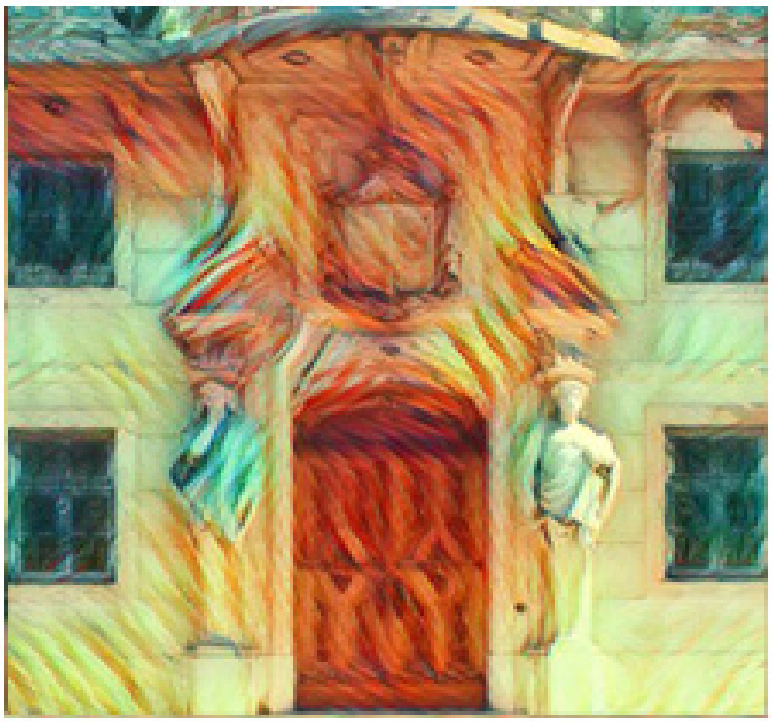
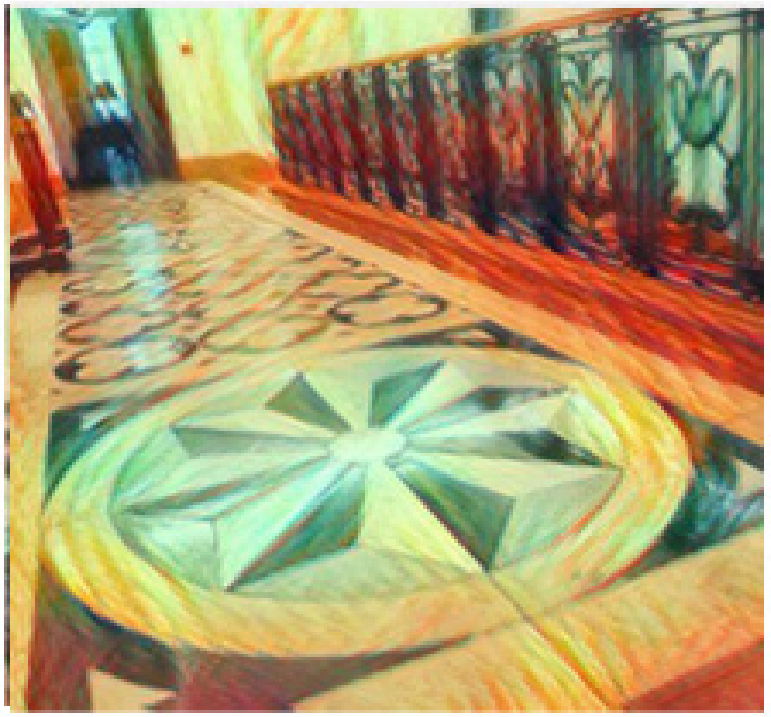




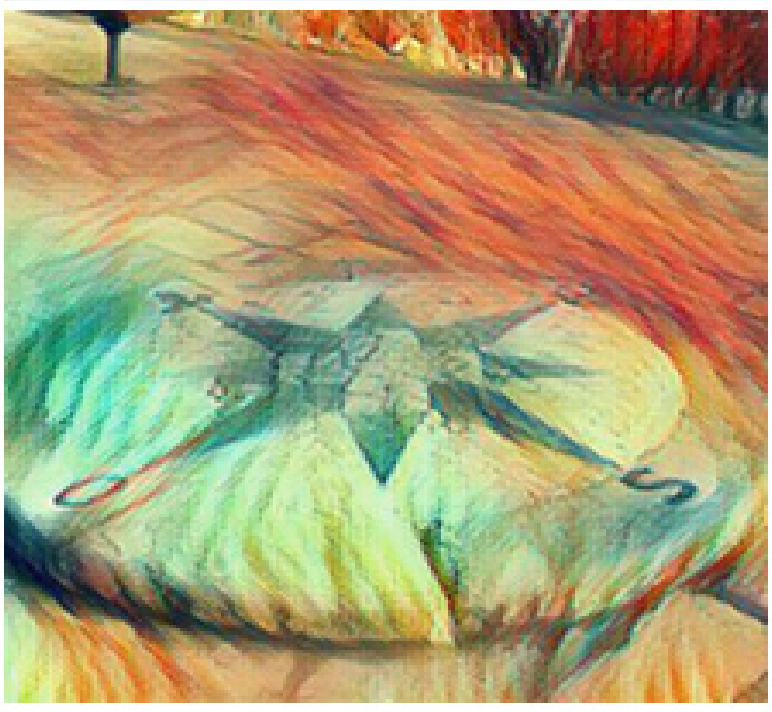
COLEÇÃO FORMAÇÃO — MINISTÉRIO PÚBLICO

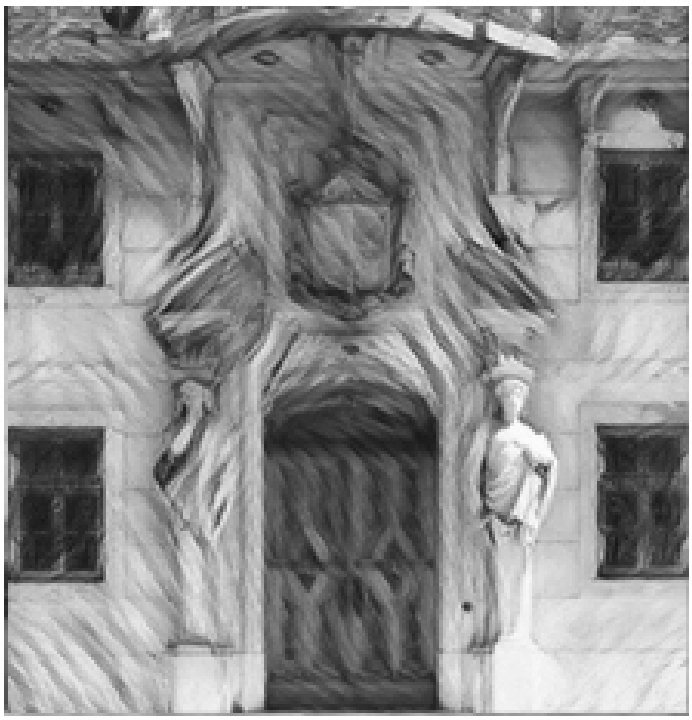
MEIOS DE OBTENÇÃO DE PROVA E MEDIDAS CAUTELARES E DE POLÍCIA

TRABALHOS DO 2.º CICLO DO 32.º CURSO

ABRIL 2019

CENTRO DE ESTUDOS JUDICIÁRIOS





Diretor do CEJ: João Manuel da Silva Miguel, *Juiz Conselheiro*

Diretores Adjuntos:
Paulo Alexandre Pereira Guerra, *Juiz Desembargador*
Luís Manuel Cunha Silva Pereira, *Procurador-Geral Adjunto*

Coordenador do Departamento de Formação:
Edgar Taborda Lopes, *Juiz Desembargador*

Coordenadora do Departamento de Relações Internacionais:
Helena Leitão, *Procuradora da República*

Grafismo: Ana Caçapo, *CEJ*

Fotos da capa: Edifício da Procuradoria Geral da República,Rosa dos ventos na PGR, Rosa dos ventos e pormenor da fachada do CEJ.

Apresentação

Dando continuidade à publicação da série de *e-books* da colecção Formação – Ministério Público "Trabalhos Temáticos de Direito e Processo Penal", o Centro de Estudos Judiciários tem o grato prazer de proceder à divulgação dos volumes que compreendem os trabalhos temáticos realizados pelos auditores de justiça do 2.º ciclo, do 32.º Curso de Formação.

Como introdução a estes volumes remete-se, em grande medida, para as considerações efectuadas no momento da publicação dos seus antecessores.

Sem embargo, não será de mais salientar que as fases designadas por 2.º Ciclo e Estágio, que se desenrolam num contexto puramente judiciário e que correspondem a dois terços de toda a formação inicial organizada pelo Centro de Estudos Judiciários, constituem um tempo e um lugar onde se visa a qualificação de competências e práticas e o conferir de uma coerente sequência ao quadro de objectivos pedagógicos e avaliativos definidos como estruturantes para a preparação dos futuros magistrados do Ministério Público.

Neste contexto, a par da formação pessoal (*o saber e o saber-ser*) é fundamental continuar a desenvolver nessas fases formativas a dimensão institucional, traduzida na aquisição e aperfeiçoamento de competências, cultura, ética e deontologia judiciárias (o *saber-fazer* e o *saber-estar*).

Os *e-books* que agora se publicam recolhem o conjunto dos trabalhos elaborados pelos auditores de justiça do Ministério Público em formação no 2.º ciclo para a denominada *semana temática*, enquanto componentes de um modelo de avaliação que pretendeu privilegiar fins formativos.

A centralização da actividade onde foram publicamente apresentados, a dinamização que nela imprimiram os seus promotores, e o bom acolhimento que a iniciativa teve por parte dos formandos, permitiu confirmar o seu significado e impacto efectivo na execução de uma estratégia pedagógica coerente.

A apresentação dos trabalhos temáticos serviu de teste à validação das competências práticas que foram sendo adquiridas na comarca junto dos formadores, ao mesmo tempo que se avaliaram competências de adequação e de aproveitamento quanto a todos os auditores, uma vez que a aludida apresentação ocorreu na mesma oportunidade, perante os mesmos avaliadores e perante os pares, que assim também beneficiaram de efectiva formação.

Tratou-se, pois, de uma excelente oportunidade para apreciar competências relativas a todos os parâmetros avaliativos, tanto no que se refere ao estrito aproveitamento como, também, à adequação.

Pelo trabalho escrito foi possível avaliar, entre outros, o conhecimento das fontes, a destreza do recurso às tecnologias de informação e comunicação, a eficácia da gestão da informação, a gestão do tempo, o domínio dos conceitos gerais, o nível de conhecimentos técnico-jurídicos, a capacidade de argumentação escrita e oral, a capacidade de síntese ou o nível de abertura às soluções plausíveis. Por seu turno, a apresentação oral permitiu fazer um juízo sobre aspectos da oralidade e do saber-estar, sociabilidade e adaptabilidade (trabalho de equipa), permitindo igualmente a apreciação da destreza de cada auditor no que respeita à capacidade de investigação, à capacidade de organização e método, à cultura jurídica, à capacidade de ponderação e, sobretudo, à atitude na formação, que tem de ser (ainda que difícil e exigente) uma atitude de autonomia e responsabilidade.

A tónica na preparação e supervisão dos trabalhos pelos coordenadores regionais assentou sobretudo nos aspectos da prática e da gestão do inquérito ou da gestão processual, que são tão mais importantes quanto impõem aos auditores uma transição entre a teoria e a prática, evitando-se trabalhos com intuito e conteúdo exclusivamente académico.

É inegável que alguns temas têm dificuldades associadas, mesmo na circunscrição de um objecto passível de tratar em espaço e tempo limitados. Essa foi também uma oportunidade de testar a capacidade de gestão da informação e mesmo da destreza na identificação e formulação das questões essenciais, o nível de abertura às soluções plausíveis, a autonomia e personalização e o sentido prático e objectividade. A opção do

auditor, face ao tempo e espaço limitados de que dispõe, envolverá sempre riscos e a circunscrição do objecto do trabalho revelará a inteligência, o sentido prático, o grau de empenhamento individual e respectivo nível de iniciativa, de capacidade de indagação e de capacidade de gestão da informação.

Estes trabalhos não pretendem que, através deles, o futuro magistrado cultive a polémica, a retórica ou o academismo do direito sem experiência e sem aplicação. Trata-se de uma oportunidade para teorizar a prática, em consonância com a fase de formação de 2.º ciclo, fazendo com que a *praxis* se abra à pluralidade de contextos sociais, económicos, comunicacionais, político-legislativos, em atenção concomitante aos sentimentos e opiniões sociais que fazem apelo às ideias de Justiça, reclamando dos princípios e normas a capacidade de se adaptarem a esses contextos e às suas mutações.

Uma breve nota final descritiva da forma como se operacionalizou a elaboração destes trabalhos:

Na sequência de prévias reuniões dos coordenadores com o Director Adjunto, foram seleccionadas as temáticas que viriam a constituir o objecto dos trabalhos escritos.

Seguidamente foram difundidas aos auditores as seguintes orientações:

a) Um tema para cada grupo de 4 auditores de justiça (sem possibilidade de repetição).
b) Cada trabalho temático escrito seria individual, sujeito a avaliação.
c) A escolha do tema e a constituição de cada grupo de auditores por tema decorreu de forma consensual entre os auditores de justiça.
d) Foi fixada uma data limite para o envio do trabalho escrito e do suporte da respectiva apresentação aos coordenadores regionais.
e) O trabalho escrito teve o limite de 30 páginas A4.
f) A apresentação oral teve lugar no Centro de Estudos Judiciários, em Lisboa, em Junho de 2018.
g) Nas apresentações orais foram utilizados meios de apoio, designadamente, o recurso a *data-show* (suporte «*powerpoint*» ou «*Prezi*»).

h) Os auditores de justiça que trabalharam o mesmo tema, sempre na prossecução do conceito de trabalho em equipa, foram encarregados de se articularem entre si, empreendendo as diligências necessárias por forma a investirem, na oportunidade devida, numa apresentação oral que resultasse coordenada, lógica e sequencial, sem repetição de conteúdos e portanto operada num contexto de partilha de saber e de estudo e com observância do limite temporal fixado.

i) A comparência foi obrigatória para todos os auditores de justiça (incluindo nos dias que não estiveram reservados à respectiva intervenção).

Luís Manuel Cunha da Silva Pereira
Director-Adjunto do Centro de Estudos Judiciários
Jorge Manuel Vaz Monteiro Dias Duarte
Coordenador Regional Norte – Ministério Público
Ângela Maria B. M. da Mata Pinto Bronze
Coordenadora Regional Centro – Ministério Público
José Paulo Ribeiro de Albuquerque
Coordenador Regional Lisboa – Ministério Público
Olga Maria Caleira Coelho
Coordenadora Regional Sul – Ministério Público

Ficha Técnica

Nome:

Meios de obtenção de prova e medidas cautelares e de polícia

Coleção:

Formação Ministério Público

Conceção e organização:

Luís Manuel Cunha da Silva Pereira (Director-Adjunto do Centro de Estudos Judiciários)
Jorge Manuel Vaz Monteiro Dias Duarte (Coordenador Regional Norte – Ministério Público)
Ângela Maria B. M. da Mata Pinto Bronze (Coordenadora Regional Centro – Ministério Público
José Paulo Ribeiro de Albuquerque (Coordenador Regional Lisboa – Ministério Público)
Olga Maria Caleira Coelho (Coordenadora Regional Sul – Ministério Público)

Intervenientes:

Flávio Manuel Carneiro da Silva*
Henrique Gustavo Ribeiro Ferreira de Antas e Castro*
Marta Saúde*
Raul Estêvão Ramos Trancoso*
Rui Miguel dos Santos Real*
Sílvia Catarina Pais Silva*
Telmo Oliveira*
Vera Lúcia Quadros de Oliveira e Santos*

Revisão final:

Edgar Taborda Lopes – Juiz Desembargador, Coordenador do Departamento da Formação do CEJ
Ana Caçapo – Departamento da Formação do CEJ
Lucília do Carmo – Departamento da Formação do CEJ

* Auditores/as de Justiça do 32.º Curso de Formação de Magistrados – MP à data da apresentação dos trabalhos.

Notas:

Para a visualização correta dos e-books recomenda-se o seu descarregamento e a utilização do programa Adobe Acrobat Reader.

Foi respeitada a opção dos autores na utilização ou não do novo Acordo Ortográfico.

Os conteúdos e textos constantes desta obra, bem como as opiniões pessoais aqui expressas, são da exclusiva responsabilidade dos/as seus/suas Autores/as não vinculando nem necessariamente correspondendo à posição do Centro de Estudos Judiciários relativamente às temáticas abordadas.

A reprodução total ou parcial dos seus conteúdos e textos está autorizada sempre que seja devidamente citada a respetiva origem.

Forma de citação de um livro eletrónico (NP405-4):

AUTOR(ES) – **Título** [Em linha]. a ed. Edição. Local de edição: Editor, ano de edição.
[Consult. Data de consulta]. Disponível na internet: <URL:>. ISBN.

Exemplo:
Direito Bancário [Em linha]. Lisboa: Centro de Estudos Judiciários, 2015.
[Consult. 12 mar. 2015].
Disponível na
internet: <URL: http://www.cej.mj.pt/cej/recursos/ebooks/civil/Direito_Bancario.pdf.
ISBN 978-972-9122-98-9.

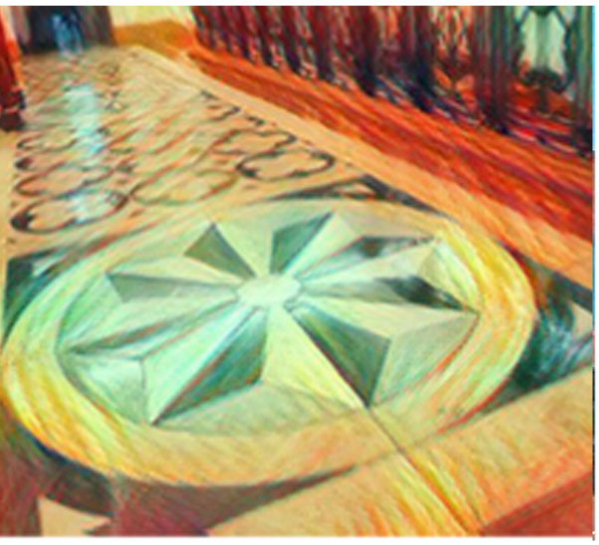
Registo das revisões efetuadas ao e-book

Identificação da versão	Data de atualização
1.ª edição –04/04/2019	

Meios de obtenção de prova e medidas cautelares e de polícia

Índice

CENTRO
DE ESTUDOS
JUDICIÁRIOS



1.

Apreensão e utilização processual de meios de prova existentes em material informático

Flávio Manuel
Carneiro da Silva

CENTRO
DE ESTUDOS
JUDICIÁRIOS

1. APREENSÃO E UTILIZAÇÃO PROCESSUAL DE MEIOS DE PROVA EXISTENTES EM MATERIAL INFORMÁTICO

Flávio Manuel Carneiro da Silva

I. Introdução

A dependência social aos meios tecnológicos e a proliferação da criminalidade cometida por meio informático são fenómenos incontornáveis da Sociedade de Informação.

A investigação e a efectiva repressão dos crimes informáticos, *maxime* crimes praticados através da informática, constitui hoje um desafio para o Estado, pela forma dissimulada e potencialmente oculta que os encerra, designadamente quanto à sua autoria, mas também pela capacitada propagação nociva inerente à interligação em rede dos sistemas informáticos.

Por outro lado, é inegável o contributo da prova armazenada em suporte informático na investigação de qualquer crime, num momento histórico em que a localização, as preferências, o círculo de amizades, as conversações, os elementos de trabalho, as fotografias, os vídeos, são dados recolhidos e armazenados pelos sistemas informáticos.

No plano judiciário atravessa-se, ainda, um período de grande indefinição quanto à margem de actuação constitucionalmente e legalmente permitida à investigação e prossecução da acção penal em confronto com o respeito pelos direitos fundamentais dos cidadãos.

Dificuldade potenciada pelos inúmeros obstáculos na interpretação e aplicação do direito constituído relativo à prova digital em processo penal, fruto de uma desconcertante insistência do legislador em manter inalterado o quadro normativo-regulador da matéria, não só sistematicamente disperso em vários diplomas como também de conteúdo aparentemente conflituante.

Em todo o caso, assiste-se com agrado ao paulatino abandono da intuitiva necessidade de integração dos fenómenos da criminalidade informática e da recolha de prova digital aos institutos jurídicos clássicos, por parte dos pensadores e aplicadores do Direito.

II. Objectivos

Pretende-se analisar criticamente o regime de obtenção e utilização processual de prova digital regulado pela Lei n.º 109/2009, de 15 de Setembro (Lei do Cibercrime), introduzindo uma nova visão conjugada das concretas medidas processuais legalmente previstas, por forma a aproximar os entendimentos doutrinais e procedimentais à realidade técnico-empírica da prova digital.

Com especial incidência na desmistificação da oportunidade de invocação e utilização do regime da apreensão de dados informáticos (artigo 16.º e 17.º da Lei do Cibercrime), tentar-se-á definir em que situações e em que moldes deve ser dado cumprimento às regras processuais aí previstas, designadamente, saber-se qual o papel do Ministério Público e do Juiz de Instrução na autorização e validação da apreensão da correspondência electrónico-informática.

1. Conceptualização

1.1. Introdução

A correcta construção e interpretação dogmática de uma realidade regulada pelo Direito não dispensa um esforço de conceptualização das suas diversas manifestações empírico-naturalísticas e jurídico-normativas.

A evolução tecnológica e a complexidade tecnocientífica da computação e da informática não facilitam o necessário trabalho de conceptualização jurídica dos intérpretes do Direito, cujos conhecimentos na área estão limitados, não raras vezes, à óptica do utilizador dos sistemas informáticos e tecnológicos disponíveis.

Este contexto tem potenciado a utilização e densificação de múltiplos conceitos operativos que espelham uma mesma realidade e, por outro lado, a utilização sinónima de conceitos que espelham realidades diferentes. Por essa razão, importa antes de mais, esclarecer o sentido e a abrangência dos conceitos mais utilizados nestes escritos, por forma a permitir uma melhor compreensão do seu conteúdo.

1.2. Criminalidade Informática

O conceito de **criminalidade informática** abarca duas diferentes realidades criminológicas, quais sejam **os crimes praticados contra os sistemas informáticos**, actualmente previstos e punidos no nosso sistema jurídico no Capítulo II da Lei n.º 109/2009, de 15 de Setembro (Lei do Cibercrime) – falsidade informática (artigo 3.º), dano relativo a programas ou outros dados informáticos (artigo 4.º), sabotagem informática (artigo 5.º), acesso ilegítimo (artigo 6.º), intercepção ilegítima (artigo 7.º) e reprodução ilegítima de programa protegido (artigo 8.º) -, e **os crimes praticados por meio de um sistema informático**, aqui se englobando todo o crime perpetrado com o recurso aos meios tecnológicos – *e.g.*, a burla informática (artigo 221.º do CP), a pornografia de menores (artigo 176.º do CP), a devassa por meio de informática (artigo 193.º do CP), e em geral, os crimes de falsificação, os crimes contra a honra, entre muitos outros.

Do um ponto de vista processual-penal é inoperante qualquer categorização material do espectro de crimes englobados no conceito de criminalidade informática, adoptando-se um sentido amplo capaz de abranger *"toda a panóplia de actividade criminosa que pode ser levada a cabo por meios informáticos, ainda que estes não sejam mais que um instrumento para a sua prática, mas que não integra o seu tipo legal"* ([1]), já que para efeitos da obtenção da prova digital, o regime legal não distingue uns dos outros (artigo 11.º, alíneas a) e b), da Lei n.º 109/2009, de 15 de Setembro).

1.3. Prova Digital

A **prova digital** pode ser definida como a *"informação passível de ser extraída de um dispositivo electrónico (local, virtual ou remoto) ou de uma rede de comunicações"* ([2]) ([3]).

Assim definida, a prova digital abarca não apenas os dados informáticos ([4]), incluindo os dados de tráfego ([5]), como também outros meios de prova que historicamente antecedem aquele conceito, como as escutas telefónicas e a localização celular ([6]).

[1] VENÂNCIO, Pedro Dias, "Lei do Cibercrime Anotada e Comentada", 1.ª ed., Coimbra Editora, Coimbra, 2011, p. 16.
[2] RAMOS, Armando Dias, "A Prova Digital em Processo Penal", 1.ª ed., Chiado Editora, Lisboa, 2014, p. 86.
[3] BENJAMIM SILVA RODRIGUES define prova digital como *"qualquer tipo de informação, com valor probatório, armazenada em repositório electrónico-digital de armazenamento, ou transmitida em sistemas e redes informáticas ou redes de comunicações electrónicas, privadas ou publicamente acessíveis sob a forma binária ou digital"*, *in* RODRIGUES, Benjamim Silva, *"Direito Penal Parte Especial"*, Tomo I, Direito Penal Informático-Digital, Coimbra, 2009, p. 722.

Por essa razão, e como veremos mais detalhadamente, a obtenção de prova digital não obedece a um regime legal unitário, muito embora a informação extraível de dispositivos electrónicos e de redes de comunicação assuma características comuns, designadamente a sua **imaterialidade** para efeitos de recolha e utilização processuais.

A natureza imaterial da prova digital implica necessariamente uma corporização no processo que pode revestir diferentes formas – *e.g.* documental, reprodução mecânica -, sem que tal pressuponha a perda da sua identidade electrónico-informática. Assim, prova digital será toda a informação **extraída** de dispositivos electrónicos e/ou sistemas informáticos ([7]) independentemente da forma de corporização que poderá revestir no processo ([8]).

O endereço de IP (*Internet Protocol*) utilizado para estabelecer uma ligação à Internet através da qual se praticou um determinado crime é prova digital independentemente de no processo essa informação vir corporizada sob a forma documental.

2. Enquadramento normativo

2.1. Introdução

Ao contrário da experiência de outros países europeus ([9]) ([10]), o legislador nacional decidiu não integrar no Código de Processo Penal o regime jurídico regulador do Cibercrime, quer na sua dimensão substantiva quer na dimensão processual, tendo optado por descentralizar o quadro normativo-regulador da matéria, especialmente o regime processual da obtenção da prova digital, em vários diplomas legais.

---

[4] Definidos no artigo 2.º, alínea b) da Lei n.º 109/2009, de 15 de Setembro (Lei do Cibercrime) como *"qualquer representação de factos, informações ou conceitos sob uma forma susceptível de processamento num sistema informático, incluindo os programas aptos a fazerem um sistema informático executar uma função"*.

[5] Definidos no artigo 2.º, alínea c) da Lei n.º 109/2009, de 15 de Setembro, como *"os dados informáticos relacionados com uma comunicação efectuada por meio de um sistema informático, gerados por este sistema como elemento de uma cadeia de comunicação, indicando a origem da comunicação, o destino, o trajecto, a hora, a data, o tamanho, a duração ou o tipo do serviço subjacente"*.

[6] A intercepção de escutas telefónicas e a localização celular não serão temas aqui abordados.

[7] A definição de sistema informático vem plasmada no artigo 2.º, alínea a), da Lei n.º 109/2009, de 15 de Setembro: *"qualquer dispositivo ou conjunto de dispositivos interligados ou associados, em que um ou mais de entre eles desenvolve, em execução de um programa, o tratamento automatizado de dados informáticos, bem como a rede que suporta a comunicação entre eles e o conjunto de dados informáticos armazenados, tratados, recuperados ou transmitidos por aquele ou aqueles dispositivos, tendo em vista o seu funcionamento, utilização, protecção e manutenção"*.

[8] Muito embora possa ser colocada em causa a fidedignidade da prova digital, por eventual falta de meios de certificação (como a assinatura digital) – o que deverá ser tido em conta nas boas práticas dos órgãos de polícia criminal -, esse é um problema de apreciação e valoração da prova.

[9] Na Alemanha, o Código de Processo Penal regula os meios de obtenção de prova, incluindo-se a apreensão de correspondência virtual, intercepção de telecomunicações e buscas em computadores. Em Espanha, o regime de recolha da prova em ambiente digital (apreensão de correspondência, intercepção de comunicações, escutas telefónicas) vem regulado num único artigo da "Ley de Enjuiciamento Criminal".

[10] Aquando da Proposta de Lei n.º 289/X/4.ª (que serviu de base à Lei do Cibercrime), PAULO DÁ MESQUITA defendia já *"a integração das regras [penais materiais e processuais do cibercrime] no Código de Processo Penal"*, *in* "Processo Penal, Prova e Sistema Judiciário", Coimbra Editora, Coimbra, 2011, p. 101.

A obtenção da prova digital está actualmente regulada em três diplomas legais: o **Código de Processo Penal**, a **Lei n.º 32/2008**, de 17 de Julho (que regula a conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas) e, ainda, a **Lei n.º 109/2009**, de 15 de Setembro (Lei do Cibercrime). Esta opção não tem sido isenta de críticas na doutrina, dadas as assinaláveis incoerências das soluções legais previstas nos diferentes diplomas e as patentes dificuldades que o intérprete enfrenta na aplicação do direito constituído.

A este propósito JOÃO CONDE CORREIA escreve: *"persistindo numa estranha lógica legislativa, que tem resistido incólume ao irremediável volver dos tempos, o legislador nacional continua a manter em vigor três diplomas legais diferentes para regular aspectos parcelares da mesma realidade concreta. Esta trilogia, para além de acentuar o actual paradigma da descodificação e de negar a desejável centralidade normativa do Código de Processo Penal, contribui para a assimetria, para a incoerência das soluções legais e, sobretudo, para o seu indesejável e nefasto insucesso prático. A prova digital (…) continua mergulhada num verdadeiro pântano prático, e sobretudo, normativo, que só poderá ser superado mediante uma intervenção legislativa coerente, global e, cientificamente sustentável"* ([11]). Em sentido convergente, ALBERTO GIL CANCELA constata que *"o panorama legislativo actual revela incoerências, sendo de tal forma complexo, que nos podemos deparar com duas situações aquando do confronto normativo das leis existentes: ou estas se autonomizam ou convergem, superando-se sucessivamente, dificultando a função interpretativa. Ao seguir o caminho legislativo pluralista, o legislador anarquizou o sistema, não permitindo ao espírito e à letra da lei a melhor interpretação, complicando a sua aplicação legal"* ([12]).

