Estratégia da Procuradoria-Geral da República

Cibercrime

março de 2025

ESTRATÉGIA CIBERCRIME

2025 / 2027

MAIS EFICÁCIA NA INVESTIGAÇÃO

 http://cibercrime.ministeriopublico.pt/

 cibercrime@pgr.pt

*O **Gabinete Cibercrime** foi criado, em 2011, no seio do Ministério Público, como uma estrutura informal da Procuradoria-Geral da República, ao qual foi atribuída a genérica finalidade de coordenar a atividade do Ministério Público na área da cibercriminalidade e da obtenção de prova digital.*

Após a alteração do Estatuto do Ministério Público (Lei nº 68/2019, de 27 de agosto, em vigor a partir de 1 de janeiro de 2020), por Deliberação do Conselho Superior do Ministério Público de 20 de outubro de 2020, o Gabinete Cibercrime passou a ter o estatuto de Gabinete de Coordenação Nacional (artigo 55º do EMP).

Um dos mais concretos e eficazes instrumentos práticos de coordenação a nível nacional é a Rede Cibercrime. Trata-se de uma rede de magistrados do Ministério Público que conta com pontos de contacto em todas as comarcas do país. Existe desde 2012, embora apenas tenha tido corpo formal a partir de 2019, por via da Diretiva nº 1/2019 da Procuradora-Geral da República. Além de instituir a Rede Cibercrime, esta Diretiva também aponta para a necessidade de especialização na área do cibercrime, no seio da estrutura de investigação criminal do Ministério Público.

1. RESPOSTA AO CRESCIMENTO DO FENÓMENO

Desde 2012 está ativo e disponível o endereço eletrónico cibercrime@pgr.pt, que originariamente teve como primordial propósito o de permitir aos cidadãos contactar com o Gabinete Cibercrime. Porém, após o início de 2016, passou também, expressamente, a aceitar denúncias da prática de crimes relacionados com a atividade daquele Gabinete. Tais denúncias, crescente e persistentemente mais numerosas de ano para ano, representam apenas uma pequena parte daquelas que são recebidas por todos os serviços do Ministério Público, mas constituem uma fiel amostragem desta realidade.

No ano de 2020 as denúncias recebidas por via daquele endereço de correio eletrónico aumentaram de forma excecional após a eclosão da pandemia da COVID 19. Em 2021, o aumento foi ainda mais expressivo que em 2020: na totalidade do ano de 2021 foram recebidas 1160 denúncias, enquanto em 2020 tinham sido recebidas 544. Em 2022 esta tendência manteve-se: foram

recebidas 2124 denúncias. Portanto, em relação a 2021 (1160 denúncias) registou-se um aumento de 73,58%. Quanto a 2023, foram recebidas 2916 denúncias – correspondendo a 137,29% das denúncias do ano anterior (em 2022 tinham sido recebidas 2124 denúncias). Por último, em 2024, foram recebidas 3973 denúncias, ou seja, mais 36,25% que no ano anterior.

Portanto, pode dizer-se que de forma consistente, de ano para ano, são recebidas muitíssimas mais denúncias que no ano anterior. Este sinal é indicador de que a cibercriminalidade é um fenómeno em permanente e claríssima expansão.

É verdade que esta enorme expansão foi impulsionada pela pandemia da COVID 19, altura em que a digitalização de inúmeros aspetos da vida e da economia fez incrementar a economia *online*. Porém, o crescimento dos crimes denunciados já superou em muito aquele que se verificou durante a pandemia. Passado o efeito daquela, ficou um aumento estruturado, que persiste de forma constante e consistente.

Esta amostragem de denúncias, recebidas por correio eletrónico, indica claramente que importa reequacionar a forma como está a responder-se ao fenómeno da cibercriminalidade sob pena de, perante o aumento crescente e constante de casos, a pressão dos mesmos sobre o sistema de investigação criminal vir a esgotar e esmagar a capacidade de reação. Além disso e por outro lado, tendo em vista a eficácia da atividade do Ministério Público, é imprescindível encarar o fenómeno a partir de outro ângulo.

