministério Público de todas as Comarcas. Esta rede é um dos instrumentos essenciais da atividade de coordenação do Ministério Público nesta área e constitui também um privilegiado fórum permanente de reflexão e discussão sobre estas temáticas.

As exigências de especialização na investigação de criminalidade informática ou de outros ilícitos que suponham, de forma complexa, a obtenção de prova digital apontam para uma configuração mais robusta, formal e interventiva da rede de pontos de contacto por forma a que a estes magistrados especializados sejam, sempre que possível, privilegiadamente, distribuídos inquéritos destas temáticas. Algumas das Comarcas já deram importantes passos nesse sentido, mas noutras este percurso está por fazer.

Assim, em conformidade com o exposto, com vista à eficácia da intervenção do Ministério Público, ao abrigo do disposto na al. b) do nº 2, do art. 12º do Estatuto do Ministério Público, determino:

1. A criação da Rede Nacional de Procuradores Especializados em Cibercrime e Prova Digital (Rede Cibercrime), coordenada pelo Gabinete Cibercrime da Procuradoria-Geral da República.

2. Os Senhores Magistrados do Ministério Público Coordenadores de Comarca indicam ao Gabinete Cibercrime, segundo a dimensão e as caraterísticas da comarca, o número e o nome dos magistrados a integrar a Rede Cibercrime. Da mesma forma, indicam ao Gabinete Cibercrime a respetiva substituição, por exemplo, quando ocorra movimentação do magistrado indicado, ou por qualquer outra razão de serviço.

3. Assumem de imediato a função de pontos de contacto da Rede Cibercrime, sem necessidade de qualquer diligência nesse sentido, os magistrados previamente designados para a rede informal pré-existente, os quais constam da lista anexa à presente Ordem de Serviço.

4. O Gabinete Cibercrime mantém atualizada, e disponível no SIMP, a lista dos pontos de contacto da Rede Cibercrime, promovendo uma reunião dos mesmos, pelo menos, duas vezes por ano.

5. Os pontos de contacto da Rede Cibercrime participam na respetiva atividade e devem, designadamente:

a. Recolher, nas suas circunscrições, informação sobre as problemáticas da realidade processual concreta na área da cibercriminalidade, para debate nas reuniões de pontos de contacto;
b. Transmitir aos magistrados da respetiva circunscrição as conclusões alcançadas nas reuniões;
c. Recolher, tendo em vista a sua partilha, os casos e decisões mais significativos que, nesta área, tenham sido proferidas nos tribunais da respetiva circunscrição.

6. Os Senhores Diretores dos Departamentos de Investigação e Ação Penal com sede na área dos Tribunais da Relação e os Senhores Magistrados do Ministério Público Coordenadores de Comarca devem favorecer, sempre que as especificidades daqueles DIAP e das Comarcas o consintam, um modelo de distribuição concentrada, privilegiadamente aos pontos de contacto, dos processos de inquérito referidos no número seguinte.

7. Devem considerar-se para efeitos de distribuição concentrada, designadamente, os inquéritos em que se investiguem:

a) Crimes previstos na Lei do Cibercrime e na Lei de Proteção de Dados Pessoais;
b) Crimes de burla informática, previstos no Artigo 221º do Código Penal, e;
c) Outros crimes, se na prática dos mesmos houver recurso a meios tecnológicos particularmente sofisticados, ou quando haja particulares exigências na obtenção de prova digital ou, ainda, quando se investiguem factualidades particularmente complexas, praticadas com o uso de tecnologias.

8. Não serão de incluir na distribuição concentrada os processos de inquérito respeitantes a levantamento de quantias por via de uso de cartões bancários em máquinas ATM ("Multibanco"), com obtenção abusiva do cartão e/ou do respetivo código.

Divulgue-se a através do SIMP (página principal e SIMP temático Cibercrime) e insira-se no módulo "Documentos Hierárquicos" do SIMP e do Portal do Ministério Público, subespécie "Ordens de Serviço".

Lisboa, 16 de janeiro de 2019

A Procuradora-Geral da República

(Lucília Gago)