Apesar das assinaláveis incongruências, cremos ser viável analisar e interpretar o regime de forma sistematicamente consistente, resistindo à tentação de, a par e passo, procurar nas soluções clássicas do processo penal a resposta aos problemas específicos do mundo digital, devendo sim encetar-se um esforço de harmonização e coerência no confronto entre a realidade técnico-empírica e o regime introduzido pela Lei n.º 109/2009, de 15 de Setembro (Lei do Cibercrime).

2.2. Fontes Internacionais

A natureza transfronteiriça do fenómeno da criminalidade informática justifica a abundante actividade legislativa aos níveis Internacional e Europeu que tem vindo a influenciar e padronizar os regimes jurídico-reguladores nacionais da matéria.

Destacam-se, pela sua influência na legislação portuguesa, a **Convenção sobre o Cibercrime do Conselho da Europa**, de 23 de Novembro de 2001, a **Decisão-Quadro nº 2005/222/JAI, do**

[11] CORREIA, João Conde, "Prova Digital: as leis que temos e a lei que devíamos ter", Revista do Ministério Público, 139, Julho : Setembro de 2014, pp. 29-30.
[12] CANCELA, Alberto Gil Lima, "A Prova Digital: Os meios de obtenção de prova na Lei do Cibercrime", Dissertação de Mestrado, Faculdade de Direito da Universidade de Coimbra, Coimbra, 2016, p. 25.

Conselho, de 24 de Fevereiro e a **Directiva nº 2006/24/CE**, do Parlamento e do Conselho, de 15 de Julho.

Considerada pelo legislador nacional, *"o primeiro e mais importante trabalho internacional de fundo sobre crime no ciberespaço"* ([13]), a **Convenção sobre o Cibercrime** procurou definir *"uma política criminal comum"* visando *"proteger a sociedade da criminalidade no ciberespaço, nomeadamente através da adopção de legislação adequada e da melhoria da cooperação internacional"* ([14]).

A Convenção contempla um conjunto de conceitos jurídico-informáticos - tais como "sistema informático", "dados informáticos", "fornecedor de serviços" e "dados relativos ao tráfego" -, um elenco de ilícitos criminais (definindo crimes contra a confidencialidade, integridade e disponibilidade dos sistemas de computadores, crimes referentes aos conteúdos e crimes cometidos por via da informática), um conjunto de medidas processuais destinadas a regular a forma de obtenção da prova digital e, ainda, mecanismos de promoção da cooperação internacional e regras de aplicação espacial dos ilícitos criminais aí previstos.

Portugal aderiu à Convenção sobre o Cibercrime em 2001, contudo só procedeu à sua ratificação em 2009, por Resolução da Assembleia da República nº 88/2009 e pelo Decreto do Presidente da República nº 92/2009, ambos publicados a 15 de Setembro.

A **Decisão-Quadro nº 2005/222/JAI**, do Conselho, de 24 de Fevereiro, relativa a ataques contra os sistemas de informação, veio *"reforçar a cooperação entre as autoridades judiciárias e outras autoridades competentes (…) mediante uma aproximação das suas disposições de direito penal em matéria dos ataques contra os sistemas de informação"* ([15]), acompanhando as linhas orientadoras da Convenção do Cibercrime e tornando-as vinculativas para os Estados-Membros da União Europeia.

A **Lei n.º 109/2009**, de 15 de Setembro (Lei do Cibercrime) é o resultado da transposição (tardia) para o ordenamento jurídico interno da **Convenção sobre o Cibercrime do Conselho da Europa**, de 23 de Novembro de 2001, e da **Decisão-Quadro nº 2005/222/JAI, do Conselho**, de 24 de Fevereiro.

A **Directiva nº 2006/24/CE**, do Parlamento e do Conselho, de 15 de Julho, regula a conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações.

Esta Directiva visou, em primeira linha, a harmonização legislativa dos Estados-Membros relativa às obrigações dos **fornecedores de serviços de comunicações electrónicas** publicamente disponíveis ou de uma rede pública de comunicações em matéria de conservação de determinados dados por eles gerados ou tratados, e teve como escopo garantir a disponibilidade desses dados para efeitos de investigação, de detecção e de

[13] Exposição dos Motivos da Proposta de Lei nº 289/X/4ª – Lei do Cibercrime.
[14] Parágrafo 4 do Preâmbulo da Convenção do Cibercrime do Conselho da Europa, de 23 de Novembro de 2001.
[15] Considerando (1) da Decisão-Quadro nº 2005/222/JAI do Conselho, de 24 de Fevereiro.

repressão de crimes graves, através da obrigatoriedade da sua conservação por períodos não inferiores a seis meses e não superiores a dois anos, a definir por cada Estado-Membro. A Directiva nº 2006/24/CE foi transposta para a ordem jurídica portuguesa através da **Lei nº 32/2008, de 17 de Julho** ([16]).

2.3. Lei n.º 109/2009, de 15 de Setembro

Com a entrada em vigor da Lei n.º 109/2009 (a 15-11-2009), o legislador transpôs para o direito interno a Convenção sobre o Cibercrime e a Decisão-Quadro n.º 2005/222/JAI, do Conselho, de 24/2, relativa a ataques contra sistemas de informação.

Esta transposição ocorreu oito anos depois da adesão à Convenção, em 2001, tendo o legislador incumprido com os prazos previstos para a implementação das medidas aí previstas (terminava a 23-01-2001) e para a transposição da Decisão-Quadro 2005/222/JAI (terminava em 16-3-2007).

A Lei do Cibercrime, como é apelidada, tem por objecto estabelecer *"as disposições penais materiais e processuais, bem como as disposições relativas à cooperação internacional em matéria penal, relativas ao domínio do cibercrime e da recolha de prova em suporte electrónico"* (artigo 1.º).

Além de aí se prever um conjunto de disposições relativas à cooperação internacional penal e um catálogo de crimes informáticos *strictu sensu* (crimes praticados contra os sistemas informáticos), a Lei do Cibercrime veio introduzir *"um verdadeiro sistema processual de prova digital"* ([17]), uma vez que as medidas processuais aí previstas são de **aplicação geral**, quer nos processos relativos a crimes expressamente previstos nesse diploma quer nos processos relativos a crimes cometidos por meio de um sistema informático, como ainda em relação aos quais seja necessário proceder à recolha de prova em suporte electrónico (artigo 11.º, n.º 2).

Como refere ALBERTO GIL CANCELA, *"a Lei nº 109/2009 passa a ter como foco central a matéria de prova"* ([18]), aí se prevendo a preservação expedita de dados (artigo 12.º), a revelação expedita de dados de tráfego (artigo 13.º), a injunção para a apresentação ou concessão de acesso a dados (artigo 14.º), a pesquisa de dados informáticos (artigo 15.º), a apreensão de dados informáticos (artigo 16.º), a apreensão de correio electrónico e de registos de comunicações de natureza semelhante (artigo 17.º), a intercepção de comunicações (artigo 18.º) e as acções encobertas (artigo 19.º) ([19]).

---

[16] A Directiva nº 2006/24/CE foi declarada inválida pelo Acórdão do Tribunal de Justiça da União Europeia, de 8 de Abril de 2014 (ECLI:EU:C:2014:238), por violação do princípio da proporcionalidade e da reserva da vida privada dos cidadãos. Considerou-se que a imposição às operadores de comunicações de conservação de dados de tráfego e de localização dos seus clientes, seja pelo período que for, representa uma intromissão desproporcionada e injustificável na vida privada dos cidadãos (em prol do combate contra a criminalidade grave).

[17] CORREIA, João Conde, *ob. cit.*, p. 35.

[18] CANCELA, Gil Alberto Lima, ob. cit., p. 30.

[19] Segundo PEDRO VENÂNCIO, *"a consagração de disposições processuais relativas à preservação, revelação, apresentação, pesquisa e apreensão de dados informáticos (previstas nos artigos 12.º a 17.º da LC) impunha-se não só como um imperativo de direito internacional, face à ratificação da Convenção sobre Cibercrime, mas, acima de tudo, como*

A entrada em vigor deste diploma veio revogar tacitamente o artigo 189.º, n.º 1, do Código de Processo Penal que impunha a aplicação das normas que regulam a intercepção e gravação de comunicações telefónicas (artigos 187.º e 188.º do Código de Processo Penal) às conversações ou comunicações transmitidas por qualquer meio técnico diferente do telefone, designadamente correio electrónico ou outras formas de transmissão de dados por via telemática, mesmo que se encontrem guardadas em suporte digital, e à intercepção das comunicações entre presentes ([20]).

2.4. Lei n.º 32/2008, de 17 de Julho

A Lei nº 32/2008, de 17 de Julho regula a conservação e transmissão dos dados de tráfego, localização e dados que permitam identificar o utilizador do serviço quando perante uma investigação, detecção ou repressão de crimes graves por parte das autoridades competentes (artigo n.º 3 n.º 1).

De acordo com o disposto nos artigos 3.º, n.ºs 1 e 3 e 9.º desta lei, a transmissão dos dados de tráfego e de localização por parte dos fornecedores de serviços de comunicação só será possível no âmbito processual penal, quando em causa estiver a prática dos crimes graves elencados no artigo 2.º, alínea g) desse diploma (crimes de terrorismo, sequestro, rapto e tomada de reféns, os crimes contra a segurança do Estado, falsificação de moeda ou título equiparado, e os crimes abrangidos por convenção sobre a segurança da navegação aérea ou marítima, bem como a criminalidade violenta ou altamente organizada, cuja definição se encontra nas alíneas j) e l) do artigo 1º do Código de Processo Penal) e mediante autorização judicial, por despacho fundamentado, sempre que a obtenção dos dados se revele indispensável para a descoberta da verdade.

Este regime previsto na Lei 32/2008 para a transmissão de dados de tráfego sobrepõe-se de forma incongruente com o regime previsto na Lei do Cibercrime para a Injunção para a apresentação ou concessão de dados informáticos específicos e determinados, armazenados num determinado sistema informático, por um Fornecedor de Serviços.

Parece estar a consolidar-se na jurisprudência o entendimento, aqui perfilhado, que a Lei do Cibercrime veio revogar tacitamente e substituir o regime processual previsto na Lei 32/2008, pelo menos na parte em que regula a transmissão de dados de tráfego (artigos 3.º, n.ºs 1 e 3 e 9.º), por aquela se tratar de uma lei posterior e especialmente vocacionada à regulação das medidas processuais de obtenção da prova digital ([21]) ([22]).

---

uma inevitabilidade civilizacional.", *in* VENÂNCIO, Pedro Dias, "As Disposições Processuais Relativas a Dados Informáticos na Lei do Cibercrime", JusJornal, N.º 1183, 24 de Fevereiro de 2011, Editora Coimbra Editora, grupo Wolters Kluwer.

[20] Para uma leitura mais aprofundada do tema, sugere-se MARQUES, Maria Joana Xara-Brasil, "Os meios de obtenção de prova na lei do cibercrime e o seu confronto com o Código de Processo Penal", Dissertação de Mestrado, Universidade Católica Portuguesa, Lisboa, 2014.

[21] Neste sentido, designadamente, o Acórdão do Tribunal da Relação de Évora, de 06-01-2015, relatado por João Gomes de Sousa, disponível em www.dgsi.pt.

3. Obtenção da Prova Digital

3.1. Introdução

A actividade investigatória do Ministério Público em processo penal, com a coadjuvação dos órgãos de polícia criminal, não dispensa no hodierno paradigma sociológico-criminal, o recurso aos meios de **obtenção e recolha da prova digital** no âmbito da criminalidade em geral.

A grande indefinição legal, doutrinal e jurisprudencial do regime de obtenção da prova digital reforça a necessidade da Investigação criminal proceder, amiúde, com especial cautela na salvaguarda dos direitos fundamentais dos cidadãos, sob pena de ser inviabilizada a efectiva prossecução da acção e reacção penal em face de eventuais proibições de utilização e valoração da prova.

Apesar do tema ser já amplamente estudado e discutido pelos pensadores e intérpretes do Direito, a análise jurídica do regime da recolha da prova digital tem-se centrado mais no enfoque das incongruências legislativas e menos numa sistematização jurídico-pragmática dirigida aos operadores judiciários.

Na tentativa de ultrapassar, por via da metodização, as dificuldades amplamente assinaladas na aplicação do direito constituído nesta matéria, designadamente quanto à sobreposição dos regimes previstos nos diferentes diplomas reguladores, não se optou por partir, nestes escritos, da sistematização introduzida pela Lei do Cibercrime, abraçando-se antes como ponto de referência uma perspectiva mais pragmática e centrada nas diferentes formas como a prova digital pode chegar ao conhecimento da investigação.

Longe de se pretender abarcar aqui todas as múltiplas manifestações da realidade, sugere-se a análise relacional das medidas processuais legalmente previstas ([23]), distinguindo-se a prova digital voluntariamente disponibilizada e publicamente acessível da prova digital coercivamente recolhida, seja pela via da solicitação seja por via da pesquisa e apreensão.

3.2. Prova digital voluntariamente disponibilizada e publicamente acessível

3.2.1. Voluntariamente disponibilizada por quem tem disponibilidade/controlo

A reserva da vida privada ([24]), a proibição da intromissão nas comunicações ([25]) e mais recentemente, o direito ao anonimato e ao esquecimento na Internet ([26]) são direitos

[22] Embora não haja aqui oportunidade de aprofundar a análise dos problemas suscitados com a Lei 32/2008, sugere-se a leitura de PINHO, Carlos, "Os problemas interpretativos resultantes da Lei n.º 32/2008, de 17 de Julho", RMP, 129, Janeiro : Março 2012, pp. 63-93.
[23] Como defende PEDRO VENÂNCIO, as medidas processuais previstas na Lei do Cibercrime deverá ser *"analisadas como um todo pois em muitos aspectos se relacionam e complementam"*, *in* VENÂNCIO, Pedro, "Lei do Cibercrime Anotada e Comentada…", p. 99.
[24] Artigos 26.º, n.º 1 e 32.º, n.º 8, da Constituição da República Portuguesa.
[25] Artigos 34.º, n.º 4 e 32.º, n.º 8, da Constituição da República Portuguesa.

Internacionalmente e Constitucionalmente garantidos aos cidadãos, que preservam, no entanto, a sua natureza **disponível**.

Por essa razão, o **consentimento e a renúncia ao exercício desses direitos** pelo titular dos dados informáticos afasta a eventual ilicitude na obtenção da prova digital e a experiência tem revelado o grande contributo das vítimas, com disponibilidade ou controlo desses dados, ao fornecerem voluntariamente a prova digital à Investigação.

Nestas hipóteses, entendemos dever operar uma total **desconsideração quanto à natureza dos dados digitais** (sejam eles de natureza pessoal, íntima ou comunicacional), pois que mesmo no âmbito da correspondência electrónica, deve entender-se que o sigilo das comunicações esgota a sua tutela a partir da recepção da comunicação pelo destinatário, que poderá dispor de tais dados como bem entender ([27]). Assim, o receptor de uma comunicação poderá voluntariamente disponibilizá-la no âmbito do processo, ainda que sem o consentimento ou o conhecimento do remetente, e vice-versa.

A utilização dos meios tecnológicos deixa *rastos* nos sistemas operativos e informáticos em geral. Muitos dados informáticos são armazenados no sistema de forma automática, sob a forma de *logs*, de ficheiros temporários, ou caixa de mensagens, que ficam gravados no disco rígido do dispositivo ou nas bases de dados do sistema. Outros tantos são armazenados pela vontade do utilizador.

Por essa razão, ao utilizar um dispositivo de outrem, o utilizador conforma-se com a possibilidade desse armazenamento ocorrer, a não ser que tenha o cuidado de proceder a uma limpeza dos dados armazenados após a utilização. Os cidadãos dispõem de instrumentos capazes de eliminar ou ocultar os dados informáticos armazenados pela sua utilização do sistema, e em geral, de legitimamente vedar o acesso a tais dados em dispositivos que controlam.

Contudo, não o fazendo, o utilizador renuncia tacitamente à exclusiva disponibilidade dos dados. Assim sendo, o consentimento operante nestas hipóteses será o do **proprietário do sistema informático onde se encontra armazenada a prova digital** e não o do concreto titular de cada dado informático individualmente considerado. Nada impede, portanto, que o proprietário de um *smartphone* voluntariamente disponibilize à Investigação o conteúdo de uma *SMS* enviada pelo visado na investigação que não a apagou depois de utilizar o aparelho desse "terceiro".

Há, contudo, que distinguir, para efeitos processuais, **a disponibilização da prova digital** da **disponibilização do acesso ao sistema informático onde está armazenada a prova**.

[26] Afirmado pela primeira vez pelo Tribunal de Justiça da União Europeia, no Acórdão *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González* (ECLI:EU:C:2014:317). Agora expressamente acolhido no recente Regulamento (UE) 2016/679, do Parlamento Europeu e do Conselho (artigo 17.º).
[27] CANCELA, Alberto Gil Lima, ob. cit., pp. 60-61.

No primeiro caso, estão em causa as situações em que o cedente faz chegar ao processo dados informáticos, quer sejam corporizados em reproduções mecânicas (*CD's*, *DVD's*, *Pen-drive's*) ou em papel (impressões, *prints*, fotografias).

Nestas situações aplica-se o regime geral da admissibilidade da **prova documental**, previsto no Código de Processo Penal (artigo 164º e seguintes), uma vez que não houve intervenção activa do Ministério Público ou dos órgãos de polícia criminal na pesquisa e recolha dessa prova. Ela foi, no fundo, oferecida às instâncias de controlo formais, e como tal, nada impedirá a sua junção aos autos.

A junção de *prints* de conversas encetadas pela Internet ou por SMS, por algum dos intervenientes nessas conversas, não carece nem do consentimento do outro interveniente nem de validação judicial.

Já na segunda hipótese, de **disponibilização do acesso ao sistema informático onde está armazenada a prova**, a sua recolha pressupõe uma actividade investigatória do Ministério Público e/ou órgãos de polícia criminal na fase de Inquérito.

Por essa razão, a **pesquisa** de prova digital em sistema informático cujo acesso foi voluntariamente disponibilizado por quem tem a sua disponibilidade ou controlo deve obedecer às regras previstas nos artigos 15.º, n.º 3, alínea a) e 15.º, n.º 4, alínea b), da Lei do Cibercrime e artigo 253.º do Código de Processo Penal, a saber:

a) A necessidade de ser lavrado por escrito o consentimento do cedente;
b) A elaboração de um relatório pelo órgão de polícia criminal onde se mencione, de forma resumida, as investigações levadas a cabo, os resultados das mesmas, a descrição dos factos apurados e as provas recolhidas.
c) A remessa do relatório ao Ministério Público.

Ao nível da **junção** da prova digital pelos órgãos de polícia criminal, no decurso de uma pesquisa informática consentida, é igualmente de dispensar a prévia autorização da autoridade judiciária, **independentemente da natureza dos dados obtidos**, justamente em face do consentimento previamente prestado pelo cedente, afastando-se aqui a aplicação dos artigos 16.º, n.ºs 1 e 3 e 17.º da Lei do Cibercrime.

Em sentido convergente com o entendimento aqui perfilhado, fazem-se notar as seguintes considerações plasmadas no Acórdão do Tribunal da Relação de Guimarães, de 15-10-2012, relatado por Fernando Monterroso, disponível em www.dgsi.pt:

«Afigura-se desproporcionada a ideia de que o legislador pretendeu impor, a cada cidadão proprietário de um computador pessoal, que só possa fornecer a um tribunal os dados que nele possui depois de prévia autorização do juiz. Seria um entendimento pouco harmonioso com teleologia da lei, que visa a protecção do proprietário do sistema informático contra atentados de terceiros à privacidade dos seus próprios dados (e não a protecção dos terceiros). E

igualmente pouco harmoniosa com a perspectiva do juiz de instrução enquanto garante de direitos e liberdades, que é a do nosso processo penal.

Seria uma solução que levaria a consequências surpreendentes: o proprietário do sistema informático passaria a poder livremente exibir, facultar ou retransmitir a qualquer pessoa as mensagens e dados que armazenou (…), desde que essa pessoa não seja uma autoridade judiciária. Na realidade, a retransmissão e exibição de mensagens recebidas, seja através de sms, mails ou outros meios informáticos, é actualmente uma prática diária de milhões de pessoas em todo o planeta.»

Em sentido divergente, defende JOÃO CONDE CORREIA que *"tratando-se de um computador pessoal, quem tem disponibilidade sobre ele não terá, em princípio, legitimidade para autorizar a intromissão no seu conteúdo. Só o portador concreto daquele bem jurídico (reserva da intimidade da vida privada) poderá, validamente, prescindir dele"* ([28]). Distingue, para o efeito, o computador pessoal de um computador de uma empresa, em que *"a mera detenção já ganhará outro relevo, uma vez que não é expectável que ali estejam guardados dados pessoais, nem é expectável que aquela não tenha o controlo sobre o seu conteúdo"* ([29]).

Salvo o devido respeito, não será de propugnar com tal entendimento, uma vez que o equipamento é *pessoal* para o seu proprietário e não para todos os terceiros que o utilizem ou que com ele comuniquem. Como tal, a não ser que o terceiro visado apague os dados por si produzidos/armazenados durante a utilização, o proprietário exerce um domínio de facto sobre eles, ao ponto de os poder consultar, apagar, alterar, e como nos parece evidente, voluntariamente disponibilizar no âmbito do processo penal.

Outro entendimento também não nos parece de propugnar pela natureza muitas vezes anónima ou de difícil identificação da titularidade dos dados armazenados. Depender do consentimento do concreto titular do bem jurídico (eventual reserva da intimidade da vida privada), que nos parece ter a ele renunciado, significaria saber de antemão o que muitas vezes também se pretende demonstrar, a autoria dos factos.

Mesmo em matérias mais sensíveis, como é o tratamento e a livre circulação de dados pessoais, agora regulado pelo recente Regulamento (UE) 2016/679, do Parlamento Europeu e do Conselho, o ponto nevrálgico parece ser o da transparência para com o cidadão no tratamento e na circulação desses dados de natureza pessoal. Transpondo essa racionalização para as situações aqui em discussão, o consentimento do proprietário do sistema informático onde estão armazenados os dados só não será operante se a lei prever a impossibilidade de conservação e tratamento desses dados ou se, por qualquer forma, o proprietário se vinculou a assegurar a inviolabilidade desses dados ou ao seu carácter confidencial.

[28] CORREIA, João Conde, ob. cit., p. 51.
[29] *Idem*.

3.2.2. Prova digital publicamente acessível

Igual desconsideração quanto à natureza da prova digital deverá operar nas situações em que, apesar da prova digital não ser voluntariamente disponibilizada por quem tem a sua disponibilidade ou controlo, o Ministério Público e/ou os órgãos de polícia criminal puderam a ela ***publicamente*** aceder.

Nestes casos ocorre uma ***renúncia explícita*** do visado à eventual natureza sensível, pessoal ou íntima da informação ou comunicação, quando souber ou tiver meio de saber que tal informação passou a estar disponível a terceiros por sua própria iniciativa.

Por essa razão, e à imagem de qualquer cidadão, o Ministério Público e/ou os órgãos de polícia criminal poderão juntar aos autos a prova digital que obtiveram por meio do acesso público, aplicando-se o regime geral da admissibilidade da **prova documental**, previsto no Código de Processo Penal (artigo 164º e seguintes), independentemente da forma como a prova é corporizada no processo. Como boa prática e para prevenir futuros problemas de validade da obtenção da prova, o Ministério Público e os órgãos de polícia criminal deverão descrever, em despacho ou auto de diligência, respectivamente, o local (virtual) onde a prova foi encontrada (designadamente o endereço da web), e as circunstâncias de tempo e lugar em que tal diligência ocorreu, bem como uma descrição sintética do tipo de prova obtida e da sua relevância aos autos.

É legítima a recolha de dados (fotografias, mensagens, vídeos, informações pessoais) publicados nas redes sociais, por parte do Ministério Público e/ou dos órgãos de polícia criminal, sem prévia autorização ou posterior validação judicial.

3.3. Prova Digital Obtida por via da Injunção ([30])

Um dos mais relevantes meios de obtenção da prova digital opera por via da solicitação/injunção para a apresentação ou concessão da prova a quem tenha disponibilidade ou controlo dos dados informáticos. Nestes casos a prova não é nem voluntariamente disponibilizada nem publicamente acessível, mas sim fornecida mediante uma ordem pública emanada pela autoridade judiciária competente.

A **coercitividade** imanente deste modo de obtenção da prova digital faz incidir sobre os operadores judiciários uma especial necessidade de escrupuloso cumprimento das regras jurídicas que o regulam. Desde logo porque o incumprimento da ordem emanada pela

[30] Pelas limitações à dimensão destes escritos, não se fará menção à possibilidade de preservação e relevação expedita de dados (artigos 13.º e 14.º da Lei do Cibercrime), que são duas medidas processuais de natureza cautelar que suscitam, amiúde, problemas de ordem prático-jurídica quanto à obrigatoriedade de preservação dos dados e da duração dessa preservação pelos fornecedores de serviços de telecomunicações.

autoridade judiciária competente é cominada com a prática do crime de desobediência (artigo 14.º, n.ºs 1, *in fine*, e 3, da Lei do Cibercrime) ([31]).

É também nesta sede que se suscita o já mencionado problema da **natureza dos dados informáticos** e das três categorias conceptualizadas para os distinguir – dados de base, dados de tráfego e dados de conteúdo -, que tem uma crucial relevância para, em face dessa natureza -, saber qual é a **autoridade judiciária competente** para emanar a injunção para a sua apresentação – se o Ministério Público se o Juiz de Instrução.

3.3.1. A competência do Ministério Público

A injunção para a apresentação ou concessão de dados informáticos específicos e determinados, armazenados num determinado sistema informático, normalmente dirigida a um Fornecedor de Serviços ([32]), traduz-se numa ordem necessariamente emanada pela autoridade judiciária competente (artigo 14.º da Lei do Cibercrime) ([33]).

O problema jurídico que amiúde se suscita e ao qual a jurisprudência não tem dado resposta unânime é o de saber qual é a autoridade judiciária competente para ordenar aos Fornecedores de Serviços a apresentação ou concessão de dados relativos a **comunicações electrónicas**, designadamente todos os dados resultantes da utilização da Internet.

Enquanto *"juiz das liberdades"*, com competência para o exercício dos actos jurisdicionais até à fase de julgamento, cabe ao **Juiz de Instrução** autorizar e fiscalizar a obtenção de prova através da intromissão nas comunicações, sob pena da proibição de utilização da prova obtida em violação do princípio da proibição da intromissão nas comunicações e da reserva da vida privada (artigo 126.º, n.º 3 e 269.º, n.º 1, alínea e), do Código de Processo Penal).

Seria contudo grotesco defender-se que a tutela constitucional e legal do sigilo das telecomunicações se estende a toda a qualquer comunicação electrónica, já que, em rigor, tecnicamente, a mera ligação à Internet e a navegação são comunicações electrónicas encetadas, por impulso do utilizador, entre o equipamento de ponto de acesso (o computador, o *smartphone*, o *tablet*, o router) e os equipamentos (servidores, *routers*) de ponto de chegada.

---

[31] PAULO DÁ MESQUITA considera exagerada a punição pelo crime de desobediência, propugnando, em alternativa, pela aplicação de sanções pecuniárias compulsórias, favoráveis às exigências de celeridade processual, *in* MESQUITA, Paulo Dá, *ob. cit.*, p. 113.

[32] Definidos no artigo 2.º, alínea d), da Lei do Cibercrime como *"qualquer entidade, pública ou privada, que faculte aos utilizadores dos seus serviços a possibilidade de comunicar por meio de um sistema informático, bem como qualquer outra entidade que trate ou armazene dados informáticos em nome e por conta daquela entidade fornecedora de serviço ou dos respectivos utilizadores"*.

[33] Neste sentido, o recente Acórdão do Tribunal da Relação de Évora, de 02-05-2017, relatado por Clemente Lima, disponível em www.dgsi.pt, assim sumariado: *"Os dados, preservados ou conservados em sistemas informáticos só podem ser acedidos, em inquérito, por injunção do Ministério Público e em instrução pelo juiz de instrução. Tendo a prova em causa sido obtida pela Polícia Judiciária, sem prévio despacho do Magistrado do Ministério Público, deve ter-se por inválida"*.

Daí que historicamente se distinga os dados comunicacionais quanto à sua natureza, como **dados de base**, **dados de tráfego** ou **dados de conteúdo** ([34]), diferenciação essa que se aparta da própria Lei do Cibercrime e da Lei n.º 32/2008, de 17 de Junho.

Dados de base podem ser definidos como as informações pessoais e contratuais recolhidas pelos fornecedores de serviço (operadores de telecomunicações) sobre o cliente/assinante que com eles contratualiza o fornecimento de serviços de comunicação, tais como a identidade, a morada, o número de telefone, identificação civil e fiscal, o *e-mail*, a facturação, o tipo de serviço contratado, entre outros. Serão, enfim, todos os dados armazenados pelos fornecedores de serviço em momento anterior a qualquer comunicação electrónica e que com ela não se relacionam. Rigorosamente os dados de base poderão não consubstanciar prova digital nos termos já definidos, se não forem objecto de tratamento informático.

A **obtenção dos dados de base por via da injunção é da competência do Ministério Público** ([35]), na fase de Inquérito, como se concluiu no Parecer do Conselho Consultivo da PGR, n.º 21/2000, publicado no Diário da República, I Série, de 8 de Agosto de 2000:

"Em relação aos dados de base, ainda que cobertos pelo sistema de confidencialidade a solicitação do assinante, tendo em consideração que o sigilo profissional em causa releva de um simples interesse pessoal do utilizador que não contende com a respectiva esfera privada íntima, os correspondentes elementos de informação poderão ser comunicados, a pedido de qualquer autoridade judiciária, para fins de investigação criminal, em ordem ao prevalecente dever da colaboração com a administração da justiça".

Tem, nestes casos, aplicação o artigo 14.º, n.º 4, da Lei do Cibercrime, que torna a injunção "*aplicável a fornecedores de serviço, a quem pode ser ordenado que comuniquem ao processo dados relativos aos seus clientes ou assinantes, neles se incluindo qualquer informação diferente dos dados relativos ao tráfego ou ao conteúdo, contida sob a forma de dados informáticos ou sob qualquer outra forma, detida pelo fornecedor de serviços, e que permita determinar: O tipo de serviço de comunicação utilizado, as medidas técnicas tomadas a esse respeito e o período de serviço; A identidade, a morada postal ou geográfica e o número de telefone do assinante, e qualquer outro número de acesso, os dados respeitantes à facturação e ao pagamento, disponíveis com base num contrato ou acordo de serviços; ou qualquer outra informação sobre a localização do equipamento de comunicação, disponível com base num contrato ou acordo de serviços*".