Correntemente, após o recebimento por correio eletrónico (mas também em papel, no tribunal), de denúncias de fenómenos deste tipo, as mesmas são remetidas aos departamentos locais do Ministério Público, sendo introduzidas no circuito normal de tratamento processual de todas as restantes denúncias. Isto é, o tratamento ulterior dado às denúncias das diversas manifestações daquilo que é comummente catalogado como cibercrime é o mesmo dado a todas as restantes, recebidas pelo Ministério Público.

Sucede, porém que, pelos factos denunciados e sobretudo pela natureza da prova com eles relacionada, algumas das denúncias de cibercrime requerem ação imediata, sob pena de, não a havendo, a prova se dissipar ou a ação criminosa continuar. Assim acontece, por exemplo, quando são denunciadas atividades ilegais desenvolvidas por páginas na Internet, tais como páginas

falsas de supostas marcas de roupa ou calçado, lojas fraudulentas *online*, supostas páginas de organismos públicos que fornecem serviços públicos, como certidões, certificados, cartas de condução, entre muitas outras. O mesmo sucede quando vítimas de crimes *online* reportam que o agente do crime continua a contactá-las, o que impõe a necessidade (mas também constitui uma oportunidade) de ação urgente.

Tendo em conta a natureza, a fragilidade e a volatilidade da prova (digital) em causa, em muitas destas situações espera-se que o Ministério Público determine medidas imediatas, tais como o bloqueio de acesso a páginas ou a imediata recolha, *online*, de informação a elas respeitante. A não ser assim, quando o inquérito vier a ser despachado, com delegação de competência, para o órgão de polícia criminal, dias (se não semanas ou mesmo meses) mais tarde, toda a prova pode já ter desaparecido.

Por outro lado, os mais recentes indicadores claramente referem que na criminalidade *online* se tem registado uma enorme expansão de fenómenos criminais de "*massas*", isto é, de campanhas criminosas desenvolvidas por grupos de crime organizado, as quais se dirigem simultaneamente a inúmeras vítimas, na esperança de que algumas delas "*caiam*" no logro. São exemplos destas iniciativas criminosas as campanhas de burlas do tipo conhecido como "*olá mãe, olá pai*", ou de burlas relacionadas com o pagamento de falsas dívidas de eletricidade. O mesmo pode dizer-se das novas formas de defraudação (também dirigidas a inúmeras vítimas em simultâneo) a propósito de falsos trabalhos *online* ou as burlas praticadas por meio de falsos telefonemas de autoridades policiais. Sucede o mesmo com métodos criminosos já há muito identificados, cuja expansão persiste, como as burlas em arrendamento de imóveis, ou o *phishing*.

De entre as denúncias recebidas pelo Gabinete Cibercrime em 2023, considerando apenas as referentes aos métodos criminosos conhecidos como "*olá mãe, olá pai*" e reclamação de falsas dívidas de energia elétrica, verifica-se que as mesmas correspondem a cerca de 30% do total. Muitas delas têm origem no mesmo grupo criminoso, embora se dirijam a uma multiplicidade de vítimas.

O modelo de gestão processual tradicional aponta sempre para a abertura de um inquérito perante cada denúncia recebida. Este modelo não tem conseguido lidar com estes fenómenos: ao ser aberta uma investigação por

cada denúncia, multiplica-se enormemente o número dos casos denunciados, dispersos (tal como as vítimas) pelo território nacional – é naturalmente a dispersão das vítimas que origina uma total dispersão do local onde são apresentadas as queixas.

Este fenómeno criminal não corresponde a criminalidade isolada, nem pontual, como aquela que tradicionalmente se investiga nos tribunais. Pode dizer-se que, neste contexto, *cada caso, não é um caso*: pelo contrário, cada caso é apenas o afloramento de uma prática criminosa muito mais alargada que atinge em simultâneo, além da vítima que o denuncia, múltiplas outras. Sem considerar esta vertente, não consegue aperceber-se corretamente o caso concreto nem o contexto geral do fenómeno, nem responder adequadamente a este fenómeno.