[34] Posição sustentada em diversos pareceres do Conselho Consultivo da PGR (v. o Parecer n.º 21/2000, de 16 de Junho de 2000, homologado e publicado no Diário da República n.º 198, II Série, de 28 de Agosto de 2000, que originou a Directiva n.º 5/2000 – Despacho de 7 de Agosto de 2000, o Parecer n.º 16/94-Complementar, de 2 de Maio de 1994, publicado em Pareceres, edição da Procuradoria-Geral da República, vol. VI, pág. 535 e ss., e ainda o Parecer n.º 16/94, de 24 de Junho de 1994, que originou a Circular n.º 13/94, da Procuradoria-Geral da República) em que se estabeleceu uma distinção entre três categorias de dados: dados de base, dados de tráfego e dados de conteúdo.

[35] Neste sentido, também, o Acórdão do Tribunal da Relação do Porto, de 10-09-2014, relatado por Coelho Vieira, disponível em www.dgsi.pt.

Através da Base de Dados informaticamente disponibilizada pela NOS Comunicações, S.A, o Ministério Público poderá rapidamente aceder e fazer junção aos autos, durante a fase de Inquérito, dos dados de base respeitantes a determinado suspeito/arguido.

A definição de **dados de tráfego** vem expressamente prevista no artigo 2.º, alínea c) da Lei do Cibercrime: *"os dados informáticos relacionados com uma comunicação efectuada por meio de um sistema informático, gerados por este sistema como elemento de uma cadeia de comunicação, indicando a origem da comunicação, o destino, o trajecto, a hora, a data, o tamanho, a duração ou o tipo do serviço subjacente"*.

Em face do entendimento sufragado quanto à revogação tácita dos artigos 3.º, n.º 2 e 9.º, da Lei 32/2008, de 17 de Junho, deverá entender-se que **o Ministério Público tem competência para ordenar a apresentação ou concessão de dados de tráfego *determinados*, aos fornecedores de serviços durante a fase de Inquérito**, à luz do disposto no artigo 14.º, n.º 1, da Lei do Cibercrime.

Este é também o entendimento perfilhado em vários arestos jurisprudenciais, designadamente nos Acórdãos do Tribunal da Relação de Lisboa, de 22-04-2013 ([36]) e 19-06-2014 ([37]), e os Acórdãos do Tribunal da Relação de Évora, de 20-01-2015 e 06-01-2015 ([38]), estes últimos relatados por João Gomes de Sousa.

Com efeito, temos por certo que os dados de tráfego apenas permitirão contextualizar no tempo, espaço e meio, a realização de comunicações ([39]). Não permitindo identificar

[36] Segundo este Acórdão, relatado por Alda Tomé Casemiro, disponível em www.dgsi.pt:
«I - A Lei do Cibercrime (Lei 109/2009 de 15 de Setembro) nos seus artigos 12.º a 17.º respeitam a meios de obtenção de prova, mormente sua conservação e recolha. São eles: a "preservação expedita de dados", a "revelação expedita de dados de tráfego", a "injunção para apresentação ou concessão de acesso a dados", a "pesquisa de dados informáticos", a "apreensão de dados informáticos" e, finalmente, a "apreensão de correio electrónico e registo de comunicações de natureza semelhante". II - Com excepção desta última, em que se faz expressa menção à intervenção do juiz, todas as outras diligências são levadas a cabo por ordem da autoridade judiciária competente o que necessariamente inculca a ideia de que essa autoridade judiciária pode ser o Ministério Público ou o Juiz consoante a fase processual. IV - Significa isto, na leitura integrada de todo o regime legal, que se julga adequada a interpretação de que se os dados a obter são "dados de tráfego", de acordo com a definição do art. 2º, al. c) da Lei do Cibercrime, e tiverem de ser recolhidos junto de uma operadora localizada em território nacional, independentemente de estarmos perante "crimes graves", enunciados no artigo 2º, nº 1, alínea g) da Lei 32/2008 de 17 de Julho, poderá a autoridade judiciária competente, tendo em vista a descoberta da verdade, ordenar que estes sejam disponibilizados sob pena de punição por desobediência. É o que resulta do disposto no art. 14º, nºs 1, 2, 3 e 4 da mesma Lei.»
[37] Este Acordão, relatado por Margarida Vieira de Almeida, disponível em www.dgsi.pt, vem assim sumariado:
«I - estando apenas em causa a obtenção da identificação de um utilizador de um endereço IP ou o número de IP usado por um determinado indivíduo, em circunstâncias temporais determinadas, a competência para a respectiva obtenção é do M°P°. II - a identificação de um determinado endereço de IP conjugada com a identidade de quem o utilizou num dado dia e hora não revela informação sobre o percurso da comunicação nem sobre outro eventual tráfego comunicacional da pessoa em causa. III - os direitos constitucionais dos arguidos não são absolutos, face aos direitos dos restantes cidadãos, mormente das vítimas em processo penal, e as entidades públicas, ao enquadrar o uso dos diversos meios de prova têm de considerar os direitos dos vários intervenientes processuais.»
[38] Disponível em www.dgsi.pt.
[39] Neste sentido, referem JOSÉ LOPES e CARLOS CABREIRO que através dos dados de tráfego, apenas se saberá *"o destino da comunicação electrónica, não se descobrindo nada acerca das pessoas concretas, pelo que não se está a violar o núcleo fundamental do direito à intimidade"*, *in* LOPES, José Mouraz; CABREIRO, Carlos Antão; "A

directamente o concreto cidadão que encetou a comunicação ou o seu conteúdo, deve entender-se não haver lugar à tutela constitucional e probatória da proibição da intromissão nas comunicações e da reserva da vida privada.

Já quanto aos **dados de conteúdo**, que dizem respeito ao concreto teor da comunicação electrónica, é proibida a sua conservação pelos fornecedores serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações (artigo 1.º, n.º 2 da Lei n.º 32/2008, de 17 de Julho), pelo que não é de perspectivar a sua obtenção destas entidades por via da injunção para apresentação de dados de conteúdo.

Contudo, a injunção pode ser dirigida a quem tenha disponibilidade ou controlo dos dados, seja ou não um fornecedor de serviços de comunicações, pelo que, por esta via, é possível ordenar a apresentação de dados de conteúdo a quem deles tenha disponibilidade ou controlo, sendo que nestes casos, a autoridade judiciária competente para o ordenar será **o Juiz de Instrução**, mesmo na fase de Inquérito, valendo aqui em pleno, a tutela constitucional e legal do sigilo das comunicações.

Em conclusão, podemos afirmar que **o Ministério Público tem competência para, na fase de Inquérito, ordenar a apresentação ou concessão de dados informáticos determinados, quer sejam considerados de base ou de tráfego, a quem deles tiver disponibilidade ou controlo**.

Independentemente de se considerar o endereço de IP que esteve na origem da uma determinada comunicação como dado de base ou dado de tráfego, a sua obtenção é da competência do Ministério Público na fase de Inquérito.

3.3.2 A inaplicabilidade ao arguido/suspeito e a profissionais sujeitos a sigilo

O princípio *nemo tenetur se ipsum accusare* traduz-se na possibilidade concedida ao arguido de não contribuir processualmente para a sua auto-incriminação, que apesar de não estar expressa e directamente plasmado no texto constitucional, foi elevado pela doutrina e jurisprudência a direito fundamental de natureza constitucional ([40]).

O legislador preveniu a possibilidade de auto-incriminação do visado (arguido ou suspeito) ao **proibir que a injunção lhe possa ser dirigida** (artigo 14.º, n.º 5, da Lei do Cibercrime).

De igual modo, o legislador excluiu o uso da injunção a sistemas informáticos no exercício de actividades como a advocacia, médica, jornalística e bancária, ao abrigo do dever de sigilo destes profissionais. Para BENJAMIM SILVA RODRIGUES, esta limitação pretende defender estes profissionais, *"em nome dos valores ligados ao direito de defesa ou plenitude das garantias de defesa processuais penais, à privacidade ou reserva da intimidade ligada à saúde*

emergência da prova digital na investigação da criminalidade informática", Sub Judice - Justiça e Sociedade, Almedina, Lisboa, 2006.

[40] Neste sentido, entre outros, o Acórdão do Tribunal da Relação de Lisboa, de 17-04-2012, relatado por Simões de Carvalho, disponível em www.dgsi.pt.

e que implica o sigilo dos dados "sensíveis" da saúde das pessoas, o sigilo bancário e o sigilo profissional do jornalista e respectiva liberdade de informação e expressão implicadas, todos direitos com assento constitucional, nomeadamente, os artigos 26.º, 34.º, 37.º e 64.º da CRP 1976" ([41]).

Quanto ao **sigilo bancário**, entendemos que esta limitação constante do artigo 14.º, n.º 5, da Lei do Cibercrime deverá ter-se por **revogada**, por força do disposto no artigo 79.º, n.º 2, alínea e), do Decreto-Lei n.º 298/92, de 31 de Dezembro, na redacção dada pela Lei n.º 36/2010, de 02/09.

Actualmente as informações bancárias são, regra geral, submetidas a tratamento informático, e como a Lei n.º 36/2010, de 02/09, posterior à Lei do Cibercrime, veio introduzir uma importante excepção ao sigilo bancário, quando por solicitação de autoridade judiciária competente, no âmbito de processo penal, dificilmente se poderá conceber que a limitação constante do artigo 14.º, n.º 5, da Lei do Cibercrime (na parte em que se dirige à actividade bancária) continuará em vigor, sob pena de uma inultrapassável incoerência do sistema jurídico vigente.

3.4. Prova digital coercivamente pesquisada

Dispõe o artigo 15.º, n.º 1, da Lei do Cibercrime que *"quando no decurso do processo se tornar necessário à produção de prova, tendo em vista a descoberta da verdade, obter dados informáticos específicos e determinados, armazenados num determinado sistema informático, a autoridade judiciária competente autoriza ou ordena por despacho que se proceda a uma pesquisa nesse sistema informático, devendo, sempre que possível, presidir à diligência"*.

Na medida em que os sistemas informáticos se encontram, não raras vezes, em comunicação (ligação) com outros sistemas informáticos, o legislador admitiu a possibilidade de estender a pesquisa a esse outro sistema informático, desde que legitimamente acessível a partir do sistema inicial (n.º 5).

A pesquisa informática não é mais que uma *busca* realizada num sistema informático, como desde logo o indicia a remissão subsidiária para as regras de execução das buscas previstas no Código de Processo Penal e no Estatuto do Jornalista constante no n.º 6 do artigo.

Os órgãos de polícia criminal podem proceder à pesquisa, sem prévia autorização da autoridade judiciária, quando (n.º 3):
a) for voluntariamente consentida por quem tiver a disponibilidade ou controlo desses dados, desde que o consentimento prestado fique, por qualquer forma, documentado;
b) nos casos de terrorismo, criminalidade violenta ou altamente organizada, quando haja fundados indícios da prática iminente de crime que ponha em grave risco a vida ou a integridade de qualquer pessoa.

[41] RODRIGUES, Benjamim Silva, "Da Prova Penal, Tomo II, Bruscamente, A(s) Face(s) Oculta(s) dos Métodos Ocultos de Investigação Criminal", 1.ª ed., Rei dos Livros, Lisboa, 2010, p. 445.

No caso da alínea b) do n.º 3, os órgãos de polícia criminal comunicam, sob pena de nulidade, imediatamente à autoridade judiciária competente em ordem à validação da pesquisa efectuada, tendo em qualquer dos casos que proceder à elaboração de um relatório onde se mencione, de forma resumida, as investigações levadas a cabo, os resultados das mesmas, a descrição dos factos apurados e as provas recolhidas (n.º 4, alínea b)).

Da análise do artigo 15.º da Lei do Cibercrime, e conforme tivemos já oportunidade de frisar (em 2.1.1), existem relevantes diferenças entre a pesquisa informática consentida por quem tenha a disponibilidade do sistema informático (que neste caso, disponibiliza voluntariamente o acesso (físico ou virtual) ao sistema informático) da pesquisa informática coercivamente imposta por decisão da autoridade judiciária competente, essencialmente para efeitos da dicotomia entre junção e apreensão (*strictu sensu*) da prova digital conforme a natureza dos dados pesquisados.

4. Apreensão da Prova Digital

4.1. Introdução e delimitação

O caminho analítico e interpretativo até aqui percorrido conduz-nos finalmente ao âmago destes escritos, qual seja, a compreensão do regime de apreensão da prova digital, regulado nos artigos 16.º e 17.º da Lei do Cibercrime, e a sua integração sistemático-pragmática da recolha da prova digital em processo penal.

Foi necessário enquadrar a forma como a prova digital pré-constituída (armazenada) chega ao conhecimento da Investigação (Ministério Público e órgãos de polícia criminal) para agora proceder a uma coerente interpretação do trecho normativo inicial do artigo 16.º, n.º 1, que estipula: *"Quando, no decurso de uma pesquisa informática ou de outro acesso legítimo a um sistema informático, forem encontrados dados ou documentos informáticos necessários à produção de prova, tendo em vista a descoberta da verdade, a autoridade judiciária competente autoriza ou ordena por despacho a apreensão dos mesmos"*.

O regime da apreensão da prova digital só será aplicável quando os dados informáticos são encontrados no decurso de uma **pesquisa informática coercivamente encetada**, nos moldes *supra* descritos. É o carácter **intrusivo** da pesquisa informática que justifica não só a prévia autorização e posterior validação da autoridade judiciária competente para a apreensão (artigo 16.º, n.ºs 1 e 4), como a validação judicial quando o conteúdo dos dados seja susceptível de revelar dados pessoais ou íntimos (artigo 16.º, n.º 3), e de forma mais expressiva, a possibilidade da apreensão se processar por via da *"eliminação não reversível ou bloqueio do acesso aos dados"* (artigo 16.º, n.º 7, alínea d)).

Nas hipóteses de disponibilização voluntária de dados informáticos concretos, da apresentação por via de injunção ou revelação expedita, e dos dados publicamente acedidos, pela forma como chegam ao processo, não é concebível a aplicação do regime da apreensão previsto no artigo 16.º e 17.º da Lei do Cibercrime.

Nos casos em que a pesquisa informática é realizada pela disponibilização voluntária do acesso ao sistema informática, tem lugar o procedimento *supra* descrito em 3.2.1.

Compreende-se a tentação do intérprete em aplicar o regime da apreensão de dados informáticos na maioria das situações, muito devido às formas de apreensão previstas no artigo 16.º, n.º 7, que, em alguns casos, admitem a confusão entre apreensão *strictu sensu* e corporização dos dados para efeitos de junção aos autos. Contudo, é importante perceber que, particularmente, a realização de uma cópia dos dados, em suporte autónomo, tanto é uma forma de apreensão dos dados para efeitos do disposto nos artigos 16.º e 17.º da Lei do Cibercrime como, em geral, é uma forma admissível de corporização dos dados no processo, enquanto reprodução mecânica ou mesmo em formato papel (como defendemos em 1.3).

Fruto do que nos parece ser um grande equívoco, nos casos de apreensão de correio electrónico e registos de comunicações de natureza semelhante (nomeadamente SMS), a jurisprudência tem discutido a necessidade de validação judicial para efeitos de apreensão de transcrição de *e-mails* ou SMS voluntariamente apresentados pelas vítimas ([42]) ou mesmo consoante a comunicação já tenha sido lida ou não ([43]), quando cremos, a discussão deve centrar-se na forma como os dados ou comunicações chegam ao conhecimento das instâncias de controlo.

Só quando o conhecimento da prova digital (dados sensíveis e pessoais ou comunicações por correio electrónico ou similares) advier por intermédio da imposição público-judiciária e aquela deva ser recolhida pelas instâncias de controlo é que se impõe a necessidade do Juiz ponderar e decidir qual dos valores conflituantes deverá prevalecer – se a reserva da vida privada se o interesse da administração da justiça e da descoberta da verdade material.

Ressalva seja feita, como é evidente, aos casos em que a prova digital dessa natureza chegue ao conhecimento dos operadores judiciários pela actuação ilícita de terceiros. Não seria de todo admissível que se permitisse a utilização de prova digital que foi obtida por particulares através de acesso ilegítimo a sistema informático, por exemplo. Mas, em princípio, esse será um problema que poderá suscitar-se em fases mais avançadas no processo, em sede de valoração da prova em fase de julgamento, e não ao nível da sua obtenção, se esses dados forem publicamente acessíveis ou voluntariamente disponibilizados pelo titular do sistema informático onde se encontrem (também) armazenados, já que, à partida, o Ministério Público, enquanto *dominus* do Inquérito, ou mesmo o Juiz de Instrução (caso se propugnasse pela necessidade de aplicação do regime do artigo 17.º), não teriam forma de averiguar e decidir, *à priori*, a eventual ilicitude da obtenção desses dados ou comunicações disponibilizadas por terceiros ([44]).

[42] A título de exemplo, o recente Acórdão do Tribunal da Relação do Porto, de 05-04-2017, relatado por Moreira Ramos, disponível em www.dgsi.pt;
[43] Designadamente, os Acórdãos do Tribunal da Relação de Lisboa, de 02-03-2011, relatado por Jorge Raposo, disponível em www.dgsi.pt; 24-09-2013, relatado por Vieira Lamim, disponível em www.dgsi.pt; O Acórdão do Tribunal da Relação de Guimarães, de 12-10-2009, relatado por Tomé Branco, disponível em www.dgsi.pt.
[44] Assinalando-se um exemplo muito recente (caso dos *e-mails*), a junção aos autos do conteúdo das comunicações por correio electrónico alegadamente encetadas entre dirigentes e ex-dirigentes desportivos e árbitros, observadores e ex-árbitros desportivos, que foram voluntariamente disponibilizados e são, actualmente, publicamente acessíveis, não está sujeita ao regime previsto no artigo 17.º da Lei do Cibercrime, ou seja, a sua

4.2. Procedimento e regime legal

Se, no decurso de uma pesquisa informática coercivamente encetada em sistema informático, forem encontrados dados ou documentos informáticos necessários à produção de prova, tendo em vista a descoberta da verdade, o Ministério Público, na fase de Inquérito, e o Juiz de Instrução Criminal, durante a fase de Instrução, podem autorizar ou ordenar por despacho a apreensão dos mesmos (artigo 16.º, n.º 1, da Lei do Cibercrime).

As apreensões relativas a sistemas informáticos utilizados para o exercício da advocacia e das actividades médica e bancária estão sujeitas ao regime previsto no Código de Processo Penal, e as relativas a sistemas informáticos utilizados para o exercício da profissão de jornalista estão sujeitas às regras e formalidades previstas no Estatuto do Jornalista (n.º 5).
Excepcionalmente, os órgãos de polícia criminal poderão apreender tais dados, sem a prévia autorização da autoridade judiciária competente, sempre que a pesquisa informática tiver sido legitimamente ordenada e executada e ([45]) haja urgência e perigo na demora, estando contudo esta apreensão sujeita a validação pela autoridade judiciária, no prazo máximo de 72 horas (artigo 16.º, n.ºs 3 e 4, da Lei do Cibercrime).

Tendo em conta que a autoridade judiciária dificilmente saberá que dados serão encontrados no decurso da pesquisa informática, a não ser que presida à diligência, a apreensão dos dados pelos órgãos de polícia criminal constituí o procedimento regra na *praxis* judiciária, até porque, dada a *efemeridade* da prova digital, a urgência e o perigo de demora quase sempre se verificação, dada a possibilidade do titular do sistema informático poder facilmente apagar ou adulterar os dados.

Como a realidade se deve antepor às abstracções jurídicas, há que compreender que os dados a apreender pelos órgãos de polícia criminal podem revestir diversa natureza. Uns poderão ser simples dados informáticos e outros conteúdos de correio electrónico ou de comunicações de natureza semelhante. Quando esta prova digital é apreendida, o órgão de polícia criminal deverá apresentá-la para validação da autoridade judiciária no prazo de 72 horas. **Será, então, o Ministério Público, na fase de Inquérito, que depois de travar conhecimento com a eventual natureza pessoal, íntima ou comunicacional de alguns dos dados, decidirá se a sua apreensão efectivamente interessa à produção de prova, e em caso afirmativo, a apresentará ao Juiz de Instrução para autorização judicial da sua efectiva apreensão** (artigos 16.º, n.º 3 e 17.º da Lei do Cibercrime).

Seria altamente irrealista pensar-se ou ficcionar-se que a correspondência de correio electrónico ou uma caixa de mensagens escritas (SMS) é como uma missiva em envelope

junção aos autos não carece de validação judicial. Seria de extrema incoerência negar à investigação criminal a junção e utilização, ainda que provisória, do conteúdo dessas comunicações, tornando-as conhecidas de todos menos de um processo penal onde se pretende realizar uma incumbência constitucional tão importante como a administração da justiça e a descoberta da verdade material.

[45] A expressão utilizada na letra da lei "bem como" deve ser interpretada no sentido de se exigir **cumulativamente** que a pesquisa informática decorra nos termos da lei e que da não apreensão imediata advenha um perigo de perda da prova. Uma outra interpretação significaria admitir que a eventual nulidade da pesquisa informática em nada contende com a validade da apreensão realizada na sua sequência em caso de urgência ou perigo de demora.

lacrado, em que o Juiz seria a primeira pessoa a travar conhecimento do seu conteúdo no processo, como parece apontar alguma jurisprudência ([46]), aplicando o disposto nos artigos 179.º, n.º 3 e 268.º, n.º 1, alínea d), do Código de Processo Penal por referência do artigo 17.º da Lei do Cibercrime. Tal entendimento, que não encontra espelho na realidade, implica que, de facto, o Ministério Público seja o único a não ter conhecimento do conteúdo dessas comunicações, quando é a autoridade competente para decidir se, em abstracto, tal prova interessa ou não ao processo, tendo em conta a estrutura acusatória do processo penal português ([47]).

4.3. Formas de apreensão

No artigo 16.º, n.º 7, da Lei do Cibercrime vêm elencadas as diferentes formas de actuação apreensiva podendo ser apreendido o *"suporte onde está instalado o sistema ou (…) estão armazenados os dados informáticos, bem como os dispositivos necessários à respectiva leitura"* (alínea a)); realizar-se uma *"cópia dos dados, em suporte autónomo"*, depois junto ao processo (alínea b)); preservar-se a integridade dos dados, *"por meios tecnológicos (…) sem realização de cópia nem remoção dos mesmos"* (alínea c)); ou eliminar-se de forma não reversível ou bloquear-se o acesso aos dados (alínea d)).

A escolha destas formas de apreensão tem de satisfazer as necessidades de proporcionalidade e adequação em face dos interesses do caso concreto. Através deste catálogo taxativo, o legislador apresenta alternativas mais ou menos intrusivas. Enquanto que a realização de cópia dos dados em suporte autónomo ou a preservação da integridade dos dados sem cópia ou remoção não inviabilizam o acesso dos dados por parte do titular, já a apreensão do equipamento onde está instalado o sistema ou os dados ou a eliminação ou bloqueio dos dados evitam a utilização dos mesmos pelo titular. É de realçar a relevância da eliminação não reversível ou o bloqueio do acesso aos dados como forma de impedir a sua eventual utilização ou propagação nociva, como salienta ALBERTO GIL CANCELA, nos casos em que se trate, designadamente, de vírus, promoção ao terrorismo ou pornografia infantil ([48]).

Quando a apreensão assume a forma de cópia dos dados em suporte autónomo, impõe-se aos órgãos de polícia criminal a duplicação da cópia, sendo uma das cópias selada e confiada ao secretário judicial dos serviços onde o processo correr os seus termos (artigo 16.º, n.º 8). Nesse normativo a lei dá preferência à certificação das cópias por via da **assinatura digital**,

[46] O Acórdão do Tribunal da Relação de Lisboa, de 11-01-2011, relatado por Ricardo Cardoso, vem assim sumariado: *"(…) IIº As mensagens de correio electrónico ou registos de comunicações de natureza semelhante, que se afigurem de grande interesse para a descoberta da verdade ou para a prova, podem ser apreendidas, aplicando-se correspondentemente o regime de apreensão de correspondência previsto no CPP; IIIº Tais apreensões têm de ser autorizadas ou determinadas por despacho judicial, devendo ser o juiz a primeira pessoa a tomar conhecimento do conteúdo da correspondência apreendida, sob pena de nulidade;"*

[47] Defendendo igual solução, o Acórdão do Tribunal da Relação de Guimarães, de 29-03-2011, relatado por Maria José Nogueira, disponível em www.dgsi.pt, onde se lê: *"A apreensão de mensagens de telemóvel (SMS), mesmo que resultante de uma pesquisa de dados informáticos validamente ordenada pelo Ministério Público, deve depois ser autorizada pelo JIC. Embora o MP deva tomar conhecimento em primeira das mensagens, ordenando a apreensão provisória, deve depois ser o juiz a ordenar a apreensão definitiva - Artigo 17º da Lei do Cibercrime"*.

[48] CANCELA, Alberto Gil Lima, ob. cit., p., 45.

como uma medida de preservação, garantindo a integridade dos dados apreendidos relativamente a alterações posteriores à apreensão ([49]).

4.4. Correio electrónico e comunicações semelhantes

Como já se foi adiantando, *"quando, no decurso de uma pesquisa informática ou outro acesso legítimo a um sistema informático, forem encontrados, armazenados nesse sistema informático ou noutro a que seja permitido o acesso legítimo a partir do primeiro, mensagens de correio electrónico ou registos de comunicações de natureza semelhante, o juiz pode autorizar ou ordenar, por despacho, a apreensão daqueles que se afigurem ser de grande interesse para a descoberta da verdade ou para a prova"* (artigo 18.º da Lei do Cibercrime). Nestes casos, a lei manda aplicar *"correspondentemente o regime da apreensão de correspondência previsto no Código de Processo Penal"*.

O Código de Processo Penal, no seu artigo 179.º, prevê a possibilidade do juiz autorizar por despacho, sob pena de nulidade, a apreensão de correspondência quando esteja em causa:

(1) A correspondência dirigida ou expedida pelo suspeito ou arguido, mesmo que esteja sob nome ou pessoa diversa;
(2) Um crime punível com pena de prisão superior, no seu máximo, a três anos;
(3) Uma diligência que se revele indispensável para a descoberta da verdade ou para a prova (n.º 1), ficando excluída a possibilidade de apreensão de correspondência salvo se o juiz tiver fundadas razões para crer que aquela constitui objecto ou elemento de um crime (n.º 2).
Finalmente, determina que o juiz que tiver autorizado ou ordenado a diligência, deverá ser o primeiro a ter o conhecimento do conteúdo da correspondência apreendida, procedendo ao seu aditamento ao processo, caso esta se revele pertinente ou, pelo contrário, ordenar a sua restituição a quem de direito, impedido, consequentemente a sua utilização como meio de prova e a respectiva divulgação, uma vez que quem tiver tomado conhecimento ficará vinculado a um dever de segredo (n.º 3).

Se, como já defendemos supra, nos casos de apreensão de correio electrónico e registos de comunicações de natureza semelhante, deverá fazer-se uma interpretação ab-rogante do artigo 179.º, n.º 3 do Código de Processo Penal, no sentido do **conteúdo não dever ser apresentado em primeiro lugar ao juiz, mas sim ao Ministério Público**, pela visão sistemática da Lei do Cibercrime e realista a um nível fáctico-processual, também acompanhamos RITA CASTANHEIRA NEVES quando defende que a remissão para o regime de apreensão de correspondência (artigo 179º CPP) não abrange a alínea c) do nº 1, não sendo necessário para a aplicação da Lei do Cibercrime a verificação, no caso concreto, de um crime punível com pena de prisão superior a três anos ([50]).

[49] VENÂNCIO, Pedro Dias, "Lei do Cibercrime Anotada e Comentada…", pp. 114-115.
[50] NEVES, Rita Castanheira, "As Ingerências nas Comunicações Electrónicas em Processo Penal – Natureza e respectivo regime jurídico do correio electrónico enquanto meio de obtenção de prova", Coimbra Editora, Coimbra, 2011, p. 164.

Em primeiro lugar, porque à excepção da expressa previsão de um catálogo de crimes para efeito de intercepção de comunicações (artigo 18.º da Lei do Cibercrime), o artigo 11.º do mesmo diploma expressamente prevê um âmbito de aplicação geral das medidas processuais aí previstas.

Em segundo lugar, porque não seria coerente admitir-se a possibilidade de injunção para a apresentação de dados comunicacionais a quem deles tiver disponibilidade, sem qualquer tipo de consideração quanto ao tipo de crime praticado, mas não ser admitida a sua apreensão no decurso de uma pesquisa informática.

4.4.1. Comunicações lidas *versus* comunicações não lidas

Por força da remissão do artigo 17.º do Cibercrime para o regime da apreensão de correspondência do Código de Processo Penal, muitos são os autores que, à imagem do entendimento doutrinal ([51]) que defende a distinção entre correspondência lida e não lida, convocam à apreensão da correspondência digital o mesmo entendimento.

Segundo MANUEL COSTA ANDRADE, *"depois de recebido, lido e guardado no computador do destinatário, um e-mail deixa de pertencer à área de tutela das telecomunicações, passando a valer com um normal escrito"* ([52]).

Em sentido parcialmente concordante, PEDRO VERDELHO defendeu a aplicação do *"regime estabelecido para as escutas telefónicas para a fase de transmissão do e-mail, o regime da apreensão de correspondência para a fase em que o e-mail já chegou ao destino mas ainda não foi lido pelo destinatário e o regime da apreensão de normais ficheiros escritos quando o e-mail já foi aberto e lido pelo destinatário"* ([53]).

Este entendimento teve amplo acolhimento na jurisprudência, destacando-se o Acórdão do Tribunal da Relação de Évora, de 07-04-2015, relatado por Fernando Pina, disponível em www.dgsi.pt: *"E a mensagem recebida em telemóvel, atenta a natureza e finalidade do aparelho e o seu porte pelo arguido no momento das revistas e apreensões efectuadas, é de presumir que, uma vez recebida, foi lida pelo seu destinatário. Na sua essência, a mensagem mantida em suporte digital depois de recebida e lida terá a mesma protecção da carta em papel que tenha sido recebida pelo correio e que foi aberta e guardada em arquivo pessoal. Sendo meros documentos escritos, estas mensagens não gozam da aplicação do regime de protecção da reserva da correspondência e das comunicações"* ([54]).

[51] ANDRADE, Manuel da Costa, "Comentário Conimbricense do Código Penal", Tomo I, 2.ª ed, Coimbra Editora, Coimbra, 2012, p. 758, § 16.
[52] ANDRADE, Manuel da Costa, "Bruscamente no Verão Passado, a Reforma do Código de Processo Penal", Coimbra Editora, Coimbra, 2009, p. 157.
[53] VERDELHO, Pedro, "Apreensão do Correio Electrónico em processo Penal", RMP, Ano 25.º, n.º 100, Outubro-Dezembro, 2004, pp. 153-154.
[54] *Vide*, entre outros, Acórdão do Tribunal da Relação de Lisboa, de 02-03-2011, relatado por Jorge Raposo, disponível em www.dgsi.pt; Acórdão do Tribunal da Relação de Porto, de 20-01-2016, relatado por Artur Oliveira, disponível em www.dgsi.pt.

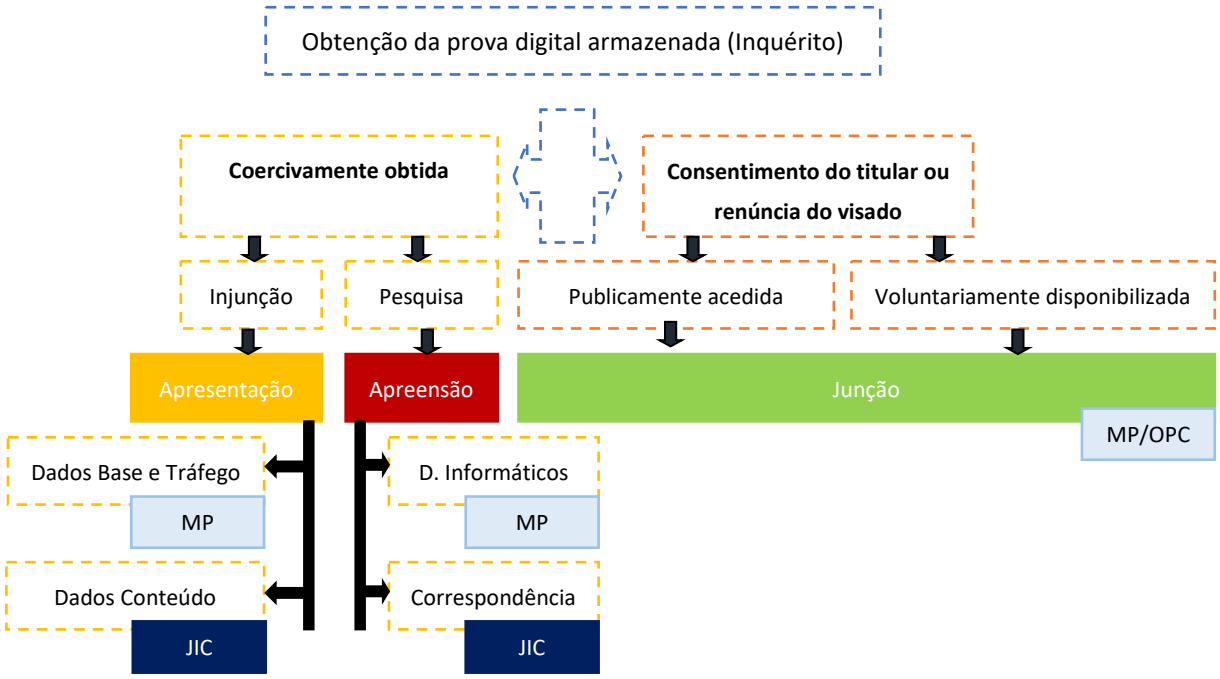
Seguindo-se este entendimento, o Ministério Público seria competente para proceder à apreensão da correspondência electrónica lida e aberta, ao abrigo do disposto no artigo 16.º, n.º 1 da Lei do Cibercrime.

Salvo o devido respeito, tal entendimento, apesar de bastante facilitador à investigação criminal, denota um desfasamento incomportável da realidade técnico-empírica e acima de tudo, parte de um erro na equiparação entre carta de papel e o armazenamento de correspondência digital. Nunca perdendo de vista que a apreensão de prova digital ocorre no decurso de uma pesquisa informática, é preciso que se perceba que os sistemas de comunicação, seja por via de correio electrónico (usando os protocolos *SMTP* e *POP3*), seja por via das mensagens telefónicas escritas (*SMS*), ou qualquer outra forma de comunicação privada (*Messenger* do *Facebook*, etc) pressupõem ao seu envio/recepção da correspondência digital o concomitante armazenamento no sistema informático. Para a intercepção de comunicações já o legislador previu, no artigo 18.º da Lei do Cibercrime o respectivo regime legal. Fora destes casos, que não estão aqui em discussão, lidas ou não lidas, as comunicações ficam armazenadas no sistema informático.

Depois de armazenada, seja no sistema operativo do equipamento (Outlook), seja em sistema informático acessível pela Internet (*Gmail*, *Facebook*, *Messenger*, *etc*.) é muitas vezes possível abrir e ler uma determinada correspondência e indicá-la como não lida assim como é possível não a abrir nem ler e indicá-la como lida, entre outras opções que as plataformas digitais admitem. Com efeito, no decurso de uma pesquisa informática, a diferença entre uma mensagem lida e não lida está à distância de um *click* de quem a está a efectuar, sem que seja possível a sindicância dessa actuação. Assim como seria uma *diabolica probatio* para o visado conseguir demonstrar que nunca abriu e leu a mensagem. É por essa razão, de ordem iminentemente empírica, que no artigo 17.º da Lei do Cibercrime se fala de mensagens e comunicações *armazenadas*, sem distinção entre lidas e não lidas.

Além de não decorrer da lei tal distinção, por estas razões apontadas, justifica-se em pleno um diferente tratamento entre uma carta em papel e a correspondência electrónica. A primeira, pela natureza das coisas, pressupõe que alguém a tenha efectivamente recebido (demonstrável pelo local onde foi encontrada no seguimento de uma busca), alguém a tenha lido (por não estar inserida num envelope lacrado), e uma vez na sua disponibilidade, alguém tenha decidido preservá-la como mero documento escrito. No segundo caso, as caixas de correio electrónico e as caixas de mensagens escritas são autênticos repositórios de informação confidencial, uma espampanante descrição de todos os aspectos da vida do cidadão, que merece, em nosso crer, uma constante tutela do sigilo das comunicações e da reserva da vida privada no decurso de uma pesquisa informática coercivamente encetada. Assim, **entendemos que a apreensão das comunicações electrónicas será sempre da competência judicial**.

IV. Conclusão Esquemática



V. Referências Bibliográficas

ANDRADE, Manuel da Costa, *Bruscamente no Verão Passado, a Reforma do Código de Processo Penal*, Coimbra Editora, Coimbra, 2009.

ANDRADE, Manuel da Costa, *Comentário Conimbricense do Código Penal*, Tomo I, 2.ª edição, Coimbra Editora, Coimbra, 2012.

CANCELA, Alberto Gil Lima, *A Prova Digital: Os meios de obtenção de prova na Lei do Cibercrime*, Dissertação de Mestrado, Faculdade de Direito da Universidade de Coimbra, Coimbra, 2016. [Disponível da web].

CORREIA, João Conde, *Prova Digital: as leis que temos e a lei que devíamos ter*, Revista do Ministério Público, 139, Julho: Setembro de 2014 [Disponível da web].

LOPES, José Mouraz; CABREIRO, Carlos Antão; *A emergência da prova digital na investigação da criminalidade informática*, Sub Judice - Justiça e Sociedade, Almedina, Lisboa, 2006.

MARQUES, Maria Joana Xara-Brasil, *Os meios de obtenção de prova na lei do cibercrime e o seu confronto com o Código de Processo Penal*, Dissertação de Mestrado, Universidade Católica Portuguesa, Lisboa, 2014 [Disponível da web].

NEVES, Rita Castanheira, "As Ingerências nas Comunicações Electrónicas em Processo Penal – Natureza e respectivo regime jurídico do correio electrónico enquanto meio de obtenção de prova", Coimbra Editora, Coimbra, 2011.

PINHO, Carlos, *Os problemas interpretativos resultantes da Lei n.º 32/2008, de 17 de Julho*, RMP, 129, Janeiro: Março 2012 [Disponível da web].

RAMOS, Armando Dias, *A Prova Digital em Processo Penal*, 1.ª edição, Chiado Editora, Lisboa, 2014.

RODRIGUES, Benjamim Silva, *Da Prova Penal, Tomo II, Bruscamente, A(s) Face(s) Oculta(s) dos Métodos Ocultos de Investigação Criminal*, 1.ª edição, Rei dos Livros, Lisboa, 2010.

RODRIGUES, Benjamim Silva, *Direito Penal Parte Especial*, Tomo I, Direito Penal Informático-Digital, Coimbra Editora, Coimbra, 2009.

VENÂNCIO, Pedro Dias, *As Disposições Processuais Relativas a Dados Informáticos na Lei do Cibercrime*, JusJornal, N.º 1183, 24 de Fevereiro de 2011, Editora Coimbra Editora, grupo Wolters Kluwer.

VENÂNCIO, Pedro Dias, *Lei do Cibercrime Anotada e Comentada*, 1.ª edição, Coimbra Editora, Coimbra, 2011.

VERDELHO, Pedro, *Apreensão do Correio Electrónico em processo Penal*, RMP, Ano 25.º, n.º 100, Outubro-Dezembro, 2004.

CENTRO
DE ESTUDOS
JUDICIÁRIOS

2.

Apreensão, exame ou perícia, e utilização processual de meios de prova existentes em material informático (documentos, correio eletrónico, memorandos pessoais, fotografias, registos, áudio, etc.). Enquadramento jurídico, prática e gestão processual

Henrique Gustavo Ribeiro Ferreira de Antas e Castro

CENTRO
DE ESTUDOS
JUDICIÁRIOS

2. APREENSÃO, EXAME OU PERÍCIA, E UTILIZAÇÃO PROCESSUAL DE MEIOS DE PROVA EXISTENTES EM MATERIAL INFORMÁTICO (DOCUMENTOS, CORREIO ELECTRÓNICO, MEMORANDOS PESSOAIS, FOTOGRAFIAS, REGISTOS, ÁUDIO, ETC…). ENQUADRAMENTO JURÍDICO, PRÁTICA E GESTÃO PROCESSUAL

Henrique Gustavo Ribeiro Ferreira de Antas e Castro

I. Introdução

Numa realidade que se vai tornando cada vez mais complexa, o que acarreta, consequentemente, uma sociedade com mais, maiores e diferentes problemas, é da maior importância que o Direito consiga fazer frente a essa tendência, tendo que acompanhar essa evolução de forma gradual, adaptando-se e readaptando-se às distintas circunstâncias, de forma a que nunca perca a sua actualidade.

Assim tem sucedido com o desenvolvimento tecnológico, com a proliferação dos aparelhos e dispositivos electrónicos e com a massificação da Internet que tornam imperativa essa permanente reflexão e estudo, único modo possível de combater novas formas de criminalidade, designadamente os fenómenos *cibercriminosos*, por um lado, e de obter e recolher prova transmitida ou armazenada por via digital, por outro lado.

Com tais avanços tecnológicos, a prova digital vem ganhando crescente importância na realidade judiciária quotidiana, constituindo talvez, hodiernamente, o âmago do direito processual penal, sendo, de facto, um instrumento essencial para o sucesso de uma investigação. Veja-se que poderemos ter informação relevante para o desfecho de um

processo crime armazenada num computador, numa *cloud*, numa *pen*, num *smartphone*, num *smartwtach*, num GPS, numa câmara fotográfica, enfim, numa multiplicidade de aparelhos electrónicos. Assim, revela-se mister o estudo da prova digital, a sua natureza e características, quadro normativo e, sobretudo, dos meios de obtenção de prova a que se pode recorrer neste campo.

II. Objectivos

Tendo em conta a cada vez maior relevância prática das disposições processuais em matéria de produção de prova digital, porquanto as mesmas se aplicam não só a crimes informáticos e cometidos por meio de sistemas informáticos, mas também a todos os crimes em relação aos quais seja necessário proceder à recolha de prova em suporte electrónico, torna-se premente o estudo das mesmas, constituindo o presente trabalho um pequeno contributo nesse sentido.

Assim, o trabalho pretende reunir, sem preocupações de exaustividade, um conjunto de ideias fulcrais e conselhos práticos referentes à prova digital, importantes sobretudo para a perspectiva do Ministério Público, sem se descurar, no entanto, os outros operadores judiciários.

Apesar de o enfoque central se traduzir na apreensão, exame e perícia, e utilização processual de meios de prova existentes em material informático, é ainda feito um enquadramento jurídico inicial relativamente à prova digital, sendo também abordados outros meios de obtenção de prova existentes na Lei do Cibercrime, aprovada pela Lei n.º 109/2009, de 15 de Setembro, além de se dedicar uma parte à prática e gestão processual, mormente para a fase de inquérito.

III. Resumo

A estrutura do presente trabalho subdivide-se em três pontos essenciais.

No capítulo de abertura é feito um breve enquadramento inicial sobre o tema, sendo designadamente abordado o conceito, especificidades e natureza da prova digital, bem como o quadro normativo que rege tal matéria no ordenamento jurídico português.

Subsequentemente, o segundo capítulo versa vários dos meios de obtenção de prova previstos na Lei do Cibercrime, identificando-se e analisando-se brevemente, num primeiro momento, os institutos da preservação expedita de dados, da revelação expedita de dados de tráfego e da injunção para apresentação ou concessão do acesso a dados. Ainda dentro do mesmo capítulo, são caracterizadas, de modo mais pormenorizado, as figuras da pesquisa informática, da apreensão de dados informáticos e de correio electrónico e registos de comunicações de natureza semelhante, bem como o regime de exames e perícias de dados informáticos, procurando-se sempre complementar tais abordagens mediante o recurso à jurisprudência mais pertinente.

O capítulo final, que está direccionado, sobretudo, para a prática e gestão processual, contém, além de um breve tratamento de algumas diligências investigatórias a realizar em sede de inquérito e que não requerem quaisquer conhecimentos informáticos específicos, um exame crítico sobre os procedimentos a adoptar pelo Ministério Público nos casos previstos nos artigos 16.º, n.º 3, e 17.º, ambos da Lei do Cibercrime.

1. Enquadramento jurídico

1.1. Conceito e natureza

De acordo com Benjamim Silva Rodrigues, "a prova digital "pode definir-se como qualquer tipo de informação, com valor probatório, armazenada [em repositório electrónico-digitais de armazenamento] ou transmitida [em sistemas e redes informáticas ou redes de comunicação electrónicas, privadas ou publicamente acessíveis], sob a forma binária ou digital"[1].

Ora, a própria definição apontada para a prova digital faz transparecer as inúmeras dificuldades que a mesma acarreta para qualquer operador judiciário. Na verdade, tendo em conta as características inerentes a tal parte do direito probatório, a investigação criminal neste ponto exige determinados conhecimentos específicos das entidades policiais e judiciárias de forma a lograr preservar, analisar, apreender, tratar e garantir a fiabilidade dessa mesma prova[2].

Veja-se que estamos, desde logo, a abordar uma prova que é imaterial, ou seja, insusceptível de apreensão material. Material é tão-somente o suporte em que a mesma se encontra, que é também, naturalmente, possível apreender, mas que não traduz, na verdade, a concreta prova digital ou electrónica.

Tal desmaterialização implica necessariamente um conjunto de outros dados caracterizadores de tal prova. De facto, a prova digital é também facilmente alterável e, nesse sentido, instável, dinâmica, dotada de grande volatilidade e temporária. É também apagável, manipulável, além de fragmentária e espacialmente dispersa, o que, sem dúvida, se revela prejudicial no campo da investigação.

[1] RODRIGUES, Benjamim Silva, "Direito Penal Parte Especial, Tomo I, Direito Penal Informático-Digital, Contributo para a Fundamentação da sua Autonomia Dogmática e Científica à Luz do novo Paradigma de Investigação Criminal: a Ciência Forense Digital e a Prova Digital", Coimbra Editora, 2009, citado por CANCELA, Alberto Gil Lima, "A Prova Digital: os meios de obtenção de prova na Lei do Cibercrime" Coimbra, 2016, disponível em https://estudogeral.sib.uc.pt/bitstream/10316/31398/1/A%20prova%20digital.pdf, consultado a 03.01.2018, p. 20.
[2] Cfr. MILITÃO, Renato Lopes, "A Propósito da Prova Digital", disponível em http://www.oa.pt/upl/%7B53f46e96-536f-47bc-919d-525a494e9618%7D.pdf, consultado a 03.01.2018. p. 261.

1.2. Quadro normativo

Realizadas estas breves considerações introdutórias sobre a prova digital, sua natureza e características, impõe-se analisar o quadro normativo que a rege no sistema processual penal português.

Nessa perspectiva, e apesar da existência de outros diplomas com relevância nesta sede, abordaremos, sobretudo, de forma mais extensa, a Lei do Cibercrime (Lei n.º 109/2009, de 15 de Setembro), e, num segundo patamar, a Lei n.º 32/2008, de 17 de Julho, e o Código de Processo Penal. Os três persistem na regulamentação de realidades similares, o que, de facto, tem provocado obstáculos interpretativos, dificultando-se, de tal forma, a desejada harmonização de todo o sistema[3].

Principiando tal exposição pelo Código de Processo Penal, importa, primacialmente, ter presente o artigo 189.º, que estende o regime previsto para a intercepção e a gravação de conversações ou comunicações telefónicas a outras conversações ou comunicações, transferidas por qualquer meio técnico diferente do telefone, designadamente correio electrónico ou outras formas de transmissão de dados por via telemática, mesmo que se encontrem guardadas em suporte digital, regulando ainda, no seu n.º 2, a obtenção e junção aos autos de dados sobre a localização celular ou de registos da realização de conversações ou comunicações. Tendo em conta as dificuldades interpretativas que gera, sobretudo ao estender o regime previsto nos artigos 187.º e 189.º do Código de Processo Penal ao correio electrónico já armazenado, esta norma já foi inclusivamente denominada de "'casa dos horrores' hermenêuticos"[4].

Por outro lado, a Lei n.º 32/2008[5] veio regular a conservação[6] e a transmissão dos dados de tráfego e de localização, bem como dos dados conexos necessários para identificar o assinante

[3] Veja-se a este propósito a expressão utilizada por João Conde Correia, segundo o qual "esta trilogia (…) contribui para a assimetria, para a incoerência das soluções legais e, sobretudo, para o seu indesejável e nefasto insucesso prático". Prosseguindo o seu raciocínio, o mesmo autor refere até que "[a] prova digital – essencial no mundo hodierno – continua mergulhada num verdadeiro pântano prático e, sobretudo, normativo". – CORREIA, João Conde, "Prova Digital: as leis que temos e a lei que devíamos ter", in Revista do Ministério Público, n.º 139, Julho/Setembro 2014, p. 30.

[4] ANDRADE, Manuel da Costa, ""Bruscamente no verão passado", a Reforma do Código de Processo Penal - Observações críticas sobre uma lei que podia e devia ter sido diferente", Coimbra, Coimbra Editora, 2009, p. 185.

[5] Lei essa que transpôs para a ordem jurídica interna a Directiva n.º 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de Março, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações, e que altera a Directiva n.º 2002/58/CE, do Parlamento Europeu e do Conselho, de 12 de Junho, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas.

[6] Nos termos do artigo 4.º, n.º 1, da Lei n.º 32/2008, "[o]s fornecedores de serviços de comunicações electrónicas publicamente disponíveis ou de uma rede pública de comunicações devem conservar as seguintes categorias de dados:
a) Dados necessários para encontrar e identificar a fonte de uma comunicação;
b) Dados necessários para encontrar e identificar o destino de uma comunicação;
c) Dados necessários para identificar a data, a hora e a duração de uma comunicação;
d) Dados necessários para identificar o tipo de comunicação;
e) Dados necessários para identificar o equipamento de telecomunicações dos utilizadores, ou o que se considera ser o seu equipamento;
f) Dados necessários para identificar a localização do equipamento de comunicação móvel".

ou o utilizador registado, para fins de investigação, detecção e repressão de crimes graves por parte das autoridades competentes (cfr. artigos 1.º, n.º 1 e 3.º, n.º 1). Assim, nos termos do artigo 9.º, n.º 1, deste diploma, a transmissão dos referidos dados só pode ser autorizada, por despacho fundamentado do juiz de instrução, se houver razões para crer que a diligência é indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter, só podendo ser transmitidos dados relativos ao suspeito ou arguido, a pessoa que sirva de intermediário, relativamente à qual haja suspeitas de que recebe ou transmite mensagens provenientes de arguido ou suspeito, e à própria vítima de crime, mediante o respectivo consentimento (artigo 9.º, n.º 3), devendo tal transmissão respeitar sempre os princípios da adequação, necessidade e proporcionalidade (artigo 9.º, n.º 4).

Por último, a Lei n.º 109/2009[7] (Lei do Cibercrime), à qual dedicaremos a maior parte da nossa atenção, introduziu um conjunto de disposições processuais penais, aplicáveis, nos termos do artigo 11.º, n.º 1, aos crimes previstos em tal diploma legal, bem como cometidos por meio de um sistema informático e ainda em relação aos quais seja necessário proceder à recolha de prova em suporte electrónico, constituindo, assim, sem dúvida, a "pedra angular"[8]de todo o sistema processual penal no que à prova digital concerne.

Dito isto, tendo em conta a vigência dos três instrumentos legislativos abordados, nem sequer é unânime, entre os vários autores consagrados no âmbito da prova digital, quais deles se encontram tacitamente revogados, bem como o âmbito de aplicação de cada um deles[9].

Por outro lado, segundo o artigo 6.º do mesmo diploma, tais entidades devem conservar os referidos dados pelo período de um ano a contar da data da comunicação.

[7] Tal lei transpôs para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de Fevereiro, relativa a ataques contra sistemas de informação, e adaptou o direito interno à Convenção sobre Cibercrime do Conselho da Europa.

[8] CORREIA, João Conde, "Prova Digital…", *ob. cit.*, p. 34.

[9] De facto, relativamente à articulação entre o Código de Processo Penal e as Leis n.º 32/2008 e 109/2009, João Conde Correia é claro ao dizer que estas revogaram tacitamente segmentos importantes do regime previsto no artigo 189.º do Código de Processo Penal, acrescentando que o âmbito de aplicação deste ficou restrito aos aspectos não especificamente regulados pelas leis extravagantes, e criticando, a final, a opção do legislador ao não o revogar formalmente, o que só cria dificuldades de ordem prática – cfr. CORREIA, João Conde, "Prova Digital…", *ob. cit.*, p. 36, bem como, no mesmo sentido, MESQUITA, Paulo Dá, "Processo Penal, Prova e Sistema Judiciário", 1.ª edição, Coimbra, Coimbra Editora, Setembro 2010, p. 123. Por outro lado, Pedro Verdelho, relativamente a esta mesma articulação, tem uma posição totalmente divergente porquanto entende que o regime previsto na Lei do Cibercrime não revogou o artigo 189.º do Código de Processo Penal nem colide com o mesmo, tendo tão-somente criado um regime específico para os crimes previstos na Lei do Cibercrime – cfr. VERDELHO, Pedro, "A nova Lei do Cibercrime", *in* Scientia Ivridica, Tomo LVIII, n.º 320, Outubro/Dezembro 2009, p. 747, e no mesmo sentido ALBUQUERQUE, Paulo Pinto de, "Comentário do Código Processo Penal à luz da Constituição da República Portuguesa e da Convenção Europeia dos Direitos do Homem", 4.ª edição, Lisboa, Universidade Católica Editora, 2011, p. 549.
Também no que concerne à complexa teia de relações entre as Leis n.º 32/2008 e 109/2009 a doutrina não tem sido unânime. Com efeito, há quem defenda que a Lei do Cibercrime revogou parte essencial do regime previsto na Lei n.º 32/2008, subsistindo a importância deste diploma apenas no que respeita ao estabelecimento de deveres para os fornecedores de serviços e prestação desses dados – cfr. MESQUITA, Paulo Dá, "Processo Penal…", *ob. cit.*, p. 123. Posição distinta manifestaram, a título exemplificativo, Rita Castanheira Neves e Renato Lopes Militão, para os quais tais instrumentos legislativos mantêm uma relação de complementaridade, tal como é, aliás, afirmado explicitamente pelo legislador no artigo 11.º, n.º 2, da Lei do Cibercrime (cfr. MILITÃO, Renato Lopes, "A Propósito…", *ob. cit.*, p. 275, e NEVES, Rita Castanheira, "As Ingerências nas Comunicações Electrónicas em Processo Penal – Natureza e respectivo regime jurídico do correio electrónico enquanto meio de obtenção de prova", Coimbra; Coimbra Editora, 2011, p. 234 e ss.).

2. Meios de obtenção de prova na Lei do Cibercrime

2.1. Preservação expedita de dados

Mais do que um meio de obtenção de prova, o artigo 12.º da Lei do Cibercrime consagra o que se pode denominar de medida cautelar não intrusiva. Isto porque, de facto, tal normativo não permite a obtenção e acesso aos dados informáticos em si mesmos, ou seja, ao seu conteúdo, mas apenas e tão-só consagra a possibilidade de as autoridades judiciárias competentes ordenarem a quem tenha disponibilidade ou controlo desses dados, designadamente a fornecedor de serviço, que preserve os dados em causa. Ou seja, o desiderato deste preceito consiste, sobretudo, na preservação e congelamento de tais dados, impedindo-se, assim, que os mesmos, virtualmente importantes no decurso de uma investigação criminal, sejam destruídos por uma qualquer forma.

Nesse sentido, a fim de se evitar que tais dados sejam perdidos, alterados ou deixem de estar disponíveis, o legislador processual penal reforçou nesta perspectiva as obrigações a que os fornecedores de serviços[10] já estavam vinculados por força da Lei n.º 32/2008. No entanto, diversamente do que sucede em tal diploma legal, esta disposição dirige-se a processos concretos[11], abrangendo ainda um leque de crimes consideravelmente mais vasto do que os incluídos no catálogo da Lei n.º 32/2008.

Relativamente às categorias de dados abrangidos pelo artigo 12.º da Lei do Cibercrime, impõe-se referir que tal preceito abrange quer dados armazenados num determinado sistema informático, quer os concernentes a transmissões de dados informáticos (dados de base e dados de tráfego[12]).

[10] O preceito visa não só os fornecedores de serviços, mas também qualquer outra entidade que tenha disponibilidade e controlo de dados informáticos específicos armazenados num sistema informático.
[11] Na Lei n.º 32/2008 está-se perante obrigações genéricas de preservação de dados.
[12] A este propósito, cumpre efectuar alguns esclarecimentos relativamente aos variados conceitos importantes nesta sede. Desde logo importa atentar no artigo 2.º da Lei do Cibercrime, que consagra um conjunto de definições importantes e pertinentes.
Assim, nos termos da alínea a) de tal preceito, o conceito de sistema informático subdivide-se em três: "qualquer dispositivo ou conjunto de dispositivos interligados ou associados, em que um ou mais de entre eles desenvolve, em execução de um programa, o tratamento automatizado de dados informáticos", "a rede que suporta a comunicação entre eles" e "o conjunto de dados informáticos armazenados, tratados, recuperados ou transmitidos por aquele ou aqueles dispositivos, tendo em vista o seu funcionamento, utilização, protecção e manutenção".
Relativamente à definição de dados informáticos, nos termos da alínea b) do mesmo preceito, os mesmos consistem em "qualquer representação de factos, informações ou conceitos sob uma forma susceptível de processamento num sistema informático, incluindo os programas aptos a fazerem um sistema informático executar uma função", abrangendo, assim, uma multiplicidade de dados: documento electrónico (nos termos do Decreto-Lei n.º 290-D/99, de 02 de Agosto), programa de computador (segundo o Decreto-Lei n.º 252/94, de 20 de Outubro), dados de conteúdo (para efeitos da Lei n.º 67/98, de 26 de Outubro), ou dados de tráfego ou localização (nos termos da Lei n.º 41/2004, de 18 de Agosto) - cfr. a este propósito VENÂNCIO, Pedro Dias, "Lei do Cibercrime Anotada e Comentada", 1.ª Edição, Coimbra, Coimbra Editora, 2011, p. 99.
Por fim, mas não menos importante, a alínea c) do mesmo preceito estipula ainda a definição de dados de tráfego: "os dados informáticos relacionados com uma comunicação efectuada por meio de um sistema informático, gerados por este sistema como elemento de uma cadeia de comunicação, indicando a origem da comunicação, o destino, o trajecto, a hora, a data, o tamanho, a duração ou o tipo do serviço subjacente". Tal categorização vem na senda de uma classificação tripartida de dados, que vem sendo adoptada quer pela jurisprudência, quer pela doutrina, contrapondo-se aos dados de tráfego os dados de base e os dados de conteúdo. Estes últimos são aqueles que se baseiam no conteúdo da comunicação transmitida pela rede de comunicações electrónicas, enquanto os dados de base consistem nos elementos fornecidos pelo utilizador à empresa que fornece o acesso à rede, desde a

A competência para ordenar a conservação dos dados em sede de inquérito pertence, naturalmente, ao Ministério Público, embora os órgãos de polícia criminal também o possam fazer nas condições estabelecidas no n.º 2 do artigo 12.º da Lei do Cibercrime[13]. O despacho fundamentado do Ministério Público a ordenar a preservação dos dados deve conter, nos termos do n.º 3 do mesmo artigo, sob pena de nulidade, a natureza dos dados, sua origem e destino, se forem conhecidos, bem como o período de tempo pelo qual deverão ser preservados, até um máximo de três meses (renovável até ao limite máximo de um ano, segundo o disposto no n.º 5).

2.2. Revelação expedita de dados

Tal como sucede com o artigo 12.º da Lei do Cibercrime, também o artigo 13.º consagra uma medida cautelar que, não obstante a epígrafe do preceito, não consiste verdadeiramente na revelação de quaisquer dados de tráfego, mas outrossim na obrigação de os fornecedores de serviços a quem tenha sido ordenada a preservação de dados nos termos do artigo anterior indicar à autoridade judiciária ou ao órgão de polícia criminal, logo que o souber, outros fornecedores de serviço através dos quais aquela comunicação tenha sido efectuada.

A necessidade desta medida explica-se tendo por base a ideia de que na transmissão de uma determinada comunicação participam frequentemente vários fornecedores de serviço, pelo que os dados de tráfego vão ficando repartidos por entre todos eles[14]. Nesse sentido, consciente de que cada fornecedor de serviço não detém a globalidade dos dados de tráfego necessários no contexto de uma investigação criminal, o legislador encontrou esta forma de obter célere e eficazmente o percurso completo de uma determinada comunicação informática, possibilitando a identificação da origem e destino de cada etapa percorrida. Assim, os fornecedores de serviços têm não só a obrigação de protegerem os dados nos termos do artigo 12.º, como também de indicarem sempre às entidades investigatórias os outros fornecedores de serviço através dos quais tal comunicação foi efectuada.