Por isso, tendo em vista a eficácia do Ministério Público, sobretudo num contexto de escassez de recursos, este tipo de manifestações criminógenas, cada vez mais frequentes (e também cada vez mais predominantes neste setor de criminalidade) exigem uma abordagem de natureza diferente: ao invés da abertura de investigações atomizadas, consoante as vítimas vão apresentando as queixas, exige-se antes uma abordagem coordenada e conjugada do fenómeno, que potencie a agregação de investigações (que pode ocorrer por via da aplicação do instituto da conexão processual, nos termos do Código de Processo Penal) ou a coordenação e conjugação de diligências processuais, entre diferentes processos, de diferentes comarcas ou departamentos.

Enfrentar eficazmente esta criminalidade requere pois uma alteração de perspetiva na abordagem da gestão dos processos e das investigações.

Espera-se que este tipo de crimes continue a aumentar no futuro próximo. Do mesmo modo, continuará correspondentemente a aumentar a necessidade de intervenção rápida do Ministério Público na recolha de elementos de prova dos mesmos. A prova de crimes ocorridos *online* é, por natureza, extremamente volátil: em muitos casos, os elementos de prova necessários a comprovar a existência de um crime não estarão já, seguramente, disponíveis mais tarde. Por isso, em muitos desses casos, sem uma intervenção rápida (imediata), a investigação será pura e simplesmente inviável.

Portanto, desenrolar todos os trâmites processuais de modo formalizado, como tradicionalmente se faz, quanto a processos em que a prova está já junta à denúncia ou depende apenas de inquirição testemunhal, por exemplo, levará a que todas estas investigações, além de provocarem cada vez mais pressão no sistema, pelo aumento do seu número, não venham a conduzir a resultados positivos.

Importa assim ajustar a estes fenómenos o atual modelo de recebimento e tramitação das denúncias nos departamentos do Ministério Público, para evitar que em muitos casos não seja depois impossível recolher prova da prática dos factos, sendo os processos arquivados, não sendo os culpados punidos nem as vítimas ressarcidas, gerando-se sentimento de impunidade nos agentes do crime e de desconfiança e incerteza nos cidadãos.

2. CONSOLIDAÇÃO DA ESPECIALIZAÇÃO

A Diretiva 1/2019 da Procuradora-Geral da República sugere claramente a necessidade de especialização na área da cibercriminalidade. No seu ponto 6, determina que "os 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". Depois, aponta critérios materiais de especialização.

Em geral, a especialização no Ministério Público é imposta pela necessidade de responder com mais eficácia às exigências de uma sociedade cada vez mais complexa e multifacetada. A dinâmica social tem sofrido o impacto de uma evolução tecnológica vertiginosa, substancialmente empurrada pela situação pandémica que se viveu a partir do início de 2020. Esta verdadeira revolução tecnológica teve claríssimos impactos sociológicos, provocando mudanças nas rotinas e nas relações humanas: teletrabalho, digitalização das diversas atividades económicas e do Estado, expansão de fenómenos como o comércio eletrónico ou a intensificação das atividades profissionais e de formação por videoconferência, são disso exemplos.

A execução prática da Diretiva 1/2009 da Procuradora-Geral da República revestiu modalidades variadas nas diversas comarcas do país. Por isso, a direção da investigação em inquéritos em que esteja em causa criminalidade em ambiente digital não tem sido distribuída pelos magistrados de acordo com critérios uniformes. Alguns dos exemplos de distribuição especializada têm sido avaliados 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; por outro, porque permitem concentrar a investigação deste tipo de processos em magistrados com maior vocação e apetência técnica para os mesmos. Além de outras, a especialização tem tido a vantagem de rentabilizar o investimento na capacitação e no reforço da competências e capacidades técnicas para lidar com este tipo de criminalidade.

Importa pois rearrumar a Rede Cibercrime, na sua vertente de conjunto de magistrados distribuídos pelas estruturas locais do Ministério Público, em todo o território nacional, a quem compete a concreta investigação da

criminalidade nesta área. Esta consolidação da Rede Cibercrime permitirá que a investigação deste tipo de crimes seja efetivamente realizada por magistrados apetrechados com conhecimentos específicos na área do cibercrime e da obtenção de prova em formato digital.