Com este mecanismo, logra-se de modo expedito obter informações relativas à cadeia de fornecedores de serviços pelos quais passou determinada comunicação, permitindo-se desde logo que também a esses seja dada ordem de preservação de dados, segundo o disposto no já analisado artigo 12.º da Lei do Cibercrime, no que traduz uma verdadeira relação de complementaridade entre as duas medidas cautelares.

identificação do utilizador e morada, bem como os dados que aquela empresa fornece, em sentido inverso, ao utilizador para efeito de ligação à rede, como por exemplo o número de acesso.

[13] Mediante autorização da autoridade judiciária competente ou quando haja urgência ou perigo na demora, devendo o órgão de polícia criminal, neste último caso, dar notícia imediata do facto à autoridade judiciária e transmitir-lhe o relatório previsto no artigo 253.º do Código de Processo Penal.

[14] Segundo o Relatório Explicativo da CCiber, citado por VENÂNCIO, Pedro Dias, "Lei do Cibercrime…", *ob. cit.*, p. 105, "na maioria dos casos, nenhum dos fornecedores de serviços detém individualmente os dados de tráfego fundamentais, em número suficiente, para possibilitar a identificação da verdadeira origem ou destino da comunicação. Cada um deles tem em sua posse uma parte do puzzle, e cada uma destas partes necessita de ser examinada de forma a detectar-se a sua origem ou o seu destino".

2.3. Injunção para apresentação ou concessão do acesso a dados

A injunção para apresentação ou concessão do acesso a dados é o primeiro verdadeiro meio de obtenção de prova digital presente na Lei do Cibercrime.

Consiste na possibilidade de, se no decurso do processo se tornar necessário[15] à produção de prova, tendo em vista a descoberta da verdade, obter dados informáticos específicos e determinados, armazenados num determinado sistema informático, a autoridade judiciária competente ordenar a quem tenha disponibilidade ou controlo desses dados que os comunique ao processo ou que permita o acesso aos mesmos. Ou seja, como a própria epígrafe do artigo faz antever, o preceito subdivide-se em duas partes essenciais: na apresentação dos dados ou na concessão de acesso a esses mesmos dados, devendo a ordem identificar os dados em causa, segundo o disposto no n.º 2 do artigo 14.º.

Relativamente à categoria de dados abrangidos por esta injunção, prescreve o n.º 4 do artigo 14.º da Lei do Cibercrime que nela se inclui qualquer informação diferente dos dados relativos ao tráfego ou ao conteúdo, contida sob a forma de dados informáticos ou sob qualquer outra forma, detida pelo fornecedor de serviços, e que permita determinar o tipo de serviço de comunicação utilizado, as medidas técnicas tomadas a esse respeito e o período de serviço; a identidade, a morada postal ou geográfica e o número de telefone do assinante, e qualquer outro número de acesso, os dados respeitantes à facturação e ao pagamento, disponíveis com base num contrato ou acordo de serviços; ou qualquer outra informação sobre a localização do equipamento de comunicação, disponível com base num contrato ou acordo de serviços.

Dito isto, resulta claro que a injunção se destina apenas a dados de base, não sendo, assim, possível que se ordene a comunicação ao processo ou a concessão de acesso a dados de tráfego ou de conteúdo. Nesse sentido constata-se que, apesar da íntima conexão deste meio de obtenção de prova com a medida cautelar prevista no artigo 12.º do mesmo diploma legal, a injunção aqui prevista tem um campo de aplicação mais restrito ao abranger apenas dados de base.
No que concerne à entidade competente para a ordem de apresentação dos dados ou concessão de acesso aos mesmos, dúvidas não há de que, em sede de inquérito, tal competência pertence ao Ministério Público.

Assim, é o Ministério Público que tem competência para o pedido de identificação do utilizador de um determinado endereço IP, num dado dia e hora, bem como o endereço IP usado por um determinado indivíduo em circunstâncias temporais determinadas. Actualmente a jurisprudência dominante aponta neste sentido, salientando precisamente que tais dados constituem dados de base, não contendendo com a privacidade do seu titular, nem revelando qualquer tipo de informação sobre o percurso da comunicação ou sobre qualquer outro eventual tráfego comunicacional da pessoa em causa[16].

[15] Não se exige mais do que a mera necessidade.
[16] Neste sentido, *vide*, entre outros, os Acórdãos do Tribunal da Relação de Lisboa de 19.06.2014, relatado por Margarida Vieira de Almeida, do Tribunal da Relação de Lisboa de 22.01.2013, relatado por Alda Tomé Casimiro, ou do Tribunal da Relação do Porto de 10.09.2014, relatado por Coelho Vieira.

Esta disposição legal não permite, no entanto, que se dirija a injunção contra suspeitos ou arguidos no processo, o que seria, aliás, violador do princípio *nemo tenetur se ipsumaccusare* (cfr. n.º 5 do artigo 14.º da Lei do Cibercrime – que não invalida a obtenção de tais dados por outras vias legítimas, previstas na própria Lei do Cibercrime).

Por outro lado, conforme dispõe o n.º 6 do mesmo preceito, não pode igualmente fazer-se uso da injunção prevista quanto a sistemas informáticos utilizados para o exercício da advocacia, das actividades médica e bancária e da profissão de jornalista, sendo ainda aplicável oregime de segredo profissional ou de funcionário e de segredo de Estado previsto no artigo 182.º do Código de Processo Penal. Assim, se é certo que tal meio de obtenção de prova visa, primacialmente, os fornecedores de serviço, o artigo 14.º da Lei do Cibercrime permite também o acesso a informações de outros sistemas informáticos, tais como computadores de estruturas empresariais onde suspeitos exerciam ou exerçam funções[17], cominando o seu incumprimento com o crime de desobediência[18].

2.4. Pesquisa de dados informáticos

A pesquisa de dados informáticos corresponde "grosso modo" a uma busca de dados em ambiente digital, motivo pelo qual lhe é aplicável subsidiariamente o regime de execução das buscas previsto no Código de Processo Penal (cfr. artigo 15.º, n.º 6, da Lei do Cibercrime).

Ora, no caso de ser necessário para a prova, tendo em vista a descoberta da verdade, obter dados informáticos específicos e determinados, armazenados num determinado sistema informático, a autoridade judiciária competente (que consiste no Ministério Público em sede de inquérito) autoriza ou ordena que se proceda a uma pesquisa nesse mesmo sistema informático. Nunca é demais sublinhar que se está perante uma disposição que permite a pesquisa tão-somente de dados informáticos armazenados, não se permitindo, por esta via, a intercepção de comunicações em curso.

Mais ainda, se no decurso de tal pesquisa surgirem razões para crer que os dados procurados se encontram noutro sistema informático (ou em parte diferente do mesmo sistema informático), o n.º 5 do artigo 15.º da Lei do Cibercrime confere, mediante autorização ou ordem da autoridade competente, a possibilidade de estender a pesquisa a tal sistema desde que os dados sejam legitimamente acessíveis a partir do sistema inicial, o que reveste cada vez maior importância prática hodiernamente, tendo em consideração, por exemplo, as redes sociais, servidores de correio electrónico ou *clouds*[19].

Em sentido contrário, *vide* a título exemplificativo o Acórdão do Tribunal da Relação de Coimbra de 03.10.2012, relatado por Alice Santos, que considera o endereço IP como um dado de tráfego, sujeitando, por isso, a sua obtenção à autorização de juiz de instrução.

[17] Cfr. VERDELHO, Pedro, "A nova Lei…", *ob. cit*., p.739.

[18] A propósito desta cominação, Paulo Dá Mesquita entende que a mesma é "uma medida processual e materialmente inadequada no plano jurídico-prático para os fins pretendidos", defendendo que, mais do que um mecanismo sancionatório, o legislador português deveria ter adoptado medidas compulsórias, fundamentalmente sanções pecuniárias compulsórias – cfr. MESQUITA, Paulo Dá, "Processo Penal…", *ob. cit.*, p. 113.

[19] Como bem refere João Conde Correia, não se consagra neste preceito a possibilidade de realização de buscas *online*, sem o conhecimento e consentimento do visado. De facto, o que está aqui em causa é apenas a "extensão

Realce-se que este artigo versa apenas sobre a pesquisa de dados informáticos. Questão diferente consiste na forma de acesso do Ministério Público a tais dados, designadamente ao suporte físico onde os mesmos se encontram armazenados, o que deixa desde já transparecer necessária articulação e harmonização deste regime com, por exemplo, os regimes das buscas e apreensões previstos no Código de Processo Penal. Por outro lado, refira-se ainda que tais dados informáticos podem ser levados ao conhecimento do Ministério Público, independentemente da realização de quaisquer buscas. Pensa-se, sobretudo, naqueles casos em que a própria vítima, por exemplo, entrega voluntariamente o suporte físico (telemóvel, computador ou qualquer outro dispositivo de natureza semelhante) que contém o sistema informático, onde se encontram armazenados os dados informáticos necessários à produção da prova (voltaremos a este tema *infra*).

O despacho do Ministério Público a ordenar a pesquisa de dados informáticos deve ser fundamentado, contendo os motivos pelos quais tal diligência é necessária à descoberta da verdade, e é válido por 30 dias. A diligência de pesquisa de dados informáticos deve ser presidida por magistrado, sendo que, caso tal se revele impossível, deve ser justificada a referida impossibilidade no despacho que ordena a pesquisa, o que será, porventura, a regra tendo em consideração as dificuldades de ordem prática que tal exigência colocaria na eficiente gestão do tempo de cada magistrado. Por outro lado, nas situações identificadas no n.º 3 do artigo 15.º da Lei do Cibercrime pode o órgão de polícia criminal proceder à realização de pesquisa de dados informáticos, sem necessidade de prévia autorização da autoridade judiciária, sendo, porém, necessária a comunicação à autoridade judiciária com vista à sua validação, bem como a elaboração e remessa do relatório previsto no artigo 253.º do Código de Processo Penal[20].

Por fim, no que concerne às formalidades da pesquisa informática, deve ser tido em conta o disposto no artigo 176.º do Código de Processo Penal (aplicável *ex vi* artigo 15.º, n.º 6, da Lei do Cibercrime).

2.5. Apreensão de dados informáticos

É fundamental, num primeiro momento, sublinhar novamente a interpenetração deste regime com o da pesquisa de dados informáticos, bem como com os regimes das buscas, revistas e apreensões, previstos no Código de Processo Penal, os quais são necessariamente complementares. De facto, quando se fala em apreensão de dados informáticos importa, desde logo, ter presente que tal não é o mesmo que a apreensão do suporte físico, do dispositivo em que os mesmos se encontram. Na verdade, para a apreensão de um aparelho

online de uma pesquisa de dados informáticos em curso. Não se trata, pois, de uma diligência complementarmente oculta, realizada à revelia do visado". Cfr. CORREIA, João Conde, "Prova Digital…", *ob. cit.*, p. 42.

[20] Questão que se levanta nesta sede prende-se com a alínea a) do referido n.º 3 do artigo 15.º da Lei do Cibercrime, segundo o qual a pesquisa pode ser efectuada por órgão de polícia criminal desde que a mesma seja voluntariamente consentida por quem tiver a disponibilidade ou controlo desses dados. Ora, nestes termos admitir-se que um terceiro com disponibilidade sobre os dados (pessoa diferente do visado) possa permitir o acesso a tais dados compromete a reserva da intimidade da vida privada do próprio visado. No entender de João Conde Correia, só o portador do concreto bem jurídico (reserva da vida privada) pode prestar o consentimento a que alude este preceito. Cfr. CORREIA, João Conde, "Prova Digital…", *ob. cit.*, p. 51.

não é necessário recorrer aos meios de obtenção de prova estipulados na Lei do Cibercrime, sendo bastante para o efeito os que constam do Código de Processo Penal.

Ora, o que o artigo 16.º da Lei do Cibercrime regula são as situações em há necessidade de apreender dados ou documentos informáticos necessários à produção de prova em processo penal, que forem encontrados no decurso de uma pesquisa informática (regulada no artigo 15.º da Lei do Cibercrime) ou de outro acesso legítimo a um sistema informático (por exemplo, uma perícia informática ou um exame).

Quanto à forma de apreensão dos dados ou documentos informáticos, rege o n.º 7 do referido artigo 16.º da Lei do Cibercrime, podendo a mesma processar-se de várias formas distintas consoante a que seja mais adequada e proporcional, tendo em consideração as necessidades do caso concreto, devendo ser sempre utilizado o meio menos oneroso para o visado pelas apreensões. Assim, o primeiro dos modos de apreensão previstos[21] não se traduz, a nosso ver, na decorrência do que já foi sendo expresso, numa verdadeira apreensão de dados informáticos. Se é apreendido, a título ilustrativo, um telemóvel (simultaneamente suporte e sistema informático onde se encontram armazenados dados informáticos), tal apreensão não consiste na apreensão dos dados aí presentes; para se obter tal informação é necessária a realização de uma pesquisa informática e subsequentemente uma apreensão dos dados informáticos, tal como expressamente regulado na Lei do Cibercrime. Veja-se que, por vezes, pode ser apreendido um suporte onde se encontram armazenados dados informáticos sem que se esteja, contudo, a apreender tais dados. Pense-se, por exemplo, numa situação em que um telemóvel é furtado ou objecto de um outro crime contra o património (receptação). Em tal caso, não é relevante a pesquisa e apreensão dos dados informáticos, conforme prevê a Lei do Cibercrime, sendo bastante para a produção de prova a apreensão do concreto aparelho, pelo que mal se compreende que a apreensão do suporte seja encarada como uma forma de apreensão de dados informáticos, tal como consagrado na alínea a) do n.º 7 do artigo 16.º do referido diploma legal[22]. Afigura-se-nos serem realidades juridicamente distintas, ainda que possam coincidir em termos materiais[23].

[21] Para Paulo Dá Mesquita, este preceito trata como formas de apreensão "realidades material, semântica e juridicamente inconfundíveis (nomeadamente misturando apreensão, com cópia, preservação e eliminação não reversível ou bloqueio do acesso aos dados)" – cfr. MESQUITA, Paulo Dá, "Processo Penal…", *ob. cit.*, p. 116.

[22] Veja-se o que a este propósito escreveram Pedro Verdelho, Rogério Bravo e Manuel Lopes Rocha: "Com excepção da mera apreensão de dados no seu suporte, que em nada se distingue de uma mera apreensão, todas estas medidas (incluindo a apreensão de dados separadamente do seu suporte) são medidas específicas do espaço virtual" – cfr. VERDELHO, Pedro, BRAVO, Rogério, ROCHA, Manuel Lopes, "Leis do Cibercrime", Volume I, 2003, disponível em http://www.centroatl.pt/titulos/direito/imagens/excerto-ca-leisdoCibercrime1.pdf, consultado a 03.01.2018, p. 18.

[23] Recuperando o exemplo de um telemóvel, no qual, neste caso, possam estar armazenadas provas do cometimento de um determinado crime (nos memorandos, agenda, listas de contactos). Se tal telemóvel for alvo de uma apreensão (na sequência de uma revista ou busca domiciliária), o regime legal que rege tal caso encontra-se previsto nos artigos 178.º e seguintes do Código de Processo Penal. Sendo necessária a realização de pesquisa informática, terá aplicação o regime previsto no artigo 15.º da Lei do Cibercrime. A conjugação desses dois regimes não é suficiente, a nosso ver, para se considerarem apreendidos os dados informáticos. A apreensão do suporte físico (que contém os referidos dados) não consiste na apreensão dos dados. Caso se revele necessária, por outro lado, a apreensão de tais dados, é necessário recorrer ao mecanismo previsto no artigo 16.º da Lei do Cibercrime, podendo a mesma efectuar-se através da realização de uma cópia dos dados em suporte autónomo, sem prejuízo de se manter a apreensão (física) do suporte físico onde tais dados informáticos se encontram armazenados.

Por outro lado, tal preceito prevê ainda, nas alíneas b), c) e d), como modos de apreensão de dados informáticos, a realização de uma cópia dos dados, em suporte autónomo, que será junta ao processo (neste caso, a cópia é efectuada em duplicado, sendo uma das cópias selada e confiada ao secretário judicial dos serviços onde o processo corre os seus termos e, se tal for tecnicamente possível, os dados apreendidos são certificados por meio de assinatura digital, por forma a garantir que os dados copiados são iguais aos originais – cfr. artigo 16.º, n.º 8, da Lei do Cibercrime[24]), a preservação, por meios tecnológicos, da integridade dos dados, sem realização de cópia nem remoção dos mesmos, ou ainda a eliminação não reversível ou bloqueio do acesso aos dados. Estas duas últimas alternativas também não consistem, no nosso prisma, em verdadeiras apreensões de dados, pois os mesmos não passam a estar na posse da autoridade judiciária com vista à produção da prova, sendo necessário subsequentemente efectuar cópia dos mesmos. São, no entanto, medidas de grande relevância quando a mera posse dos dados for ilícita, como programas com vírus ou pornografia infantil, casos nos quais é fundamental que o visado deixe de ter acesso aos dados.

Tal como sucede relativamente à pesquisa informática, também nesta sede é o Ministério Público a entidade competente para, no decurso do inquérito, ordenar a apreensão de dados informáticos, sem prejuízo da faculdade conferida aos órgãos de polícia criminal de efectuarem tais apreensões nos casos previstos no artigo 16.º, n.º 2, da Lei do Cibercrime. Em tais casos, como, aliás, em todos aqueles em que a apreensão seja efectuada por órgão de polícia criminal ainda que em cumprimento de mandado, é necessária posterior validação por autoridade judiciária (Ministério Público) no prazo máximo de 72 horas.

Contudo, na eventualidade de serem apreendidos dados ou documentos informáticos reveladores de dados pessoais ou íntimos, susceptíveis de colocar em causa a privacidade do respectivo titular ou de terceiro, tais dados ou documentos devem ser, sob pena de nulidade, apresentados ao juiz, que ponderará a sua junção aos autos tendo em conta os interesses do caso concreto, nos termos do disposto no artigo 16.º, n.º 3, da Lei do Cibercrime[25].

O regime previsto no artigo 16.º da Lei do Cibercrime, conjugado com o artigo 15.º do mesmo diploma, relativo à pesquisa informática, permite a utilização processual de vários meios de prova existentes em material informático, tais como memorandos pessoais, fotografias, agenda telefónica, lista telefónica, documentos, registos áudio, entre outros, não se incluindo todavia, nesta sede, os *e-mails* ou *sms's*, sujeitos a um regime normativo distinto. A utilização de tais meios de prova, cada vez mais premente em sede de investigação criminal, não depende de prévia autorização judicial, sendo bastante a intervenção do Ministério Público, excepto se contiverem dados pessoais ou íntimos. Tais dados, que não dizem respeito a qualquer comunicação já realizada ou em transmissão, estão apenas armazenados na memória

[24] Para Pedro Dias Venâncio, a certificação por meio de assinatura digital é uma forma tecnicamente idónea de assegurar a integridade dos dados informáticos apreendidos, relativamente a alterações posteriores à apreensão, não podendo, contudo, garantir a genuinidade dos mesmos até ao momento anterior à aposição de tal assinatura. Cfr. VENÂNCIO, Pedro Dias, "Lei do Cibercrime…", *ob. cit.*, p. 114.

[25] Para Paulo Dá Mesquita, este preceito visa dar expressão normativa ao Acórdão do Tribunal Constitucional n.º 607/2003, relativo à temática dos diários íntimos – cfr. MESQUITA, Paulo Dá, "Processo Penal…", *ob. cit.*, p. 116. No mesmo sentido, *vide* VERDELHO, Pedro, "A nova Lei…", *ob. cit.*, p. 741.

interna do telemóvel ou no cartão de memória. Nesse sentido pronunciou-se o Acórdão do Tribunal da Relação de Évora de 07.04.2015, relatado por Fernando Pina, também no que concerne ao registo de chamadas recebidas, não atendidas e efectuadas, em relação ao qual, sendo mero documento demonstrativo de comunicações telefónicas, a respectiva apreensão não depende de ordem judicial. No entanto, relativamente ao registo de telefonemas, afigura-se-nos difícil transpor a barreira criada pelo disposto no artigo 17.º da Lei do Cibercrime, segundo o qual os *registos* de comunicações de natureza semelhante ao correio electrónico, o que tanto pode incluir dados de conteúdo, como dados de tráfego, encontram-se sujeitos ao regime previsto nesse preceito.

Por outro lado, já se questionou também em sede jurisprudencial se a utilização processual de cópias de informação que alguém publicita no seu mural do Facebook, sem restrições de acesso, está ou não sujeita à disciplina prevista no artigo 16.º da Lei do Cibercrime. Ora, a esse propósito concluiu-se no Acórdão do Tribunal da Relação do Porto de 05.04.2017, relatado por Moreira Ramos, que nada impede que sejam utilizadas, no âmbito de procedimento criminal, as cópias de informação livremente acessível a todos. Diferente seria o caso, porém, se fosse necessário apreender os dados informáticos originais (não um simples "*print*") inseridos no Facebook (ou noutra plataforma), se, por exemplo, fosse colocada em causa a genuinidade das cópias extraídas legitimamente. Em tal hipótese, a recolha da referida prova estaria sujeita ao regime previsto na Lei do Cibercrime, nomeadamente ao artigo 16.º.

2.6. Apreensão de correio electrónico e registos de comunicações de natureza semelhante

A Lei do Cibercrime prevê um artigo específico quanto à matéria do correio electrónico e registos de comunicações de natureza semelhante, como *sms's*, mensagens enviadas pelo *whatsapp* ou outras aplicações idênticas, quando tais dados (de conteúdo ou tráfego) sejam encontrados no decurso de uma pesquisa informática ou outra forma de acesso legítimo a um sistema informático, aplicando-se correspondentemente nestes casos o regime da apreensão de correspondência previsto no artigo 179.º do Código de Processo Penal[26].

A apreensão de tais dados só pode ser ordenada por despacho do juiz nos casos em que a mesma se revele de grande interesse para a descoberta da verdade ou para a prova, de forma idêntica ao que estipula o Código de Processo Penal para a apreensão de correspondência, não resultando expressamente da lei em que momento processual deverá ser proferido tal despacho (tema a que voltaremos *infra*).

O que também não tem sido absolutamente unânime na doutrina e jurisprudência é o tratamento a dar ao correio electrónico ou registos de natureza semelhante quando já lidos. Isto porque o artigo 179.º do Código de Processo Penal, para o qual remete o artigo 17.º da Lei do Cibercrime, se reporta apenas à comunicação em curso, não versando sobre o conteúdo de comunicações já recebidas e lidas pelo destinatário, que decide guardá-las.

[26] Sobre as dúvidas, confusões e indefinições existentes relativamente à problemática da existência de várias normas potencialmente aplicáveis ao correio electrónico, *vide* MESQUITA, Paulo Dá, "Processo Penal…", *ob. cit.*, pp. 119 e ss.

Ora, desde logo impõe-se afirmar que não é necessária intervenção judicial (ou sequer do Ministério Público) quando o destinatário das mensagens de correio electrónico ou *sms's* as fornecer aos autos, autorizando a sua utilização como prova. Tal sucede, sobretudo, nos casos em que o ofendido armazena em aparelho digital (telemóvel, computador) tais registos, facultando-o para consulta e apreensão por parte das autoridades judiciárias[27]. Se os mesmos são fornecidos por quem pode dispor deles livremente, a intervenção judicial não teria qualquer fundamento.

A questão coloca-se, sobretudo, nos casos em que as mensagens estão armazenadas em aparelho de quem não autoriza a sua apreensão e junção de tal prova aos autos, nomeadamente se devem ou não tais mensagens/correio electrónico já recebidas e lidas ser tratadas como um simples documento escrito, à imagem do que sucede com o correio, deixando, consequentemente, de ser tuteladas como telecomunicações.

Ora, por um lado, o artigo 17.º da Lei do Cibercrime não efectua qualquer distinção entre os casos, parecendo que o legislador conferiu uma tutela superior aos escritos previstos no Código de Processo Penal do que ao correio electrónico. Mais ainda, o legislador utilizou, na formulação do referido artigo 17.º, o vocábulo "armazenados", o que subentende que é indiferente concluir pela leitura ou não da comunicação electrónica pelo destinatário, desde que a mesma esteja guardada em sistema informático. Adoptando-se essa perspectiva, só um juiz poderá, nos termos de tal preceito, autorizar ou ordenar a apreensão de tais ficheiros[28].

Por outro lado, muitas têm sido as vozes discordantes de tal opção legislativa, propugnando tese distinta, nomeadamente que um *e-mail* ou uma mensagem, depois de recebidos e lidos pelo seu destinatário, passam a valer como um qualquer documento escrito, podendo ser apreendido nos termos gerais. No caso, tendo em conta que estamos a abordar dados informáticos, tal apreensão pode ser efectuada nos termos do artigo 16.º da Lei do Cibercrime, sendo, assim, suficiente a intervenção do Ministério Público, não carecendo de despacho judicial. Sendo meros documentos escritos, deixam de gozar do regime de protecção da correspondência e das telecomunicações, ficando sujeitos ao regime geral de um qualquer outro documento que o visado armazena em determinado sistema informático, na medida em que não existe qualquer fundamento para tratar de forma diferente a correspondência prevista no Código de Processo Penal daquela que é abrangida pelo artigo 17.º da Lei do Cibercrime[29]. Assim, de acordo com esta tese, o momento de leitura do correio electrónico ou da mensagem traça a fronteira da tutela do sigilo da correspondência.

---

[27] Cfr. neste sentido, a título exemplificativo, os Acórdãos do Tribunal da Relação do Porto de 20.01.2016, relatado por Artur Oliveira, do Tribunal da Relação de Guimarães de 15.10.2012, relatado por Fernando Monterroso, ou do Tribunal da Relação de Lisboa de 29.03.2012, relatado por João Carrola.

[28] Nesse sentido, *vide* os Acórdãos do Tribunal de Relação de Guimarães de 29.03.2011, relatado por Maria José Nogueira, ou do Tribunal da Relação do Porto de 12.09.2012, relatado por Alves Duarte, segundo o qual em nada releva que as *sms's* tenham sido ou não abertas e lidas pelo destinatário, pois a lei não distingue entre as situações, invocando-se o princípio *ubi lex non distinguitnec nos distingueredebemus*.

[29] Assim defende, por exemplo, ANDRADE, Manuel da Costa, "Bruscamente no verão…", *ob. cit.*, p. 157. Também João Conde Correia, segundo o qual "aquilo que já não o é não pode nem tem que estar sujeito ao seu regime restritivo. Invocar o ritualismo da apreensão de correspondência quando já não há correspondência é um *contra-senso*. (…) A proteção do sigilo das comunicações (sejam elas por correio tradicional ou através dos meios que o progresso disponibilizou) deve terminar quando a mensagem chega ao seu destinatário e aquele processo de transmissão se encontra concluído". – cfr. CORREIA, João Conde, "Prova Digital…", ob. cit., p. 41. Em sentido

2.7. Perícia e exames de dados informáticos

Como já foi sendo referido, a Lei do Cibercrime não é taxativa relativamente aos meios de prova e meios de obtenção de prova nela existentes, tendo o legislador deixado margem de manobra ao aplicador do Direito para adoptar outras alternativas em matéria probatória para além da pesquisa informática. Isto resulta claro da análise dos artigos 16.º e 17.º da Lei do Cibercrime que expressamente referem "no decurso de uma pesquisa informática ou outro acesso legítimo a um sistema informático", não restando, portanto, dúvidas sobre a idoneidade probatória de outros meios de prova e de obtenção de prova.

Assim, não tendo a Lei do Cibercrime estipulado quaisquer disposições especiais relativamente à perícia e exame, previstos respectivamente nos artigos 151.º e seguintes e 171.º, do Código de Processo Penal, há que aplicar o regime previsto na lei geral com as necessárias adaptações à natureza da prova digital.

Ora, surgem, com regularidade, dúvidas na destrinça entre a prova pericial e os exames, sem que se deva, contudo, gerar confusão entre as duas realidades. Com efeito, os exames são um meio de obtenção de prova, cuja realização não carece de quaisquer conhecimentos específicos e que no panorama digital não se confundem com a figura da pesquisa informática[30].

Por contraponto, a perícia é um meio de prova, que, nos termos do artigo 151.º do Código de Processo Penal, "tem lugar quando a percepção ou a apreciação dos factos exigirem especiais conhecimentos técnicos, científicos ou artísticos". Nesse sentido, a prova pericial está sujeita a um conjunto de pressupostos e procedimentos, sendo que, segundo o disposto no artigo 163.º, n.º 1, do Código de Processo Penal, o juízo técnico, científico ou artístico inerente a tal prova presume-se subtraído à livre apreciação do julgador. Precisamente por tal motivo, o valor probatório de um auto de exame ou de um relatório pericial é diametralmente distinto.

Face à complexidade técnica da prova digital, à permanente inovação e proliferação de novos aparelhos, programas e sistemas informáticos, que contêm um manancial de informação nem sempre facilmente acessível ao utilizador médio, a prova pericial reveste-se de importância ímpar neste panorama, inclusivamente face aos referidos exames[31], os quais são sobretudo

idêntico, o Acórdão do Tribunal da Relação de Lisboa de 24.09.2013, relatado por Vieira Lamim, no qual se escreveu que "[a]s mensagens electrónicas (sms) deixam de ter a essência de uma comunicação em transmissão para passarem a ser antes uma comunicação já recebida, que terá porventura a mesma essência da *correspondência*», em nada se distinguindo de uma «carta remetida por correio físico»".

[30] Cfr. neste sentido VERDELHO, Pedro, "A nova Lei…", *ob. cit*., p. 740.

[31] A este propósito Pedro Verdelho, referindo-se ao "caso, por exemplo, dos rotineiros exames a computadores apreendidos em processos, quase sempre efectuados por inspectores da Polícia Judiciária", questionou se "[a] sofisticação de procedimentos adoptados e a complexidade da informação que é suposto analisar não deveria levar a que o formato de tais diligências fosse o da perícia?". Cfr. VERDELHO, Pedro, "Técnica no Novo C.P.P.: Exames, Perícias e Prova Digital", *in* Revista do CEJ, n.º 9, 1.º Semestre 2008, p. 147.
Mais ainda, o mesmo autor defendeu a particular importância das perícias no ambiente informático numa dupla perspectiva: por um lado, a opinião dos especialistas permite a quem investiga melhor compreender os factos em investigação; por outro, facilita a percepção e produção de prova em julgamento – cfr. VERDELHO, Pedro, "A obtenção de prova no ambiente digital", *in* Revista do Ministério Público, n.º 99, Julho/Setembro 2004, pp. 120-121.

relevantes quando os vestígios não são de tal forma complexos que exijam a realização de perícia[32].

Assim, o processo de realização de uma perícia informática ou digital forense, sempre tendo em vista a recolha de prova da prática de um crime no seio de uma investigação criminal, divide-se em quatro momentos essenciais: a identificação da origem da prova digital; a preservação dos dados identificados (eventualmente mediante realização de cópias de segurança/*backups* dos mesmos para suporte autónomo); a recolha, análise e investigação da própria prova digital; e, por fim, a apresentação dos relatórios periciais no processo.

3. Prática e gestão processual

3.1. Pedidos de dados a operadores

Face à necessidade de articular e harmonizar procedimentos nos pedidos de dados aos operadores de telecomunicações, a Procuradoria-Geral da República criou um protocolo de cooperação com os mesmos, no âmbito da investigação da cibercriminalidade e de obtenção de prova digital.

De facto, os referidos operadores têm importância significativa no contexto da preservação, armazenamento e produção de informação necessária à produção de prova em processo penal. Nesse sentido, a Circular n.º 12/2012, de 25.09.2012, da Procuradoria-Geral da República, consagrou um conjunto de formulários uniformizadores de procedimentos, mais definindo um leque de directrizes de molde a facilitar a satisfação pelos operadores de comunicações dos pedidos de colaboração do Ministério Público.

Assim, o Ministério Público tem disponíveis no Sistema de Informação do Ministério Público um conjunto de formulários pré-elaborados, quer relativos a pedidos de preservação de dados em processos crime, quer a pedidos de informação. Nos primeiros, o Ministério Público, fazendo uso dos meios de obtenção de prova (ou medidas cautelares) previstos nos artigos 12.º e 13.º da Lei do Cibercrime, indica a natureza dos dados a preservar, o período temporal abrangido, bem como, se possível, a origem e destino dos dados, podendo ainda solicitar, logo que sejam conhecidos outros fornecedores de serviço através dos quais as comunicações tenham sido efectuadas, informação com vista a permitir identificar todos os fornecedores de serviço usados por aquelas comunicações. Quanto aos pedidos de informação, permite-se, nos termos do artigo 14.º da Lei do Cibercrime, a obtenção de vários géneros de dados informáticos: números de IMEI's, números de telemóveis, identificação de titulares de telefones com respectivos dados pessoais, titulares de contas de correio electrónico, endereço de IP utilizado para aceder à conta de correio electrónico, todos os elementos disponíveis de identificação do utilizador de determinado IP num dado contexto temporal, entre muitos outros.

[32] Cfr. VERDELHO, Pedro, "A obtenção de prova…", *ob. cit.*, p. 121.

É, no entanto, importante que o pedido de solicitação do Ministério Público seja objecto de ponderação quanto à sua necessidade, bem como que em cada pedido seja especificado o respectivo objectivo, o que se traduz, sobretudo, na indicação concreta dos dados que se pretende.

Mais se diga ainda que, para além dos pedidos de dados às operadoras de telecomunicações, o Ministério Público tem disponíveis outras ferramentas essenciais no campo da recolha e obtenção de prova digital, sem necessidade de recorrer aos mecanismos de cooperação internacional, designadamente formulários a dirigir ao *Facebook, Instagram, YouTube, Microsoft, Google*, entre outras entidades estrangeiras, os quais são de utilização simples e expedita por qualquer magistrado do Ministério Público, ainda que sem conhecimentos informáticos relevantes, e que permitem, assim, obter, por exemplo, os dados referentes à identificação do titular de uma conta (nome, morada e endereço IP a partir do qual a conta foi aberta).

Por fim, cumpre ainda reafirmar que é ao Ministério Público, no âmbito dos seus poderes de direcção de inquérito, que compete efectuar a solicitação de informações a fornecedores de serviço, não devendo delegar tal tarefa em órgão de polícia criminal.

3.2. Procedimento no caso previsto no artigo 16.º, n.º 3, da Lei do Cibercrime

Os artigos 16.º, n.º 3, e 17.º, da Lei do Cibercrime não são absolutamente esclarecedores no que concerne ao momento e forma de intervenção do juiz de instrução no caso de apreensão de dados pessoais ou íntimos e correio electrónico ou registos de comunicação com natureza semelhante.

Com efeito, no que ao primeiro dos mencionados preceitos concerne, já se referiu *supra* que a entidade competente para ordenar a apreensão de dados informáticos é o Ministério Público; porém, caso sejam apreendidos dados ou documentos reveladores de dados pessoais ou íntimos susceptíveis de pôr em causa a privacidade dos respectivos titulares, revela-se necessário apresentar os dados ao juiz de instrução que ponderará a sua junção aos autos tendo em consideração os interesses do caso concreto. Assim, o teor literal do artigo parece apontar no sentido de que é bastante a intervenção legitimadora do Ministério Público para o órgão de polícia criminal proceder à apreensão dos dados, sendo que o juiz de instrução só intervém caso sejam apreendidos dados pessoais ou íntimos.

Ora, perante o exposto, a questão que se coloca na prática é se deve o Ministério Público, sem ter a noção precisa do que pode ser encontrado no decurso de uma busca (domiciliária ou não), seguida de apreensão do suporte, pesquisa e apreensão de dados informáticos, requerer, *a priori*, antes da realização das referidas diligências, ao juiz de instrução, a junção aos autos do que vier a ser encontrado[33]. Por um lado, tal procedimento poderia obviar à falta

[33] A nível prático, poder-se-ia levantar um problema se o juiz de instrução, quando requerida a sua intervenção, entendesse não ser da sua competência naquele momento autorizar em genérico a junção aos autos dos dados íntimos ou pessoais. Ora, a propósito das dúvidas e indefinições no que concerne à actuação do juiz de instrução

de definição legislativa do que sejam dados pessoais ou íntimos, não deixando nas mãos do órgão de polícia criminal a concretização de tal conceito[34].

Por outro, não parece ter sido essa a intenção do legislador. Assim, o Ministério Público, quando emite mandados de busca (ou promove a realização de busca domiciliária), pode desde logo ordenar também a pesquisa e apreensão de dados informáticos, informando o órgão de polícia criminal do procedimento que deve ser adoptado no caso previsto no artigo 16.º, n.º 3, da Lei do Cibercrime. Verificando-se a apreensão de dados íntimos ou pessoais, susceptíveis de pôr em causa a privacidade dos respectivos titulares, devem os autos ser presentes, em suporte autónomo, ao Ministério Público, que os apresentará ao juiz de instrução, justificando os motivos pelos quais, tendo em conta os interesses do caso concreto, tais dados devem ser juntos aos autos.

3.3. Procedimento no caso previsto no artigo 17.º da Lei do Cibercrime

O caso do artigo 17.º da Lei do Cibercrime contém contornos substancialmente divergentes.

De facto, relativamente ao correio electrónico ou registos de natureza semelhante, é o juiz que determina a apreensão daqueles que se revelem de grande interesse para a descoberta da verdade ou para a prova. Nesse sentido, a questão que aqui se coloca prende-se com a exigência prévia de despacho judicial a ordenar a apreensão das referidas mensagens. Ou seja, deve o Ministério Público, na pendência do inquérito, suscitar a intervenção judicial no sentido de ser autorizada a apreensão das mensagens que venham a ser encontradas no decurso de uma pesquisa informática ou outro acesso legítimo a um sistema informático antes da realização de tais diligências probatórias?

A lei não é absolutamente clara, sendo possível adoptar, portanto, duas perspectivas. Uma no sentido de que o despacho judicial a ordenar a apreensão tem de ser prévio. Ou seja, o Ministério Público pode determinar a realização de pesquisa informática, apreensão de dados (com a especificidade do artigo 16.º, n.º 3, da Lei do Cibercrime, quanto a dados pessoais ou íntimos), mas teria de ser o juiz de instrução a ordenar previamente a apreensão de correio electrónico ou mensagens similares. Nesse prisma, obtendo-se autorização judicial prévia, salvaguardar-se-ia à partida a hipótese de serem encontrados tais dados no decurso de um acesso legítimo a um sistema informático, pese embora o juiz de instrução não tivesse efectivo conhecimento dos mesmos, o que poderia redundar na prolação de um despacho demasiado

nas diligências probatórias atinentes à prova digital e na divisão das competências judiciárias e processuais, Paulo Dá Mesquita tem uma perspectiva curiosa, propugnando que "importaria ponderar uma maior flexibilização em termos de legitimação de um procedimento judicial de cautela, ao nível da intervenção judicial provocada por impulso do titular da acção penal". Assim, defende o mesmo autor o estabelecimento de maior maleabilidade na apreciação judicial preventiva "no sentido de a eventual cautela procedimental do titular da acção penal determinar dois correlativos: (1) Auto-vinculação na sujeição a uma pronúncia judicial sobre a questão suscitada; (2) Dever judicial de apreciação do mérito do pedido ainda que se admitisse a competência do requerente para conhecer a questão" – MESQUITA, Paulo Dá, "Processo Penal…", *ob. cit.*, p. 124.

[34] Imagine-se o caso em que o órgão de polícia criminal, após apreensão, por entender que os dados ou documentos não contêm dados pessoais ou íntimos, não apresenta os autos ao Ministério Público (e subsequentemente ao juiz de instrução), provocando, assim, a nulidade da prova.

genérico, quase fornecendo uma verdadeira *carta em branco* à investigação, não sendo possível efectuar a ponderação de valores que o preceito em causa exige[35].

A outra posição, que se nos afigura o procedimento mais correcto para a gestão processual do inquérito pelo Ministério Público, consiste na apreensão cautelar/provisória do correio electrónico ou mensagens análogas por tal autoridade judiciária, sendo o despacho judicial apenas posterior. Assim, o Ministério Público pode autorizar a pesquisa informática de dados (ou outra forma legítima de acesso ao sistema informático), sendo que, se no respectivo decurso forem encontradas mensagens, estas são apreendidas provisoriamente (ou, porventura, informalmente), devendo, ulteriormente, o Ministério Público apresentar tais mensagens, em suporte autónomo, ao juiz de instrução, que determinará, consoante conclua pelo grande interesse das mesmas para a descoberta da verdade ou para a prova, a sua apreensão definitiva (ou formal) e consequente junção aos autos[36].

Nesse sentido, tem que se entender, contrariamente ao que sucede com o regime da apreensão de correspondência, que não é o juiz de instrução a primeira pessoa a tomar conhecimento do conteúdo da correspondência apreendida, podendo ser o órgão de polícia criminal ou o Ministério Público. De facto, só assim pode ser porquanto a própria pesquisa informática (ou outro acesso legítimo ao sistema informático) podem obrigar desde logo a entidade investigatória a ter conhecimento do conteúdo das mensagens, que, assim, efectuam logo o filtro das mensagens com relevância para o caso concreto, apenas encaminhando essas mesmas para o juiz de instrução[37].

3.4. Outras diligências de investigação

Há um manancial de outras diligências de investigação que um magistrado do Ministério Público mais pró-activo na direcção do inquérito pode realizar por si só, sem necessidade de delegação noutras entidades, e que não requerem conhecimentos técnicos específicos.

Desde logo, pode-se naturalmente efectuar qualquer pesquisa nos diferentes motores de busca disponíveis na Internet, tais como o *Google, Bing, Yahoo, Sapo*, as quais podem assumir contornos importantes em determinados contextos.

É possível também a obtenção de informação relativa à prática de ilícitos criminais nas redes sociais. Bem se sabe que a proliferação das mesmas criou novos tipos de criminalidade e

[35] Relativamente à possibilidade de despacho judicial prévio, Pedro Verdelho manifestou-se contra tal posição, defendendo que "em regra, antes de uma busca ainda não se sabe se vai encontrar-se, no seu decurso, um computador. E menos ainda se sabe se em tal computador vão encontrar-se mensagens de correio electrónico ou análogas. E muito menos pode prever-se se essas mensagens podem ou não a vir a ter interesse para a investigação." Mais conclui o mesmo autor pela inviabilidade de um sistema ´"que exigisse, antes de toda e qualquer busca, a obtenção de autorização judicial para a eventual possibilidade de vir a ser encontrado (…) um computador e que tal computador contivesse registos de comunicações, e que tais comunicações fossem prova necessária à investigação do caso concreto" – cfr. VERDELHO, Pedro, "A nova Lei…", *ob. cit*., pp. 743-744.

[36] Cfr. neste sentido, VERDELHO, Pedro, "A nova Lei…", *ob. cit*., pp. 743-744, e o Acórdão do Tribunal da Relação de Guimarães de 29.03.2011, relatado por Maria José Nogueira.

[37] *Vide*, em sentido contrário, o Acórdão do Tribunal da Relação de Lisboa de 11.01.2011, relatado por Ricardo Cardoso.

desenvolveu novas formas de praticar ilícitos criminais já existentes. Muitas das páginas, perfis, grupos *online*, por via dos quais tais crimes são cometidos, são públicos, sendo, destarte, acessíveis por qualquer pessoa, possibilitando a recolha e obtenção de prova digital pelo próprio magistrado do Ministério Público.

Por outro lado, também através da análise aos cabeçalhos técnicos de correio electrónico é possível encontrar indícios a fim de identificar a identidade de determinado remetente que tenha utilizado o correio electrónico para a prática de determinado crime. Com efeito, as informações constantes dos cabeçalhos técnicos de correio electrónico incluem vários detalhes técnicos como, por exemplo, o endereço de correio electrónico do remetente, o endereço IP do dispositivo que se ligou ao correio electrónico de onde se enviou a mensagem, a identificação da própria mensagem, a sua data, hora e fuso horário, o *software* utilizado para a escrever, o endereço de correio electrónico do destinatário, bem como os servidores de correio electrónico por que passou a mensagem no seu percurso para o destinatário. Com uma simples pesquisa num motor de busca, facilmente se encontram guias ou manuais electrónicos, fornecidos pelos próprios servidores de *e-mail* (*Gmail, Microsoft Outlook, Hotmail*, por exemplo) sobre a forma de recolher e ler a informação presente nos cabeçalhos técnicos, de molde a interpretar-se devidamente o respectivo conteúdo.

Por fim, uma última referência para outra ferramenta de investigação facilmente disponível para a prática processual e recolha de prova em sede de inquérito e que não requer quaisquer conhecimentos específicos técnicos fora da óptica do utilizador médio, que consiste nos diferentes localizadores de IP's disponíveis gratuitamente, importantes no sentido de apurar a identidade de determinados agentes da prática de crime, dos quais são exemplo:

– https://whois.domaintools.com/
– https://centralops.net/co/
– http://dnstools.com/
– https://whatismyipaddress.com/
– http://smart-ip.net/whois
– https://www.ultratools.com/tools/ipv6Info.

IV. Referências bibliográficas e hiperligações

Referências bibliográficas

ALBUQUERQUE, Paulo Pinto de, "Comentário do Código Processo Penal à luz da Constituição da República Portuguesa e da Convenção Europeia dos Direitos do Homem", 4.ª edição, Lisboa, Universidade Católica Editora, 2011;

ANDRADE, Manuel da Costa, ""Bruscamente no verão passado", a Reforma do Código de Processo Penal - Observações críticas sobre uma lei que podia e devia ter sido diferente", Coimbra, Coimbra Editora, 2009;

CANCELA, Alberto Gil Lima, "A Prova Digital: os meios de obtenção de prova na Lei do Cibercrime" Coimbra, 2016, disponível em https://estudogeral.sib.uc.pt/bitstream/10316/31398/1/A%20prova%20digital.pdf, consultado a 03.01.2018;

CORREIA, João Conde, "Prova Digital: as leis que temos e a lei que devíamos ter", *in* Revista do Ministério Público, n.º 139, Julho/Setembro 2014, pp. 29-59;

DIAS, Vera Elisa Marques, "A problemática da investigação do Cibercrime", *in*DataVenia Revista Jurídica Digital, N.º 1, Julho-Dezembro, 2012, disponível em https://www.datavenia.pt/ficheiros/edicao01/datavenia01_p063-088.pdf, consultado a 03.01.2018;

MESQUITA, Paulo Dá, "Processo Penal, Prova e Sistema Judiciário", 1.ª edição, Coimbra, Coimbra Editora, Setembro 2010;

MILITÃO, Renato Lopes, "A Propósito da Prova Digital", disponível em http://www.oa.pt/upl/%7B53f46e96-536f-47bc-919d-525a494e9618%7D.pdf, consultado a 03.01.2018;

NEVES, Rita Castanheira, "As Ingerências nas Comunicações Electrónicas em Processo Penal – Natureza e respectivo regime jurídico do correio electrónico enquanto meio de obtenção de prova", Coimbra, Coimbra Editora, 2011;

RODRIGUES, Benjamim Silva, "Da Prova Penal – Tomo IV, DaProva Electrónico-Digital e da Criminalidade Informático-Digital", 1.ª Edição, Rei dos Livros, 2011;

VENÂNCIO, Pedro Dias, "Lei do Cibercrime Anotada e Comentada", 1.ª Edição, Coimbra, Coimbra Editora, 2011;

VERDELHO, Pedro, "A Convenção sobre Cibercrime do Conselho da Europa - Repercussões na Lei Portuguesa", Direito da Sociedade da Informação, volume VI, Coimbra, Coimbra Editora, 2006;

VERDELHO, Pedro, "A obtenção de prova no ambiente digital", *in* Revista do Ministério Público, n.º 99, Julho/Setembro 2004, pp. 117-136;

VERDELHO, Pedro, "A nova Lei do Cibercrime", *in* ScientiaIvridica, Tomo LVIII, n.º 320, Outubro/Dezembro 2009, pp. 717-749;

VERDELHO, Pedro, "Técnica no Novo C.P.P.: Exames, Perícias e Prova Digital", *in* Revista do CEJ, n.º 9, 1.º Semestre 2008;

VERDELHO, Pedro, BRAVO, Rogério, ROCHA, Manuel Lopes, "Leis do Cibercrime", Volume I, 2003, disponível em http://www.centroatl.pt/titulos/direito/imagens/excerto-ca-leisdoCibercrime1.pdf, consultado a 03.01.2018.

Hiperligações

Sistema de Informação do Ministério Público

3.

Apreensão, exame ou perícia, e utilização processual de meios de prova existentes em material informático (documentos, correio eletrónico, memorandos pessoais, fotografias, registos, áudio, etc.). Enquadramento jurídico, prática e gestão processual

Marta Saúde

CENTRO
DE ESTUDOS
JUDICIÁRIOS

3. APREENSÃO, EXAME OU PERÍCIA, E UTILIZAÇÃO PROCESSUAL DE MEIOS DE PROVA EXISTENTES EM MATERIAL INFORMÁTICO (DOCUMENTOS, CORREIO ELECTRÓNICO, MEMORANDOS PESSOAIS, FOTOGRAFIAS, REGISTOS ÁUDIO ETC…). ENQUADRAMENTO JURÍDICO, PRÁTICA E GESTÃO PROCESSUAL

Marta Saúde

I. Introdução

As novas tecnologias de informação e comunicação, ao trazerem novas formas de interacção, despoletaram uma evolução radical no desempenho das actividades quotidianas das pessoas e das instituições, invadindo quase todos os domínios da sociedade, designadamente político, social e económico.

A *Internet* desempenha um papel essencial no actual estádio de desenvolvimento da sociedade moderna, a denominada "*sociedade da informação*", caracterizada pela aquisição, tratamento e difusão de informação por via das redes de comunicação digitais – a informação encontra-se na disponibilidade de todos, à escala global.

Porém, o desenvolvimento tecnológico aliado à massificação da *Internet* potencia a sua instrumentalização para práticas ilícitas no ciberespaço, cujo combate e perseguição, em razão dessa imaterialidade e globalidade, apresenta inúmeras dificuldades e fragilidades, revelando-se um verdadeiro desafio para a investigação criminal.

A Lei n.º 109/2009, de 15 de Setembro (Lei do Cibercrime) erige-se como o primeiro diploma do ordenamento jurídico português a prever a recolha da prova digital, consagrando os meios de obtenção de prova digital disponíveis para a investigação da criminalidade informática.

Procede-se, assim, à análise desta temática, partindo das opções legislativas vigentes, nacionais e internacionais, tendo em conta as soluções doutrinárias e jurisprudenciais, com o desiderato de analisar as soluções processuais ao alcance da investigação criminal na repressão da criminalidade informática.

II. Objectivos

O presente trabalho, realizado no âmbito do 2.º Ciclo de Formação do 32.º Curso de Formação Normal de Magistrados, tem uma índole eminentemente teórico-prática, com vista à abordagem da temática em causa – os meios de obtenção de prova digital – em particular, do ponto de vista jurídico-penal, mas sem olvidar as concomitantes questões de cariz mais prático, em particular, no que à gestão processual concerne. Destina-se, em especial, aos colegas Auditores de Justiça, com vista propiciar o debate e uma reflexão mais aprofundada sobre a prova digital, esclarecendo quais os seus diplomas reguladores e eventuais questões práticas que se colocam no quotidiano dos Tribunais, com vista a, dentre os meios probatórios disponíveis na Lei do Cibercrime e considerando a finalidade visada pela investigação, adoptar a estratégia mais eficaz na condução do inquérito.

III. Resumo

Iniciaremos o nosso estudo com uma exposição geral e muito sumária do fenómeno da cibercriminalidade, designadamente o contexto em que surgiu, a sua evolução, a tentativa de aproximação ao conceito e desafios que se colocam no combate a este fenómeno.

Prosseguimos o estudo do tema com o conceito de prova digital, dos princípios que a regem, por referência a orientações internacionais, e a sua caracterização enquanto meio probatório, evidenciando as dificuldades que essas características acarretam para a investigação.

Posteriormente, como forma de encetar o enquadramento jurídico-processual desta temática, e em termos sintéticos, abordamos a evolução legislativa da prova digital, desde a sua origem no ordenamento jurídico-penal português, com menção dos principais instrumentos nacionais e internacionais que inspiraram o legislador nacional (com destaque para a Convenção do Cibercrime) e se mostraram impulsionadores do actual regime – a Lei n.º 109/2009, de 15 de Setembro (Lei do Cibercrime.)

Após, fazemos menção aos diplomas actualmente em vigor no direito interno, alertando para as dificuldades da sua conjugação e sobreposição, aludindo às dificuldades práticas.

Seguidamente, analisamos o enquadramento jurídico da prova digital, em termos genéricos e de um ponto de vista sistemático, fazendo uma viagem pela Lei do Cibercrime, com enfoque nas principais definições por si consagradas, dado revelarem-se elucidativas para a compreensão do tema que nos propomos estudar com o presente trabalho, sem descurar o elenco das disposições materiais de direito penal nela previstas.

Depois, seguimos para o principal objecto do presente trabalho, iniciando a análise das disposições de âmbito processual consagradas na Lei do Cibercrime e elencando, com a profundidade possível, os meios de obtenção de prova digital aí expressamente consagrados, ao dispor da investigação criminal, procurando demonstrar as diferenças existentes entre os referidos meios de prova, por forma a determinar qual o meio mais indicado em face do problema prático suscitado.

Assim, analisamos a preservação expedita de dados (artigo 12.º), a revelação expedita de dados de tráfego (artigo 13.º), a injunção para apresentação ou concessão do acesso a dados (artigo 14.º), a pesquisa de dados informáticos (artigo 15.º), a apreensão de dados informáticos (artigo 16.º), a apreensão de correio electrónico e registos de comunicações de natureza semelhante (artigo 17.º), a intercepção de comunicações (artigo 18.º) e as acções encobertas (artigo 19.º), todos consagrados na Lei do Cibercrime (Lei n.º 109/2009, de 15 de Setembro).

Por último, mas não menos importante, considerando a internacionalização do fenómeno "*cibercrime*" e o consequente desafio que coloca às autoridades judiciárias no plano internacional, fazemos uma breve incursão pelas medidas específicas no domínio da cooperação internacional em matéria de obtenção de prova digital e consagradas, especificamente, nos artigos 20.º a 26.º da Lei do Cibercrime.

1. A Cibercriminalidade

O desempenho das nossas actividades quotidianas tem experienciado uma evolução radical com o aparecimento das novas tecnologias de informação e comunicação, que, associadas ao fenómeno da globalização, monopolizam quase todos os domínios da sociedade, impulsionando mudanças políticas, sociais e económicas.[1]

A *Internet* assume um papel fundamental no desenvolvimento da sociedade. Contudo, apesar de poder ser utilizada de maneira inócua, potencia, paralelamente, o livre desenvolvimento da prática de actos ilícitos, que atentam contra as pessoas, o património, a própria estrutura organizativa da sociedade, a liberdade sexual, a honra, entre outros. Deve, por isso, ser vista

[1] MONGE CALLEJA, Álvaro Manuel, "*A dimensão virtual vinculada à chamada «Era Digital» é pensada por alguns autores como o produto da matização de uma modernização simples para uma reflexiva, em que a sociedade se vê regulada por uma rede nevrálgica – Internet – perante a qual mantém uma posição reticente face à sua potencial bipolaridade*." CALLEJA, Álvaro Manuel Monge, *A Investigação criminal face à globalização e o cibercrime*, Investigação Criminal, Lisboa, Nº 11 (Fevereiro 2017), pp. 172 e 173.

como uma espada de dois gumes[2], pois a informação passou a ser também o centro de muitos receios.

Enquanto plataforma intrincada, a *Internet* mostra-se muito favorável à invisibilidade da identidade individual e colectiva, onde o fluxo constante e convergente de conteúdos, o uso se *softwares* e a incorporeidade, a transformam numa arma silenciosa, com efeitos devastadores à escala mundial.

No que à cibercriminalidade concerne, as novas tecnologias da informação e comunicação trazem não só novos instrumentos para a prática de crimes já conhecidos, como novas realidades, que no entendimento dos Estados merecem dignidade penal. Assim, as especificidades da criminalidade informática colocam-se tanto na "*transferência de comportamentos ilícitos para o ambiente digital, como na tipificação de novos crimes com elementos caracterizadores de natureza digital.*"[3]

As práticas informáticas potenciam, pois, uma exponencial internacionalização da criminalidade e simultaneamente, tornam árdua a tarefa da reconstituição do percurso das informações entre o emissor e o receptor, permitindo a dissimulação de actos e agentes criminosos.[4]

Ora, este facilitismo tem proporcionado uma "*deslocação criminosa para a Internet*", levando as pessoas a encetar a prática de actividades criminosas que, possivelmente, por outros meios não praticariam e, por outro lado, é muito simples transferir a informação para outro ponto na *Internet*, caso as autoridades descubram esse ponto da Internet e o encerrem.

Adicionalmente, este desenvolvimento alucinante do mundo virtual propicia o desenvolvimento de novas técnicas de dissimulação ou ocultação, em ordem a impedir ou dificultar a identificação do autor das actividades criminosas pelas autoridades.

Relativamente ao conceito de criminalidade informática, GARCIA MARQUES e LOURENÇO MARTINS alertam para a inexistência de um conceito expressamente consagrado na legislação, mas ainda assim avançam que "*é frequente encarar a criminalidade informática como todo o acto em que o computador serve de meio para atingir um objectivo criminoso ou em que o computador é o alvo simbólico desse acto ou em que o computador é objecto de crime".*

No entendimento de PEDRO DIAS VENÂNCIO, "*em sentido amplo, a criminalidade informática englobará toda a panóplia de actividade criminosa que pode ser levada a cabo por meios informáticos, ainda que estes não sejam mais que um instrumento para a sua prática, mas que não integra o seu tipo legal, pelo que o mesmo crime poderá ser praticado por recurso a outros*

[2] *Idem*.
[3] DIAS VENÂNCIO, Pedro, *Lei do Cibercrime: Anotada e Comentada*, Coimbra Editora, Coimbra, 2011, pp. 14 e 15.
[4] Nas palavras de MONGE CALLEGA "*O delito online – ou cibercrime – deve ser concebido como uma acção legalmente indevida, semelhante às realizadas tradicionalmente, mas embebidas num marco etéreo e volúvel, o Ciberespaço. Entre os aspectos que beneficiam a produção do ciberdelito, encontramos: 1) o número de usuários; 2) o anonimato; 3) a distribuição indiscriminada e veloz de dados; 4) a desnecessária confluência entre sujeitos; e 5) a localização global e a ausência de autoridades dissuasoras*", *in* ob. cit., p. 175.

meios. Em sentido estrito, (…) a criminalidade informática abarcará apenas aqueles crimes em que o elemento digital surge como integrador do tipo legal ou mesmo como seu objecto de protecção."[5]

É este contexto de inovação tecnológica, com a inerente dificuldade estatal no acompanhamento deste processo evolutivo, que tem proporcionado uma generalizada desadequação da resposta do direito e do processo penal no combate eficaz ao fenómeno da criminalidade informática, em especial pelo facto de as normas legais assentarem na territorialidade e na materialidade da prática dos crimes, o que não se coaduna com a natureza transfronteiriça e virtual dos actos praticados na *Internet*. Essa dificuldade é, aliás, extensível à generalidade dos países ocidentais.

1.1. Os conceitos de Prova digital, princípios e as dificuldades colocadas pela sua natureza

Na senda do que se vem discorrendo relativamente ao desenvolvimento da tecnologia e com a diversidade de meios técnicos ao dispor com vista ao cometimento de crimes informáticos, tem de se imprimir aos actos da investigação uma constante evolução e capacidade de adaptação, com o desenvolvimento dos instrumentos investigatórios.

Dada a relativa novidade do tema, poucos têm sido os autores que se comprometem com uma noção do conceito de prova digital. BENJAMIM SILVA RODRIGUES, descreve a prova digital como "*qualquer tipo de informação, com valor probatório, armazenada em repositório electrónico-digital de armazenamento, ou transmitida em sistemas e redes informáticas ou redes de comunicações electrónicas, privadas ou publicamente acessíveis, sob a forma binária ou digital*"[6]. Já ARMANDO DIAS RAMOS classifica a prova digital como a "*informação passível de ser extraída de um dispositivo electrónico (local, virtual ou remoto) ou de uma rede de comunicações. Pelo que esta prova digital para além de ser admissível, deve ser também autêntica, precisa e concreta*".

Apesar do impacto na determinação dos *standards* caracterizadores da prova digital, são inúmeras as dificuldades sentidas na investigação, em razão da sua enorme complexidade técnica, e consequente necessidade interpretação especializada.