Além da eficácia funcional, este reforço do modelo de especialização garantirá uma aplicação mais consistente do direito, assegurando um maior respeito pelo princípio da unidade de ação do Ministério Público, e uma maior prossecução dos princípios de justiça material e de igualdade dos cidadãos perante a lei.

Por outro lado, a consolidação da especialização, com inerente concentração de processos desta natureza num número mais reduzido de magistrados, trará vantagens práticas processuais. Por exemplo, facilitará a identificação de fenómenos criminais que requeiram coordenação nacional nas respetivas investigações.

De acordo com o modelo já traçado pela Diretiva 1/2019, o critério substantivo da distribuição especializada deve incidir sobre uma boa parte, mas não todos os crimes ocorridos online.

O meio tecnológico ou digital tem sido o elemento diferenciador de alguma da criminalidade moderna. Aos cibercrimes propriamente ditos (os previstos na Lei Cibercrime) associam-se muitos outros crimes, de natureza diversa, que têm de comum entre eles serem praticados com auxílio das tecnologias, ou por via das tecnologias. A eles se aplicam os mesmos métodos e modelos de investigação do cibercrime. Também quanto a eles (da mesma forma que 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 informático.

As razões que se enumeraram aplicam-se também, além de a processos em que se investiguem crimes previstos na Lei do Cibercrime, a investigações respeitantes a crimes de burla informática, previstos no Artigo 221º do Código Penal. Por outro lado, a recente sofisticação das formas de defraudação online tem vindo a recomendar também que se incluam na especialização as investigações de clássicas burlas, quando ocorridas online, ou recorrendo às tecnologias de informação e comunicação, se este último elemento for decisivo na prática do crime.

Já não será de estender a especialização a investigações de crimes relacionados com pornografia infantil online, por as mesmas terem

características específicas, diferenciadas, a requerer outro tipo de competências.

O mesmo sucede com investigações respeitantes a crimes ditos tradicionais, apenas diferentes porque na sua prática são utilizados meios tecnológicos. Será por exemplo o caso de difamações, ameaças online, ou a violação de privacidade cometida online, já que a respetiva investigação, em geral mais simples, não tem a complexidade dos restantes nem supõem, pela sua própria natureza, sofisticação técnica e, consequentemente, não exige de quem investiga os mesmos elevados conhecimentos técnicos. É suposto que a generalidade dos magistrados do Ministério Público atinja, pelo menos, o nível médio de conhecimento de um habitual utilizador das tecnologias.

3. APOIO ÀS VÍTIMAS

O conjunto das muitas denúncias recebidas por correio eletrónico pelo Gabinete Cibercrime inclui muitas mensagens de cidadãos que, tendo sido vítimas de crimes online, não expressam vontade de que se dê início a uma investigação criminal. Em muitos casos, o denunciante apenas solicita ajuda para superar a situação em que se viu envolvido, saindo assim este tipo de casos (mero apoio à vítima, sem abertura de processo-crime) da esfera de intervenção principal do Ministério Público.

Sem prejuízo de se manter o encaminhamento de denúncias para investigação criminal, quando assim se justificar, como tem vindo a ser feito, importa também considerar os casos em que a vítima, não desejando procedimento criminal, ou carecendo de mais iniciativa que aquele que o mero procedimento criminal vai espoletar, pode ser encaminhada para outras entidades, mais vocacionadas para tal apoio.

Importa, pois, explorar mecanismos de cooperação com entidades terceiras, especializadas no apoio às vítimas de crimes e mais vocacionadas que o Ministério Público para esta valência.

4. REFORÇO DA CAPACIDADE INSTITUCIONAL

a. Ponto 24/7 para a cooperação internacional

A Convenção de Budapeste sobre Cibercrime, ratificada por Portugal[1], impôs ao país (artigo 35º) a criação de um "*ponto de contacto que deverá estar disponível vinte e quatro horas por dia, sete dias por semana, a fim de assegurar de imediato a prestação de auxílio nas investigações e nos procedimentos relativos a infrações penais relacionadas com sistemas informáticos, ou na recolha de provas sob a forma eletrónica, da prática de infrações penais*".