O investigador, no processo de recolha da prova digital deve considerar a sua natureza *efémera*, caracterizada pelo seu período curto de conservação no dispositivo electrónico-digital, devendo agir de forma célere e cumprir todos os trâmites necessários em ordem a que a mesma não perca a sua integridade. O investigador deve igualmente observar a sua *fragilidade* e *alterabilidade*, o que lhe impõe, antes da recolha, a identificação do concreto tipo de prova digital em causa. Importa igualmente frisar a sua natureza *volátil* e *instável*, adveniente da sua mutabilidade, o que dificulta a apreensão da mesma, pois inicialmente apresenta determinadas características que, mais tarde, parcial ou totalmente, se alteram, exigindo-se uma investigação estruturada temporalmente.

[5] DIAS VENÂNCIO, Pedro, ob. cit., pp. 16 e 17.
[6] *Idem*, p. 17.

Ademais, a prova digital consiste numa prova *imaterial*, o que acarreta ao investigador o conhecimento de técnicas específicas.

A *complexidade* e a *codificação* são também caracterizadoras da prova digital, o que exige ao investigador o domínio do máximo de técnicas e conhecimentos científicos.

Acresce que em muitas das situações, a investigação se depara com o carácter *disperso* da prova digital, que poderá encontrar-se distribuída por vários terminais, computadores e redes, abrangendo uma vasta área geográfica.

Em Outubro de 1999 realizou-se em Londres o *International Hi-Tech Crime and Forensic Conference*, e o *Scientific Working Group on Digital Evidence* apresentou algumas definições, princípios e *standards* de relevo, com o intuito de apresentar à comunidade forense internacional a natureza da prova digital e todo o percurso investigatório a seguir, com vista a salvaguardar o valor probatório da mesma.

À prova digital serão aplicáveis, naturalmente, todos os procedimentos e regras que se aplicam aos demais tipos de prova, com respeito pelo princípio da cumulação dos *princípios probatórios do processo penal e da investigação forense*.

Acresce que a prova digital deve respeitar o *princípio de não alteração no acto de recolha*, por forma a garantir a sua integridade no acto de recolha, armazenamento e tratamento, exigindo-se ao investigador que se abstenha de praticar qualquer conduta susceptível de contaminar os dados obtidos.

Releva igualmente o *princípio da especialização ou qualificação do pessoal adstrito à investigação forense digital*. O acesso, recolha, conservação e análise, competem a pessoal especializado, dotado dos conhecimentos técnicos necessários para o efeito, salvaguardando a sua posterior admissibilidade.

Destaca-se, do mesmo modo, o *princípio da garantia da documentação em todas as fases processuais (acesso, recolha, armazenamento, transferência, preservação e apresentação ou repetição da prova digital).* Ou seja, todo o processo de obtenção e tratamento da prova digital deverá ser exaustivamente documentado e preservado para futura auditoria e revisão, uma vez que só através da "*reversão dinâmica*" se torna possível repetir a prova, razão pela qual impende sobre os investigadores descrever de forma detalhada os resultados obtidos na fase anterior.

Salientamos também o *princípio da responsabilidade pessoal,* uma vez que cada investigador que interage com a prova digital ao longo da sua cadeia é responsável pelas suas acções e omissões. É devido ao carácter tendencialmente pessoal conferido à investigação que leva a que a prova seja recolhida, manuseada e analisada por peritos tecnicamente qualificados e cuja identificação constará no processo.

Por último, o princípio que rege a prova digital é o da *responsabilização repartida dos vários intervenientes na produção da prova no respeito dos princípios forenses digitais.* Cada organismo incumbido da apreensão, acesso, armazenamento ou transporte da prova digital ao longo da sua cadeia da prova é responsável pelas suas acções e omissões sobre esta, assegurando assim, complementar e cumulativamente, o valor probatório da prova objecto da investigação forense digital.

Em suma, com vista a salvaguardar a integridade da prova digital recolhida no decurso do processo de investigação, cumprirá aos investigadores observar estes princípios obrigatórios, em todas as fases processuais, por forma a garantir a sua admissibilidade legal no processo[7].

1.2. Evolução legislativa em matéria de prova digital

O fenómeno da prova digital tem sido introduzido paulatinamente no nosso ordenamento jurídico-penal e os avanços mais significativos devem-se, essencialmente, ao contributo europeu.

O pleno exercício de direitos e liberdades dos cidadãos esteve na origem da criminalidade informática, tendo sido "*associado à questão da compatibilização do direito dos cidadãos exercerem as suas liberdades e de verem respeitados os seus direitos, nomeadamente de privacidade, com a necessidade da sociedade recolher informações acerca dos indivíduos que a compõem, com vista ao seu melhor funcionamento e segurança*".[8] O artigo 35.º da Constituição da República Portuguesa consagrou, de forma expressa, a protecção das pessoas contra o tratamento informático de dados pessoais, salvaguardando o direito de acesso dos cidadãos aos seus dados pessoais registados em sistemas informáticos e proibindo o tratamento informático de dados pessoais específicos, como convicções políticas, fé religiosa ou vida privada.[9]

Esta matéria apenas foi regulamentada no direito interno em 1991, pela Lei n.º 109/91, de 17 de Agosto, o primeiro diploma que consagra a tipificação da cibercriminalidade, na sequência da Recomendação n.º R (89) do Conselho da Europa, acolhendo todos os tipos legais nela consagrados, com excepção da burla informática, já prevista no Código Penal. Do ponto de vista sistemático, o legislador optou por uma divisão em três capítulos: princípios gerais, a tipificação criminal e um capítulo atinente às penas acessórias, abstendo-se, contudo, de regulamentar os aspectos processuais.

O primeiro instrumento de fundo sobre a criminalidade informática, no plano internacional, foi a "*Convenção sobre o Cibercrime*" do Conselho da Europa, adoptada em Budapeste, em 23 de

[7] ALBERTO GIL LIMA CANCELA, *A prova digital: os meios de obtenção de prova na Lei do Cibercrime*, Dissertação de Mestrado de especialização em Ciências Jurídico-Forenses na Universidade de Coimbra, 2016, pp. 21-25.
[8] DIAS VENÂNCIO, *ob. cit.*, p. 13.
[9] A revisão constitucional de 1982 introduziu algumas alterações à versão originária do artigo 35.º, das quais importa destacar, por um lado, a proibição do acesso a terceiros de ficheiros com dados pessoais e a proibição da interconexão de dados pessoais informatizados e, por outro, a remissão para a lei ordinária da definição do conceito de "*dados pessoais*" para efeitos de registo informático.

Novembro de 2001, elaborada por um comité de peritos internacionais[10]. Sendo certo que teve na sua origem os países membros do Conselho a Europa, a sua vocação é universal.

A "*Convenção sobre o Cibercrime*", enquanto primeiro tratado internacional sobre a criminalidade no ciberespaço, teve como desiderato a harmonização das várias legislações nacionais, mediante a delimitação dos conceitos jurídico-informáticos, promovendo a implementação de medidas de cooperação internacional de combate à criminalidade informática, com a tipificação de cibercrimes e a consagração de medidas processuais de obtenção de prova digital, com vista a simplificar os mecanismos de investigação criminal nesta matéria[11] [12]. Assim, a Convenção consagra disposições de direito penal material[13], inclui medidas processuais e de cooperação judiciária internacional.

No âmbito da União Europeia, merece destaque a Decisão-Quadro n.º 2005/222/JAI, do Conselho, de 24/02, relativa a ataques contra sistemas de informação, que, na esteira da "Convenção sobre o Cibercrime", visou harmonizar as legislações dos Estados-membro neste domínio, uma vez que a "*As consideráveis lacunas e diferenças entre as legislações dos Estados-Membros neste domínio podem entravar a luta contra a criminalidade organizada e o terrorismo e podem dificultar uma cooperação policial e judiciária eficaz no âmbito de ataques contra os sistemas de informação*."[14]

Conforme acima já aludimos, estes avanços no reforço do combate à cibercriminalidade foram cautelosos e compatibilizados com a defesa dos direitos e liberdades individuais, questão que foi sempre ponderada pela União Europeia. A este nível, não podemos deixar de fazer menção à Directiva n.º 95/46/CE do Parlamento Europeu e do Conselho, transposta para o direito interno com a Lei n.º 67/1998 de 26/10 (Lei da Protecção de Dados Pessoais).

[10] Por deliberação CDPC/103/211196, datada de Novembro de 1996 foi constituído o Comité Europeu para os Problemas Criminais (CDPC), integrado por especialistas em cibercriminalidade, que, partindo da análise das Recomendações nº (89) 9 e (95) 13, ficaria responsável pela elaboração de um instrumento internacional vinculativo, eficaz no combate a este novo fenómeno, que só viria a ser adoptado em 2003.

[11] VERDELHO, Pedro, "*A Convenção sobre Cibercrime do Conselho da Europa – Repercussões na Lei Portuguesa*", Direito da sociedade da informação, Coimbra Editora, 2006. - Vol. 6. - 257-276, p. 258. Veja-se ainda, sobre este aspecto, LOPES MILITÃO, Renato, *A propósito da prova digital no processo penal*, ROA, 2012 (Ano 72), nº 1, pp. 247-283.

[12] O Preâmbulo da Convenção estabelece como seus objectivos "*impedir os actos praticados contra a confidencialidade, integridade e disponibilidade de sistemas informáticos, de redes e de dados informáticos, bem como a utilização fraudulenta desses sistemas, redes e dados, prevendo a criminalização desses comportamentos, tal como se encontram descritos na presente Convenção, e a criação de competências suficientes para combater eficazmente essas infracções, facilitando a detecção, a investigação e a acção penal relativamente às referidas infracções, tanto ao nível nacional como ao nível internacional, e adoptando medidas que visem uma cooperação internacional rápida e fiável*" Diário da República, 1.ª série — N.º 179 — 15/9/2009, disponível em https://dre.pt/application/dir/pdf1sdip/2009/09/17900/0635406378.pdf, acedido em 13.02.2018.

[13] A nível sistemático, as infracções organizam-se em quatro núcleos: as infracções relativas à privacidade e integridade de sistemas informáticos, onde se integram os crimes de acesso ilegítimo (art. 2.º) e intercepção ilegítima (art. 3.º), infracções relativas a computadores, que incluem os crimes de falsidade informática (art. 7.º) e burla informática (art. 8.º), infracções relativas ao conteúdo, onde apenas se tipificou o crime de pornografia infantil (art. 9.º) e um crime respeitante à protecção dos direitos de autor e direitos conexos (art. 10.º). Na globalidade, os tipos legais nela consagrados já se encontravam previstos pela lei portuguesa (Lei n.º 109/91, de 27 de Agosto). Porém, as medidas processuais e a cooperação judiciária internacional são novidade.

[14] Decisão-Quadro nº 2005/222/JAI do Conselho, de 24/2, disponível em http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32005F0222 e acedido a 13.02.2018.

Nesta matéria, nas questões relacionadas com o cibercrime, assume especial relevo a Lei n.º 41/2004, de 18 de Agosto (Lei de Protecção de Dados Pessoais nas Telecomunicações) alterada pela Lei n.º 46/2012, de 29 de Agosto, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas. Incumbindo ao Estado a garantia do exercício dos direitos, liberdades e segurança dos seus cidadãos, estipulou-se no referido diploma que os dados de tráfego relativos aos utilizadores de empresa que disponibilizam serviços de comunicações electrónicas os eliminem ou tornem anónimos logo que se mostrem desnecessários para a facturação dos assinantes e pagamentos de interligações. Quer tal significar que sempre foi uma preocupação do Estado a garantia da liberdade, segurança e privacidade, inclusivamente nos casos em que as tecnologias de informação e comunicação se encontram instrumentalizadas para fins associados à cibercriminalidade.

Merece ainda destaque, no plano internacional, a Directiva n.º 2006/24/CE do Parlamento Europeu e do Conselho, de 15/3, cuja transposição para o ordenamento jurídico português veio a ocorrer pela Lei n.º 32/2008, de 17/7 (Lei da Conservação de Dados Gerados ou Tratados no Contexto Oferta de Serviços de Comunicações Electrónicas), reportada à conservação de dados nas comunicações electrónicas. Este diploma consagrou o prazo de um ano a contar da data da conclusão da comunicação para conservação dos referidos dados de tráfego, desde que tenham por finalidade a investigação, detecção e repressão de crimes graves pelas autoridades e que essa transmissão seja ordenada por despacho fundamentado do juiz. Conforme *infra* se exporá, esta é uma das leis complementares no âmbito da obtenção da prova digital.

2. As leis reguladoras da prova digital

Actualmente, os diplomas reguladores da prova digital, a considerar pelo Ministério Público, são os que doravante se indicam:

- "Convenção sobre o Cibercrime", adoptada em Budapeste em 23 de Novembro de 2001 (DR 1.ª S - 15.09.2009);
- Directiva 2013/40/EU do Parlamento Europeu e do Conselho de 12 de Agosto de 2013, relativa a ataques contra os sistemas de informação e que substitui a Decisão-Quadro 2005/222/JAI do Conselho;
- Lei n.º 109/2009, de 15 de Setembro (Lei do Cibercrime);
- Lei n.º 32/2008, de 17 de Julho (Conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas);
- Lei n.º 5/2004, de 10 de Fevereiro (Lei das Comunicações Electrónicas);
- Lei n.º 7/2004, de 7 de Janeiro (Comércio Electrónico no Mercado Interno e Tratamento de Dados);
- Lei n.º 41/2004, de 18 de Agosto (Protecção de dados pessoais);
- Lei n.º 67/98, de 26 de Outubro (Lei de Protecção de Dados Pessoais);
- Circular PGR n.º 12/2012 (Cibercrime - Uniformização de procedimentos – pedidos de informação dirigidos aos operadores de comunicações.)

Atendendo à economia de escrita do presente trabalho, conferimos especial enfoque à Lei n.º 109/2009, de 15 de Setembro (Lei do Cibercrime), ao Código de Processo Penal e à Lei n.º 32/2008, de 17 de Julho (Lei da Conservação de Dados Gerados ou Tratados no Contexto Oferta de Serviços de Comunicações Electrónicas). Pelo facto de a Lei do Cibercrime merecer maiores desenvolvimentos, por ora apenas abordaremos de forma muito sintética as duas últimas referidas.

Na verdade, o legislador, no âmbito do direito interno, ao invés de englobar toda a matéria num único diploma, como pareceria ser a lógica da "Convenção do Cibercrime", optou por manter a mesma realidade dividida em três diplomas legais diferentes[15].

Com efeito, a "*teia legislativa nacional é muito complexa*" e incoerente, dificultando em grande medida a tarefa do intérprete[16].

2.1. O Código de Processo Penal

No Código de Processo Penal com a actual redacção, no que à prova digital concerne, continua a verificar-se, no artigo 189.º, n.º 1, a extensão "*às conversações ou comunicações transmitidas por qualquer meio técnico diferente do telefone, designadamente correio electrónico ou outras formas de transmissão de dados por via telemática, mesmo que se encontrem guardadas em suporte digital, e à intercepção das comunicações entre presentes*." Adicionalmente, no seu artigo 189.º, n.º 2, regula-se a obtenção e junção aos autos de dados sobre a localização celular ou de registos de realização de conversações ou comunicações[17].

Com efeito, o artigo 189.º engloba realidades muito diferentes, carecidas de tutela e exigências distintas, o que causa um elevado grau de incerteza e insegurança jurídica. Em bom rigor, submeter ao mesmo regime investigatório das escutas telefónicas o *e-mail* guardado num computador, colocará necessariamente em causa a investigação criminal[18]. Na verdade e em última instância, uma visão meramente literal desta cláusula de excepção consagrada no artigo 189.º, n.º 1, do Código de Processo Penal, implicará que a crimes informáticos ou crimes como injúrias, coacção, devassa da vida privada, quando cometidos por meios informáticos, não sejam aplicáveis estes meios de investigação, pelo facto de não integrarem o catálogo de crimes preceituado no artigo 187.º, n.º 1, do Código de Processo Penal. Constata-se, pois, que

[15] Manifesta-se contra esta solução legal CONDE CORREIA, João, in "*Prova digital: as leis que temos e a lei que devíamos ter*", RMP, n.º 139 (Jul-Set. 2014), p. 29-59, p. 29 e 30. "*Esta trilogia, para além de acentuar o atual paradigma da descodificação e de negar a desejável centralidade normativa do Código de Processo Penal, contribui para a assimetria, para a incoerência das soluções legais e, sobretudo, para o seu indesejável e nefasto insucesso prático. A prova digital – essencial no mundo hodierno – continua mergulhada num verdadeiro pântano prático e, sobretudo, normativo, que só poderá ser superado mediante uma intervenção legislativa coerente, global e, cientificamente, sustentável*".

[16] *Idem*, p. 30.

[17] COSTA ANDRADE denominou este norma de "*casa dos horrores hermenêuticos*", *apud*, CONDE CODDEIA, João, p. 32.

[18] *Idem*. Nas palavras de COSTA ANDRADE, "(…) *o preceito veio onerar e dificultar desmesuradamente a investigação criminal, assegurando a estes documentos uma tutela mais consistente do que a oferecida pelo regime das buscas ,regime a que, em princípio, seriam (e deviam) ser submetidas as intromissões nestes "documentos", não fora o gesto menos pensado do legislador de 2007 a aditar o inciso "mesmo que se encontrem guardados em suporte digital.*"

estamos perante uma disposição extremamente restritiva e que origina um obstáculo processual na investigação.

2.2. A Lei n.º 32/2008, de 17 de Julho

Apesar da revisão do Código de Processo Penal, com a Lei n.º 48/2007, de 29 de Agosto, o legislador nacional apenas procedeu à transposição para o direito interno da mencionada Directiva n.º 2006/24/CE, do Parlamento e do Conselho[19], por via da Lei n.º 32/2008, de 17 de Julho, reguladora da conservação e transmissão dos dados de tráfego e localização[20], com identificação do utilizador registado, pelo facto de estes constituírem um "*instrumento extremamente importante e útil na prevenção, investigação, detecção e de repressão de infracções penais, em especial contra a criminalidade organizada*"[21].

De acordo com o preceituado no artigo 9.º, n.os 1 e 2, da Lei n.º 32/2008, de 17 de Julho, a transmissão de dados apenas é admissível apenas quanto a um catálogo restritivo de crimes, mediante despacho fundamentado do juiz e quando houver razões para crer que são indispensáveis para a descoberta da verdade ou para a prova daqueles crimes e que esta será de outra forma impossível ou muito difícil de obter, devendo respeitar os princípios da adequação, necessidade e proporcionalidade.

Ou seja, o legislador apesar de ter criado este regime especial com a Lei n.º 32/2008, como manteve inalterados os requisitos de acesso consagrados no Código de Processo Penal, duplicou os regimes.[22]

[19] Conforme resulta do considerando (9) da Directiva, diz-se que "*a conservação de dados se tem revelado um instrumento de investigação necessário e eficaz de repressão penal em vários Estados-Membros, nomeadamente em matérias tão graves como o crime organizado e o terrorismo, é necessário assegurar que as autoridades responsáveis pela aplicação da lei possam dispor dos dados conservados por um período determinado.*"

[20] Quanto a este ponto cumpre realçar a Nota Prática n.º 7/2015, de 30 de Dezembro de 2015, emitida pelo Gabinete do Cibercrime, sobre a discussão jurídica, em Portugal e na Europa, a propósito da obrigação de os operadores de comunicações procederem à retenção de dados, questão esta levantada no âmbito do Acórdão do Tribunal de Justiça da União Europeia de 8 de Abril de 2014, sendo que no caso português está em causa ponderar se está em vigor, ou não, a Lei n.º 32/2008 de 17 de Julho, consultável em https://simp.pgr.pt/destaques/mount/anexos/4564_nota_pratica_7___retencao_de_dados.pdf

[21] *Vide* Considerando (7) da Directiva.

[22] Apresentando críticas a esta solução legal, veja-se CONDE CORREIA, *ob. cit.*, "*O legislador podia (e devia) ter mantido a centralidade normativa do Código de Processo Penal. Uma coisa é a conservação preventiva dos dados; outra coisa, bem diferente, a sua aquisição e valoração processual penal, desencadeada pela suspeita da prática de um crime.*", pp. 35 a 37.

2.3. A conjugação dos diplomas[23]

Esta regulação dispersa da mesma realidade gera, naturalmente, desafios ao nível da interpretação e da aplicação legislativas, existindo múltiplos exemplos de dificuldade na articulação dos três diplomas legais. *"A sua diferente localização geográfica na geografia processual penal, a diversidade dos objectivos enunciados e heterogeneidade das técnicas utilizadas propiciam equívocos, esquecimentos e exegeses incorrectas"*[24].

No que tange à articulação da legislação geral com a legislação extravagante, parece-nos que o artigo 189.º do Código de Processo Penal foi revogado, primeiro pela Lei n.º 32/2008 e depois pela Lei n.º 109/2009.[25]

Relativamente às relações entre a Lei n.º 32/2008 e a Lei n.º 109/2009, a doutrina diverge.

Para uns, a Lei do Cibercrime revogou o regime estabelecido pela Lei n.º 32/2008, de acesso àqueles dados, apenas subsistindo quanto ao "*estabelecimento dos deveres dos fornecedores de serviços e prestação desses dados*"[26]. Para DÁ MESQUITA, só esta interpretação é coerente, considerando o disposto no artigo 11.º, n.º 2, da Lei n.º 109/2009, o que significa que o âmbito de aplicação da Lei n.º 32/2008 se cinge apenas ao que não se encontre regulado, de forma expressa, pela Lei do Cibercrime.

Em sentido diverso, outros autores, dentre os quais RITA CASTANHEIRA NEVES, BENJAMIM SILVA RODRIGUES e RENATO LOPES MILITÃO, pronunciam-se no sentido estar subjacente dos dois regimes uma relação de complementaridade, tendo sido esta a interpretação que o legislador visou imprimir ao mencionado artigo 11.º, n.º 2, da Lei n.º 109/2009[27]. Caberia, pois, ao intérprete, delimitar o seu âmbito de aplicação[28] [29].

---

[23] Revela-se muito útil, quanto a esta questão, a Nota Prática n.º 8/2016, de 18 de Fevereiro de 2016, elaborada pelo Gabinete do Cibercrime, que apresenta uma descrição sumária das informações guardadas por operadores de comunicações (telefónicas e Internet) que podem vir a ser usadas em investigações criminais, bem como referencia os fundamentos jurídicos que delimitam os pedidos dessas informações https://simp.pgr.pt/simp_tematicos/documentos/mount/files/1456403096_2016_02_20_nota_pratica_8_pedido_de_info_a_isp.pdf

[24] *Idem*.

[25] Assim, veja-se CONDE CORREIA, João, "*As leis extravagantes sobrepõem-se àquele regime geral, que só subsiste naquilo que não foi depois especialmente regulado. Não se compreende, por isso, porque é que o legislador não o revogou formalmente, expurgando-o daquilo que não tem aplicação e impedindo que se continue a invocar a sua vigência. A sua manutenção formal só pode ser perniciosa*.", ob. cit., p. 37. No mesmo sentido, pronunciam-se PAULO DÁ MESQUITA e CASTANHEIRA NEVES, Rita, *As ingerências nas comunicações electrónicas em processo penal*, Coimbra, Coimbra Editora, 2011, p. 280. Em sentido contrário, PINTO DE ALBUQUERQUE, Paulo, *Comentário do Código de Processo Penal*, Lisboa, UCE, 2011, p. 549.

[26] CONDE CORREIA, Paulo, ob. cit, p. 36.

[27] CASTANHEIRA NEVES, Rita, *in* ob. cit., p. 234 e seguintes.; SILVA RODRIGUES, Benjamim, *apud*, CONDE CORREIA, p. 37, e LOPES MILITÃO, Renato, *in* ob. cit., p. 275.

[28] A este propósito, importa chamar à colação a Portaria n.º 469/2009, de 6 de Maio, com a redacção da Portaria n.º 694/2010, de 16 de Agosto, que estabelece os termos das condições técnicas e de segurança em que se processa a comunicação electrónica para efeitos da transmissão de dados de tráfego e de localização relativos a pessoas singulares e a pessoas colectivas, bem como dos dados conexos necessários para identificar o assinante ou o utilizador registado.

[29] Como bem refere CONDE CORREIA, João, *in ob. cit*., p. 37, "*A guarda e a conservação dos dados de tráfego e de localização, bem como dos dados conexos necessários para identificar o assinante ou o utilizador registado, para fins de investigação destes e repressão de crimes graves, independentemente de um qualquer pedido das autoridades oficiais e, mesmo, de uma qualquer suspeita da prática de um crime, justificará maior dificuldade e*

Face ao exposto, impõe-se concluir que as Leis n.os 32/2008 e 109/2009 revogaram parcialmente o regime do Código de Processo Penal. Porém, estes regimes especiais convocam frequentemente a aplicação do regime geral[30], pelo que o aplicador do direito, na sua tarefa interpretativa, se vê obrigado a articular os três diplomas, com vista à resolução do caso concreto.

3. A Lei do Cibercrime. Generalidades

Várias foram as vozes que se insurgiram no sentido da desadequação da Lei da Criminalidade Informática, em vigor desde 1991, quer pelo desenvolvimento da criminalidade, quer pelo despoletar de novas e mais eficazes formas de repressão.

A nova Lei do Cibercrime, aprovada pela Lei n.º 109/2009, de 15 de Setembro, veio revogar a Lei n.º 109/91 de 17 de Agosto e foi responsável pela transposição para o direito interno da Decisão-Quadro n.º 2005/222/JAI do Conselho e adaptou-o à Convenção sobre o Cibercrime do Conselho da Europa. Este diploma não se cingiu a uma revisão dos tipos legais substantivos previstos na Lei do Cibercrime de 1991, na medida em que introduziu novos meios de investigação e obtenção de prova específicos no âmbito da criminalidade informática.

A principal influência deste novo diploma foi o texto da Convenção sobre o Cibercrime, sendo que esta, apesar de ter sido adoptada em 2001, apenas foi ratificada pelo Estado português em 2009, datando a sua publicação precisamente do mesmo dia da publicação da Lei n.º 109/2009, de 15 de Setembro.

O legislador nacional, ao invés de alterar as fontes normativas vigentes em matéria de cibercriminalidade optou, assim, por criar um diploma extravagante, de aplicação geral, abrangendo normas penais materiais, normas penais processuais e disposições de cooperação internacional num único diploma. Ao sobrepor-se ao regime estabelecido pela Lei n.º 32/2008, relativo ao acesso aos dados gerados e tratados relativamente a comunicação electrónicas, acentuou a confusão interpretativa.

No catálogo das disposições penais materiais, o legislador consagrou a falsidade informática (artigo 3.º), o dano relativo a programas ou outros dados informáticos (artigo 4.º), a sabotagem informática (artigo 5.º), o acesso ilegítimo (artigo 6.º), a intercepção ilegítima (artigo 7.º) e a reprodução ilegítima de programa protegido (artigo 8.º), deixando de fora a devassa por meio de informática (artigo 193.º do Código Penal) e a burla informática (artigo 221.º do Código Penal.) Apesar da denominação "*do Cibercrime*", as disposições processuais nela estipuladas, conforme resulta da leitura do artigo 11.º, aplicam-se tanto aos crimes supra referidos (crimes informáticos *stricto sensu*), como aos crimes cometidos por meio de sistema informático e também aos crimes em que seja necessário proceder à recolha de prova em

cuidado no acesso a essa informação. Quanto maior for o acervo de informação sensível existente, maior deverá ser o cuidado no seu acesso. Já que o legislador impõe a conservação preventiva destes dados, ao menos que restrinja a possibilidade da sua utilização apenas aos casos que um juiz (independente e imparcial) considere indispensáveis."

[30] Veja-se os artigos 15.º, nos 4 al. b), e 6, 16.º, n.os 5 e 6, 17.º, 18.º, n.os 1, al. b) e 4, 19.º e 28.º da Lei n.º 109/2009, de 15 de Setembro.

suporte electrónico. Daqui se extrai que, em matéria de prova, espelhada no Capítulo III, a Lei do Cibercrime é trave mestra, consagrando a preservação expedita de dados (artigo 12.º), a revelação expedita de dados de tráfego (artigo 13.º), a injunção para a preservação ou concessão de acesso a dados (artigo 14.º), a pesquisa de dados informáticos (artigo 15.º), a apreensão de dados informáticos (artigo 16.º), a apreensão de correio electrónico e de registos de comunicações de natureza semelhante (artigo 17.º), a intercepção de comunicações (artigo 18.º), as acções encobertas (artigo 19.º), e, por último, a cooperação internacional (artigos 20.º a 26.º).

Com a nova Lei do Cibercrime, o legislador nacional consagrou "*um verdadeiro sistema processual de prova digital*"[31], dotando a prova digital de maior eficácia e satisfazendo as exigências internacionais.

Todavia, o Código de Processo Penal nunca foi adaptado ao desenvolvimento conseguido pela consagração deste regime geral da prova digital, previsto em legislação extravagante. Assim sendo, para o espaço físico manteve-se a aplicação da lei processual penal, integrando apenas esse campo o regime das escutas telefónicas, previsto no artigo 189.º do Código de Processo Penal, aplicável a todas as comunicações transmitidas por meio diverso de telefone ou guardado em suporte digital.

4. Os conceitos previstos pela Lei do Cibercrime. Definições

A Lei do Cibercrime consagra, no seu artigo 2.º, um elenco de definições legais, técnica legislativa recorrentemente adoptada pelo legislador para regulamentar aspectos relacionados com áreas dotadas de uma maior tecnicidade, designadamente relacionadas com a sociedade de informação[32].

De acordo com o disposto na alínea a), é sistema informático "*qualquer dispositivo ou conjunto de dispositivos interligados ou associados, em que um ou mais de entre eles desenvolve, em execução de um programa, o tratamento automatizado de dados informáticos, bem como a rede que suporta a comunicação entre eles e o conjunto de dados informáticos armazenados, tratados, recuperados ou transmitidos por aquele ou aqueles dispositivos, tendo em vista o seu funcionamento, utilização, protecção e manutenção*"[33].

À luz do disposto na alínea b), são dados informáticos, "*qualquer representação de factos*[34]*, informações ou conceitos sob uma forma susceptível de processamento num sistema*

[31] CONDE CORREIA, *ob. cit.*, p. 35.
[32] As definições elencadas nas al. a) a d) do artigo 2.º, resultam da transposição do disposto no artigo 1.º da Convenção sobre o Cibercrime, ainda que em termos não exactamente coincidentes.
[33] Este novo conceito de sistema informático visou substituir os conceitos de "rede informática" e de "sistema informático" consagrados, respectivamente, nas alíneas a) e b) do artigo 2.º da Lei n.º 109/91, que, face ao novo contexto tecnológico, se revelavam desactualizados. Esta nova definição de sistema informático, mais abrangente, permite a inclusão, para além dos clássicos computadores, de todos os dispositivos informáticos e comunicacionais, cujas funcionalidades são amplamente coincidentes com as funcionalidades dos computadores, como é o caso dos telemóveis.
[34] Designadamente fotografias, filmes, registos áudio.

informático, incluindo os programas aptos a fazerem um sistema informático executar uma função"[35].