Cumprindo esta obrigação internacional, a Lei do Cibercrime[2] consagrou (artigo 21º), que "*a Polícia Judiciária assegura a manutenção de uma estrutura que garante um ponto de contacto disponível em permanência, vinte e quatro horas por dia, sete dias por semana*", para "*fins de cooperação internacional, tendo em vista a prestação de assistência imediata*".

Por sua vez, a Diretiva 2013/40/UE[3] do Parlamento Europeu e do Conselho, de 12 de agosto de 2013, relativa a ataques contra os sistemas de informação (artigo 13º), impõe aos Estados Membros da União Europeia que assegurem a "*existência de um ponto de contacto operacional nacional e recorrer à rede existente de pontos de contacto operacionais disponível 24 horas por dia e sete dias por semana*". Embora seja claro que este ponto de contacto é o já resultante da Convenção de Budapeste, a mesma Diretiva determina ainda que os "*Estados Membros devem também assegurar a existência de procedimentos que, em caso de pedidos de assistência urgentes, lhes permitam indicar, no prazo máximo de oito horas a contar da receção do pedido, se o pedido de ajuda será deferido, e a forma e o prazo estimado de resposta*".

Este último aspeto requere, dos Estados, que o ponto de contacto disponha de acesso a uma autoridade com funções de direção da investigação criminal (e não apenas de execução técnica dessa investigação). É que se supõe que o ponto de contacto possa indicar num prazo muito expedito se o pedido de cooperação será ou não cumprido, de que forma e em que prazo.

---

[1] https://files.dre.pt/1s/2009/09/17900/0635406378.pdf.
[2] https://files.dre.pt/1s/2009/09/17900/0631906325.pdf.
[3] https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32013L0040&from=DE.

A Diretiva 2019/713/UE[4], do Parlamento Europeu e do Conselho, de 17 de abril de 2019, relativa ao combate à fraude e à contrafação de meios de pagamento que não em numerário inclui (artigo 14º) uma norma exatamente do mesmo teor.

Em cumprimento desta obrigação, a Lei do Cibercrime foi alterada, pela Lei nº 79/2021[5], de 24 de novembro, que introduziu um novo nº 5 no artigo 21º, o qual dispõe que "*o Ministério Público deve, de modo a responder prontamente a pedidos de assistência imediata, assegurar a disponibilidade de magistrados e meios técnicos para levar a cabo quaisquer intervenções processuais urgentes da sua competência*".

Não se afigura que esta novidade legal altere a alocação do ponto de contacto 24/7, para efeitos internacionais, na Polícia Judiciária. A respetiva regulamentação mantém-se intocada. O que parece resultar deste novo nº 5 é que, do lado do Ministério Público, terá que ser criada a disponibilidade de meios para responder a solicitações que, por serem da sua competência legal, lhe sejam feitas pelo já existente ponto 24/7.

b. Cooperação internacional e troca de experiências e boas práticas

O Ministério Público está representado na *European Judicial Cybercrime Network*, a rede europeia de procuradores especializados em cibercrime, baseada na Eurojust, fazendo parte do respetivo *Board* executivo.

Por outro lado, foi acometida à Procuradoria-Geral da República de Portugal a tarefa de coordenar a *CiberRed*, a rede de Ministérios Públicos Ibero-Americanos especializados em cibercrime.

O Ministério Público de Portugal coordena também o *Fórum Lusófono sobre Cibercrime e Prova Digital*, do qual fazem parte todos os Ministérios Públicos da CPLP.

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

[4] https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32019L0713.
[5] https://files.dre.pt/1s/2021/11/22800/0000900038.pdf.

concretas. Mas resulta também que é essencial o intercâmbio de experiências e boas práticas entre as autoridades judiciárias dos vários países.

É determinante tirar o melhor partido das vantagens de todos os canais e instrumentos disponíveis de ajuda judiciária mútua. Importa intensificar o diálogo internacional neste contexto, participando ativamente na dinamização e operacionalização destes vários grupos. Por essa via será possível melhorar a cooperação na obtenção de provas noutros países, quando a mesma for requerida, em investigações concretas.

c. Coordenação com outras entidades

Pela sua própria natureza, as violações deliberadas de regras de cibersegurança constituem normalmente também violação de regras de natureza criminal. Mais do que noutras áreas, em que a segurança e o judiciário se cruzam, os fenómenos de cibercrime supõe uma intervenção multi-institucional, de diferentes entidades e autoridades do Estado.

O rápido conhecimento da notícia do crime e a realização de diligências urgentes de obtenção de prova são condições de eficácia e sucesso na investigação de crimes no ambiente digital. Este objetivo exige o desenvolvimento da articulação e cooperação com outras entidades, para além dos órgãos de polícia criminal responsáveis pela investigação criminal. É designadamente o caso de outros atores e entidades com funções e responsabilidades na área da cibersegurança.

Quanto aos órgãos de polícia criminal, auxiliares imprescindíveis do Ministério Público na investigação criminal, a procura de eficácia requere que com os mesmos se discutam linhas de evolução e iniciativas futuras neste domínio, sobretudo no que respeita à obtenção de prova eletrónica. Esta discussão deve também abranger boas práticas, que podem por exemplo passar pelo desenvolvimento conjunto de modelos ou formulários de apreensão de elementos de prova.

d. Atualização formativa prática

Desde a sua criação, o Gabinete Cibercrime tem tido, como um dos seus propósitos principais, o da formação específica de magistrados do Ministério Público na área do cibercrime e da obtenção de prova eletrónica.

Não faz parte dos objetivos do Gabinete desenvolver atividades formativas de conteúdo generalista, as quais são estatutariamente uma atribuição do Centro de Estudos Judiciários. Pelo contrário, o Gabinete Cibercrime privilegia atividades dirigidas a pequenos grupos, cuja dinâmica permite a troca direta de impressões e abordagem do caso concreto. Mais do que genéricas ações de formação, tais iniciativas são sessões de trabalho e de coordenação sobre aspetos concretos da investigação criminal, realizadas diretamente nas comarcas e dirigidas aos magistrados do Ministério Público aí colocados.

Com tais sessões formativas pretende facultar-se aos magistrados do Ministério Público com funções de investigação criminal melhor preparação para dirigir a investigação em casos da área do cibercrime ou que, em geral, suponham a obtenção de prova digital.

Este tipo de iniciativa chegou já a cerca de 700 magistrados do Ministério Público. Tais sessões, sempre presenciais, tiveram no passado, grande acolhimento dos magistrados das comarcas, pela proximidade e por facilitarem a discussão de casos concretos.

Em muitas das situações, os participantes expressaram a necessidade de que tais sessões se repitam com regularidade, de forma a manter atualização, numa área de evolução tão constante e tão rápida: surgem diariamente novos métodos criminosos, que exigem novas formas de abordagem e de investigação.

Por outro lado, a regular movimentação de magistrados e a constante evolução técnica tornam necessária a repetição periódica destas sessões formativas. Esta necessidade é mais vincada nas comarcas do interior do país, onde estão colocados muitos magistrados mais jovens, frequentemente em locais mais isolados, privados do contacto direto e imediato com colegas mais velhos, e que nunca tiveram oportunidade de participar em iniciativas do Gabinete Cibercrime.

Igualmente muito bem acolhidas, foram as experiências formativas à distância, por videoconferência. Empurradas pelo contexto pandémico, tais sessões vieram a revelar-se confortáveis e fáceis de operacionalizar, tendo a potencialidade de atingir um grande número de destinatários com custos inexpressivos. Revelaram-se sobretudo muito úteis para abordar novidades legislativas ou controvérsias jurisprudenciais, pouco depois de as mesmas se suscitarem.

Embora não se mostrem capazes de substituir os eventos presenciais, nas comarcas, o balanço das sessões realizadas recomenda que se dê continuidade ao modelo experimentado.