Estipula a alínea c) o conceito de dados de tráfego, definindo-os como "*os dados informáticos relacionados com uma comunicação efectuada por meio de um sistema informático, gerados por este sistema como elemento de uma cadeia de comunicação, indicando a origem da comunicação, o destino, o trajecto, a hora, a data, o tamanho, a duração ou o tipo do serviço subjacente.*"[36] Desde já se refira que esta definição assume grande relevância, na medida em que os dados qualificados como "de tráfego" poderão se alvo de variadas medidas processuais no âmbito da investigação criminal, diversas das utilizadas para a obtenção de dados de conteúdo[37].

Fornecedor de serviço, nos termos do disposto na alínea d) do referido artigo 2.º, é "*qualquer entidade, pública ou privada, que faculte aos utilizadores dos seus serviços a possibilidade de comunicar por meio de um sistema informático, bem como qualquer outra entidade que trate ou armazene dados informáticos em nome e por conta daquela entidade fornecedora de serviço ou dos respectivos utilizadores.*"

[35] Como bem refere VERDELHO, Pedro, *A Nova Lei do Cibercrime*, Scientia Iuridica - Revista de Direito Comparado Português e Brasileiro, n.º 320, Outubro/Dezembro 2009, p. 719, "*É pacífico assumir que um programa informático é composto por dados informáticos, mas nem todos os dados informáticos integram um programa. Todavia, estes dados, que não consubstanciam um programa, podem também ser objecto de uma acção humana lesiva dos interesses de outrem, a qual merece tutela penal. Por isso, a lei optou por criar o conceito legal de dados informáticos, nele se incluindo o outro, ontologicamente de menor dimensão, de programa informático*."

[36] Muito crítico relativamente à incerteza doutrinal e jurisprudencial quanto à classificação do *Internet Protocol* (IP) como dado de base, acessível pelo Ministério Público, ou antes como um dado de tráfego, na disponibilidade exclusiva do juiz de instrução, pela ineficácia que imprime à investigação criminal, veja-se CONDE CORREIA, *ob. cit.*, p. 48 e 49. No entendimento do Autor, "*o acesso à Internet não é, de per si, uma qualquer forma de comunicação, que deva ser protegida pelo respectivo segredo, mas antes um passo prévio de conexão com uma rede global, que disponibiliza depois diversos tipos de comunicação (…) ou outras formas diversas de utilização*", pois que "*os endereços de IP dinâmicos não revelam um concreto utilizador, mas uma determinada utilização: eles são apenas um conjunto alargado de números, que, isoladamente, nada pode transmitir sobre o seu utilizador individual*". A sustentar a sua posição, invoca o Acórdão do TRL, datado de 19.06.2014, com o Processo n.º 1695/09.5PJLSB.L1-9, com a Relatora Margarida Vieira de Almeida, disponível para consulta em *dgsi.pt*.

[37] Esta definição apresenta-se contraditória com a definição da mesma expressão consagrada na lei de protecção de dados pessoais no âmbito das telecomunicações, aprovada pela Lei n.º 41/2004 de 18 de Agosto, uma vez que aí se definem os "dados de tráfego" como "*quaisquer dados tratados para efeitos do envio de uma comunicação através de uma rede de comunicações electrónicas ou para efeitos da facturação da mesma*" e os "dados de localização" como "*quaisquer dados tratados numa rede de comunicações electrónicas ou no âmbito de um serviço de comunicações electrónicas que indiquem a posição geográfica do equipamento terminal de um utilizador de um serviço de comunicações electrónicas acessível ao público.*" Ora, a Lei do Cibercrime inclui nos dados de tráfego, os dados que indiquem a *"origem da comunicação, o destino, o trajecto",* pelo que, no caso de tais dados indicarem a posição geográfica do equipamento informático, estamos perante dados que a Lei n.º 41/2004, de 18 de Agosto denomina de *"dados de localização".*

5. Disposições processuais da Lei do Cibercrime. Âmbito de aplicação

Conforme já aflorámos acima, a Lei do Cibercrime consagra normas de direito substantivo e também normas processuais.[38]

Dedica o seu artigo 11.º à definição do âmbito de aplicação das disposições processuais penais[39]. Resulta claro da leitura do artigo a extensão das disposições processuais, com excepção do disposto nos artigos 18.º e 19.º, em abstracto, a todos os tipos de crime, desde que cometidos por meio de sistema informático ou em relação aos quais seja necessário proceder à recolha de prova em suporte electrónico[40].

5.1. A preservação expedita de dados

O artigo 12.º da Lei do Cibercrime consagra a preservação expedita de dados, que se trata, nas palavras de PEDRO VERDELHO e em termos materiais, "*da possibilidade de autoridades judiciárias ordenarem a terceiros que procedam à preservação de dados informáticos que estejam na respectiva disponibilidade ou controle, sejam dados referentes a transmissões de dados informáticos ou dados meramente armazenados num sistema informático.*"[41] Portanto, o que se permite é apenas a preservação dos dados por quem tem o seu controlo, durante um certo período de tempo, e não a obtenção, pelas autoridades, dos dados informáticos.

Esta ordem de preservação, na medida em que apenas obstaculiza que informação relevante seja destruída e que pode, inclusivamente, ser emitida por órgão de polícia criminal, mais não é do que uma medida cautelar e destina-se, principalmente, aos fornecedores de serviço de *Internet*.[42]

Sendo certo que a obrigação geral de preservação de dados de tráfego imposta aos fornecedores de serviços e pelo período de um ano resultava já da Lei n.º 32/2008, a Lei do

[38] A Nota Prática n.º 6/2015, de 27 de Agosto de 2015, emitida pelo Gabinete do Cibercrime, mostra-se muito útil em matéria de prova digital, na medida em que apresenta as principais orientações jurisprudenciais nesta matéria, através da exemplificação com excertos de Acórdãos dos tribunais superiores, disponível para consulta em https://simp.pgr.pt/simp_tematicos/documentos/mount/files/1440687720_nota_pratica_6___jurispridencia_processual.pdf

[39] Esta norma não consagra qualquer novidade, uma vez que apenas reproduz, no direito interno, o artigo 14.º da Convenção do Cibercrime.

[40] Neste sentido, MESQUITA, Paulo Dá, "*Prolegómeno sobre prova electrónica e intercepção de telecomunicações no Direito Processual Penal português – o Código e a Lei do Cibercrime*", *in* Processo Penal, Prova e Sistema Judiciário, Coimbra, Coimbra Editora, p. 108 a 111, VERDELHO, Pedro, *ult. in* ob. cit., p. 734 "*o artigo 11.º estende o regime processual da Lei do Cibercrime a dois segmentos de criminalidade cuja investigação, na prática, somente será viável se puderem ser utilizados meios de prova especiais, como os utilizados na investigação da cibercriminalidade, independentemente de tais meios de prova poderem ou não, de acordo com as normas gerais do Código de Processo Penal, ser usados*". Ainda, DIAS VENÂNCIO, Pedro, *in* ob. cit., p. 91 "*Trata-se da criação de meios de obtenção de prova digitais para o combate da criminalidade, seja qual for a sua forma, atenta a generalização do uso de meios informáticos no dia-a-dia de cidadãos e de empresas, e a necessidade de adaptação dos meios de prova a essa realidade*".

[41] VERDELHO, Pedro, *ult. in* ob. cit., p. 735.

[42] Pode igualmente ser dirigida a qualquer pessoa que tenha controlo sobre sistema informático onde estão armazenados dados.

Cibercrime, no seu artigo 12.º, visou reforçar e complementar esta obrigação, estendendo-a a tipos de ilícitos que não se encontrem consagrados no catálogo da Lei n.º 32/2008 ou quanto a fornecedores não previstos naquela lei, como os bancos.[43] A diferença do regime previsto na Lei do Cibercrime no que concerne aos "dados preservados" relativamente à Lei n.º 32/2008 é precisamente o facto de servirem de prova no processo concreto em que a preservação foi ordenada, ao contrário do regime instituído pela Lei n.º 32/2008, na qual a preservação é feita por imposição legal e se destinam a ser utilizados apenas mediante intervenção judicial e na investigação de crimes graves.[44]

5.2. A revelação expedita de dados de tráfego

Prevê o artigo 13.º da Lei do Cibercrime a revelação expedita de dados de tráfego[45], meio cautelar de obtenção de prova e que consiste, essencialmente, como bem refere DAVID SILVA RAMALHO, em impor aos fornecedores de serviço, a *"divulgação dos dados de tráfego relativos a uma determinada comunicação, assim permitindo identificar, entre outros elementos, o trajecto percorrido pela comunicação*."[46]

Tendo em vista a preservação de dados, naturalmente, a sua revelação às autoridades judiciárias, estipula a Lei do Cibercrime, no seu artigo 13.º, a revelação expedita de dados de tráfego, que não se confunde nem com a injunção nem com a pesquisa informática, que adiante abordaremos.

Nas palavras de PEDRO VERDELHO esta figura *"pretende responder com eficácia e muita brevidade a uma necessidade premente de qualquer investigação nas redes de computadores: é sabido que uma determinada comunicação, por exemplo uma comunicação criminosa ou mal intencionada, nunca utilizará apenas o serviço de um fornecedor, indo pelo contrário atingindo o seu destino por via de vários fornecedores de serviços. Assim, a informação respeitante ao caminho que efectuou no seu percurso – os dados de tráfego, que não se confundem com os dados de conteúdo – vai ficando registada de forma repartida por vários fornecedores de serviço. Porém, quem investiga só vai sabendo progressivamente quem é o fornecedor de serviço que se segue no percurso da comunicação à medida que cada um destes fornecedores lhe vai dizendo de onde veio e para onde foi a comunicação que atravessou a sua rede ou usou os seus servidores. Portanto, o trabalho de reconstrução de um percurso informático, numa rede de comunicações aberta – por exemplo, a Internet – depende da gradual obtenção de informação sobre esse percurso e sobre o próximo destino, em cada uma das etapas percorridas*"[47].

[43] VERDELHO, Pedro, *in. ult.* ob. cit., p. 736.
[44] No artigo 3.º da Lei n.º 32/2008, refere-se a "investigação, detecção e repressão de crimes graves" e condiciona a utilização dos mencionados dados a autorização do juiz, por despacho fundamentado.
[45] Quanto à definição de "*dados de tráfego*", veja-se o já citado artigo 2.º, al. c), da Lei do Cibercrime.
[46] SILVA RAMALHO, David, *A investigação criminal na Dark Web*, Revista de concorrência e regulação, Almedina, n.º 14-15 (Abr.-Set. 2013), p. 398.
[47] VERDELHO, Pedro, *in ult.* ob. cit., p. 737.

Ora, a obtenção deste percurso, que poderá implicar a consulta a várias entidades, pode revelar-se morosa, com prejuízo para a eficácia da investigação. Assim sendo, torna-se necessário que a prestação de informação deste percurso seja expedita por parte de cada um dos servidores relativamente ao servidor que se segue, por forma a seguir o caminho da investigação. É precisamente com vista a ir ao encontro desta realidade que o artigo 13.º prevê a revelação expedita dos dados de tráfego pelos fornecedores de serviço às autoridades judiciárias ou aos órgãos de polícia criminal.

5.3. Injunção para apresentação ou concessão do acesso a dados

O artigo 14.º da Lei do Cibercrime consagra a injunção para apresentação ou concessão de acesso a dados, medida processual que não se confunde com as já referidas e previstas nos artigos 12.º e 13.º da Lei do Cibercrime[48] [49].

A razão de ser desta norma prende-se com complexidade dos sistemas informáticos, dotados de grande capacidade de armazenamento, características que tornam impossível ao investigador analisar todo o seu conteúdo. Assim, com vista a obviar a essa morosidade da selecção da informação relevante, consagrou o legislador o artigo 14.º da Lei do Cibercrime. Tem-se assim em vista, nessa tarefa investigatória, a obtenção da colaboração por parte de quem tem disponibilidade sobre o sistema. Ademais, importa não descurar que a falta de colaboração por parte de quem tem domínio sobre o sistema sempre pode frustrar a pesquisa de informação, quer pela possibilidade de ocultarem a informação, quer pelo bloqueio do acesso à mesma, designadamente por via da encriptação ou introdução de *passwords* no acesso a documentos.

Citando PEDRO VERDELHO, por referência ao artigo 14.º, n.º 1, da Lei do Cibercrime, traduz-se a injunção "*na ordem emitida por autoridade judiciária a quem tenha disponibilidade ou controlo sobre determinados dados informáticos, no sentido de que os comunique ao processo em causa, ou que permita o acesso aos mesmos*."[50] Esta ordem deverá especificar, de acordo com o circunstancialismo do caso concreto e das finalidades pretendidas, se o que se pretende é a comunicação dos dados ou antes o acesso aos mesmos. [51] [52]

[48] Esta norma processual resulta da transposição do dispositivo artigo 18.º da Convenção do Cibercrime.
[49] A injunção consiste num meio mais flexível e de menor intrusão nos direitos dos fornecedores de serviços, o que confere eficácia à investigação. Como se pode ler no ponto 167 do Relatório Explicativo da CCIBER, verificamos que "*Por vezes, os dados de tráfego ou, pelo menos, alguns tipos de dados de tráfego, são partilhados entre os fornecedores de serviços envolvidos na transmissão da comunicação, para fins comerciais, técnicos ou de segurança. (…) Cada um deles tem em sua posse uma parte do puzzle, e cada uma destas partes necessita de ser examinada de forma a detectar-se a sua origem ou o seu destino*".
[50] VERDELHO, Pedro, *in ult.* ob. cit., p. 738.
[51] Quanto a este ponto, designadamente a possibilidade de enquadramento do pedido de endereço de IP e identificação do seu utilizador aos operadores de comunicações no artigo 14.º da Lei do Cibercrime, veja-se a Nota Prática n.º 1/2012, emitida pelo Gabinete do Cibercrime da Procuradoria-Geral da República e disponível em https://simp.pgr.pt/simp_tematicos/documentos/mount/anexos/1358780904_2013_01_09_nota_pratica___pedido_de_ip.pdf.
[52] Veja-se ainda a Nota Prática n.º 2/2013, de 13 de Abril, emitida pelo Gabinete do Cibercrime, em https://simp.pgr.pt/simp_tematicos/documentos/mount/files/1365007943_2013_04_03_nota_pratica___jurisprudencia_sobre_ip.pdf "*De acordo com a jurisprudência predominante, o pedido a um operador de comunicações da*

A imposição de fornecer ao processo criminal tais dados necessários para a produção de prova é obrigatória, sendo que a recusa no fornecimento de informação por parte de quem tem disponibilidade ou controlo dos dados informáticos é punida por desobediência (*cfr*. artigo 14.º, n.º 1, *in fine*, da Lei do Cibercrime.)

Porém, o âmbito de aplicação da injunção é limitado. Em primeiro lugar, nunca pode ser dirigida a um suspeito ou arguido no processo em causa, conforme resulta do disposto no artigo 14.º, n.º 7, da Lei do Cibercrime[53]. Visa-se com esta norma não apenas os fornecedores de serviços, mas também as estruturas empresariais onde os suspeitos ou arguidos exerçam funções como empregados, em cujos sistemas informáticos deixem provas das suas actividades ilícitas.

De igual modo, não se pode fazer uso deste mecanismo quanto a sistemas informáticos utilizados para profissões sujeitas a sigilo, como o "*exercício da advocacia, das actividades médicas e bancárias, e da profissão de jornalista*", e "*segredo profissional ou de funcionário e de Estado*" – *cfr*. artigo 14.º, n.^{os} 6 e 7, da Lei do Cibercrime. Neste aspecto, foi notória a intenção do legislador no sentido de estabelecer um regime coerente com as garantias gerais do regime de segredo profissional ou de funcionário e de segredo de Estado, previstas no Código de Processo Penal[54].

5.4. Pesquisa de dados informáticos

O artigo 15.º da Lei do Cibercrime consagra a medida processual de pesquisa de dados informáticos[55] [56]. A pesquisa de dados informáticos é uma busca efectuada em ambiente

identificação do utilizador de um determinado endereço IP, num determinado dia e hora, ou do número de endereço IP usado por um determinado indivíduo, em circunstâncias temporais determinadas, é da competência do Ministério Público. Pelo contrário, quando se torna necessário obter informação mais alargada sobre os endereços IP utilizados num dado período de tempo ou sobre múltiplas comunicações efectuadas por um suspeito, estar-se-á já no âmbito do tráfego – informação desta natureza apenas pode ser solicitada com autorização judicial".

[53] A norma dirige-se, sobretudo, aos fornecedores de serviço, sendo que essa proibição de a mesma ser dirigida aos arguidos encontra fundamento no direito à auto-incriminação, com o qual entraria em colisão.

[54] Como bem refere BENJAMIM SILVA RODRIGUES, "*Subjaz a ideia que nos encontramos perante situações em que há uma obrigação de segredo relativamente a todos os dados que os intervenientes obtiveram conhecimento por conta e no âmbito das suas funções profissionais*", *apud*, DIAS VENÂNCIO, Pedro, *in ob. cit*., p. 109.

[55] O legislador optou pela designação "*pesquisa*", ao invés da designação "*busca informática*", por se revelar mais adequada à realidade do sistema informático. Na verdade, a própria Convenção do Cibercrime havia já alertado os Estados-Membros para a uniformização de regimes em matéria de buscas e apreensões em ambiente digital, salientando a necessidade de observar as características de intangibilidade e incorporeidade da prova digital.

[56] A Convenção do Cibercrime consagra, no seu artigo 19.º, a medida de busca e apreensão de dados informáticos armazenados. Como salienta BENJAMIM SILVA RODRIGUES, "*Em matéria de buscas e apreensões visa-se a harmonização das diversas legislações dos vários Estados, com vista a permitir que os dados informáticos sejam uniformemente considerados como coisas apropriáveis e susceptíveis de serem comunicados a terceiros"*, mais informando que *"estes procedimentos – buscas e apreensões – caracterizam-se pela: (i) identificação e apreensão do suporte (original) dos dados e do material ou programas necessário à sua leitura; (ii) admissão de cópia informática ou reprodução em suporte de papel. Com tal procedimento visa-se, sobretudo, permitir a recuperação dos dados, aí se compreendendo os casos em que eles apenas estão acessíveis com o recurso da Internet com o auxílio de um dispositivo (electrónico) de armazenamento à distância, ainda que no território de um Estado Estrangeiro. O artigo 19.º (Busca e apreensão de dados informáticos armazenados) CCiber 2001 prevê a necessidade dos Estados tomarem medidas legislativas que permitam, no limite do seu território, uma de duas coisas: (i) efectuar*

digital, uma forma de acesso coercivo ao meio informático, que não substitui os exames, previstos no Código de Processo Penal, nos seus artigos 171.º e seguintes[57]. Com esta medida, o legislador visa tornar o procedimento de acesso aos dados informáticos mais célere e eficaz, evitando a apreensão dos computadores e outros dispositivos informáticos para recolha de informação[58].

Salientamos o artigo 15.º, n.º 5, da Lei do Cibercrime, que estipula a possibilidade de, sempre que no decurso de uma busca a um sistema informático se detecte que os dados cuja obtenção se pretende se encontram guardados noutro sistema de computadores, as autoridades competentes podem autorizar a extensão da busca, por forma a obter a informação procurada[59]. Trata-se, pois, como bem refere PEDRO VERDELHO, de uma extensão da qual não resulta uma lesão adicional da privacidade do visado, uma vez que estão aqui em causa, a título exemplificativo "*situações em que o visado pela pesquisa utilize um serviço de correio electrónico baseado na Internet (um webmail), ao qual aceda habitualmente a partir do computador sujeito a pesquisa*", sendo que "*nestes casos, ninguém mais, além do visado, pode aceder à conta de correio electrónico em causa*", uma vez que "*não há outra forma de aceder a essa conta, a não ser intervindo junto do servidor/alojador dessa conta*"[60].

5.5. Apreensão de dados informáticos

A apreensão de dados informáticos é a medida processual prevista no artigo 16.º da Lei do Cibercrime, consagrando um regime similar ao das apreensões, previsto nos artigos 178.º e seguintes do Código de Processo Penal. A autoridade judiciária competente para a autorização, ordenação e validação desses dados é o Ministério Público (*cfr*. artigo 16.º, n.º 1), com excepção das situações em que se verifique urgência ou *periculum in mora* (16.º, n.º 2), casos

buscas (informático-digitais); (ii) aceder de modo similar (às buscas) aos dados informáticos", *apud*, DIAS VENÂNCIO, Pedro, *ob. cit*., pp. 111 e 112.

[57] Veja-se que o próprio artigo 15.º da Lei do Cibercrime é claro quanto a esse ponto, tanto nos seus n.os 2 a 4, ao consagrar regras materiais idênticas às previstas no regime geral das buscas, como no n.º 6, ao referir expressamente a aplicabilidade, com as necessárias adaptações, das regras de execução das buscas previstas no Código de Processo Penal.

[58] Salientamos que, *in casu*, visa-se o acesso a qualquer sistema informático, independentemente do objecto visado por esta medida. Mostra-se pertinente, para exemplificar as diferenças entre o regime geral das buscas e o regime especial da pesquisa de dados informáticos consagrado na Lei do Cibercrime, o exemplo invocado por ALBERTO GIL LIMA CANCELA, *ob. cit.*, p. 43. Como refere o Autor, a aplicar-se o regime geral das buscas, constante do Código de Processo Penal, caso o sistema informático pertencesse a um cibercafé, teria aplicação o disposto no artigo 174.º do Código de Processo Penal. Ao invés, caso a suspeita recaísse sobre um endereço IP que levasse a uma determinada morada, aplicar-se-ia o disposto no artigo 177.º do Código de Processo Penal, devendo verificar-se se se encontravam preenchidos os requisitos das buscas domiciliárias, designadamente a observância do princípio da legalidade. Assim sendo, perante a possibilidade de se aceder ao espaço digital, sem necessidade de entrar no domicílio do lesado, esbate-se esta distinção relativamente à localização física do dispositivo informático, uma vez que o que as buscas visam é precisamente a recolha de dados contidos nos sistemas informáticos.

[59] Segundo CONDE CORREIA, numa perspectiva literal, com base apenas no elemento gramatical, poder-se-ia dizer que o legislador consagrou assim, no artigo 15.º, n.º 5, da Lei do Cibercrime, as buscas *online*. Porém, na opinião do Autor, com a qual concordamos, "*o que aqui está em causa é a extensão online de uma pesquisa de dados informáticos em curso*", *ob. cit*., p. 42. Na verdade, não está em causa uma diligência oculta, realizada à revelia do visado, uma vez que o acesso ao primeiro sistema informático salvaguarda o controlo da sua legalidade.

[60] VERDELHO, Pedro, *ult. ob. cit.*, p. 742.

em que o órgão de polícia criminal poderá legitimamente apreender os dados sem prévia autorização da autoridade judiciária.

Também aqui, tal como sucede no regime previsto no artigo 15.º da Lei do Cibercrime, tem competência para autorizar a diligência a autoridade judiciária competente em cada fase do processo. Da mesma forma, o legislador, no artigo 16.º, n.º5 da Lei do Cibercrime, consagrou uma salvaguarda idêntica à prevista no já indicado artigo 15.º, n.º 5, de que os sistemas informáticos utilizados para o exercício da advocacia e das actividades médica e bancária estão sujeitas ao regime estabelecido nos artigos 182.º e seguintes do Código de Processo Penal, prevalecendo o segredo profissional ou de funcionário e o segredo de Estado.

Importa salientar que o legislador, na Lei do Cibercrime, não olvidou os direitos fundamentais relacionados com a privacidade dos visados com estas diligências e, nessa senda, estipulou no seu artigo 16.º, n.º 3 que na hipótese de tais dados se revelarem de cariz pessoal ou íntimo, susceptíveis de colocar em causa a privacidade do visado, é obrigatória a intervenção do juiz de instrução, que ponderará a sua junção aos autos, atendendo aos interesses do caso concreto e à sua força probatória. A preterição destas formalidades legais tem como consequência a nulidade da prova obtida. Na verdade, o legislador atendeu ao facto de os computadores pessoais e actualmente, e cada vez mais, os *smartphones*, serem verdadeiros repositórios de um manancial de informação da vida íntima e privada dos seus proprietários/utilizadores, materializados em fotografias, vídeos, gravações de voz ou documentos escritos, funcionando como uma verdadeira radiografia do seu quotidiano, daí que tenha sempre de presidir, aquando da ponderação deste meio de obtenção de prova, o respeito pela salvaguarda desta intimidade e privacidade, devendo a investigação criminal ceder quando dela resultem danos superiores aos interesses que se pretendem proteger.

O n.º 4 do artigo 16.º consagra um prazo máximo de 72 horas para as apreensões de dados informáticos efectuados por órgão de polícia criminal serem submetidos a validação por parte da autoridade judiciária e no n.º 5 do mesmo preceito legal consagra-se um regime diferenciado relativamente ao exercício da advocacia e das actividades médica, bancária e jornalística, previstos nos artigos 180.º e 181.º, do Código de Processo Penal, bem como a salvaguarda do segredo profissional ou do segredo de Estado (artigo 182.º do Código de Processo Penal).

Cumpre ainda fazer menção às específicas formas de apreensão, cujo fundamento legal consta do disposto no artigo 16.º, n.º 7, alíneas a) a d), da Lei do Cibercrime, que, no essencial consagra, para além da clássica apreensão do suporte físico onde está instalado o sistema informático ou onde estão armazenados os dados informáticos, a apreensão por via da realização da cópia de dados, bem como a preservação, por meios tecnológicos, da integridade dos dados e ainda a eliminação não reversível ou bloqueio de acesso aos dados[61]. Este elenco de medidas visa, essencialmente, facultar ao investigador a escolha da medida mais adequada

[61] O disposto nas alíneas c) e d) assume particular relevância sempre que os dados visados pela apreensão se afigurem nocivos para a sociedade, como vírus ou programas de promoção do terrorismo, ou dados de conteúdo ilegal, como é o caso da pornografia infantil. As técnicas de encriptação informática poderão impedir o suspeito de aceder temporariamente aos dados. Se a utilidade dos mencionados dados se esgotar no processo em causa, ou os mesmos serão eliminados, no caso de se revelarem inofensivos, ou o seu acesso poderá ser recuperado.

ao caso concreto e menos onerosa para o investigado[62], em respeito pelo princípio da proporcionalidade.

Foi igualmente consagrado pelo legislador, no seu artigo 16.º, n.º8, a imposição de os dados apreendidos serem certificados por meio de assinatura digital[63]. A mencionada norma prevê igualmente que a apreensão realizada por via de cópia de dados em suporte autónomo seja feita em duplicado[64].

5.6. Apreensão de correio electrónico e registos de comunicações de natureza semelhante

Um dos pontos merecedor de reforma no regime legal actual incide sobre a tutela processual penal atribuída à figura do correio electrónico e à sua apreensão. Foi clara a intenção do legislador no sentido de transpor para o ambiente digital o regime da apreensão de correspondência, previsto no Código de Processo Penal, com as necessárias alterações. E aqui erige-se o problema da não coincidência entre o regime previsto na Lei do Cibercrime e o regime previsto no Código de Processo Penal, que opta por aplicar à apreensão de comunicações electrónicas (e não apenas à intercepção dessas comunicações), o regime da intercepção de comunicações telefónicas.

Defende COSTA ANDRADE que "*depois de recebido, lido e guardado no computador do destinatário, um e-mail deixa de pertencer á área de tutela das telecomunicações, passando a valer como um normal escrito. E, como tal sujeito ao mesmo regime em que se encontra um qualquer ficheiro produzido pelo utilizador do computador e nele arquivado. Podendo, como tal, figurar como objecto idóneo da busca em sentido tradicional*"[65].

PEDRO VERDELHO defende que a aplicação do "*regime estabelecido para as escutas telefónicas para a fase de transmissão do e-mail, o regime da apreensão de correspondência para a fase em que o email já chegou ao destino mas ainda não foi lido pelo destinatário e o regime da apreensão de normais ficheiros escritos quando o email já foi aberto e lido pelo destinatário*"[66]. Ora, a rectificação operada ao artigo 17.º da Lei do Cibercrime é reveladora da influência desta posição doutrinária.

---

[62] Caso o dispositivo informático que constitui objecto de busca constitua material de trabalho ou modo de subsistência do arguido, a autoridade judiciária deverá tentar devolver-lho com a maior brevidade possível.

[63] Discorda desta solução legal BENJAMIM SILVA RODRIGUES, defendendo que a integridade da prova depende do "*seguimento das corretas etapas do método de obtenção de prova electrónico digital*", consagradas para manter a sua capacidade probatória. Concorda PEDRO DIAS VENÂNCIO, pugnando pela interpretação da assinatura digital como uma medida de preservação, garantindo a integridade dos dados apreendidos relativamente a alterações posteriores à apreensão, em DIAS VENÂNCIO, Pedro, *ob. cit*., pp. 114 e 115.

[64] No entendimento de PEDRO VERDELHO, ROGÉRIO BRAVO e LOPES ROCHA, a interpretação desta disposição deve ter em conta o disposto no artigo 19.º da Convenção do Cibercrime, pois todas as medidas aí presentes, com excepção da mera apreensão de dados no seu suporte, são medidas específicas do espaço virtual, não coincidindo com os conceitos actuais da lei processual. Assim, em VERDELHO, Pedro, BRAVO, Rogério e ROCHA, Manuel Lopes, *Leis do Cibercrime, Vol. I*, 2003, p. 18, disponível em http://www.centroatl.pt/titulos/direito/imagens/excerto-ca-leisdocibercrime1.pdf e acedido em 15.03.2018.

[65] CONDE CORREIA, *in ob. cit*., p. 40.

[66] VERDELHO, Pedro, *Apreensão do Correio Electrónico em processo Penal*, RMP, Ano 25.º, n.º 100, Outubro-Dezembro, 2004, pp. 153-154; e *Técnica no novo C.P.P.: Exames, Perícias e Prova Digital*, Revista CEJ, 1.º Semestre 2008, n.º 9 (Especial), pp. 145-171.

O artigo 17.º da Lei do Cibercrime tem sido, pois, objecto de uma vasta querela doutrinal[67] e jurisprudencial[68], já que o legislador não foi claro e, numa perspectiva literal, não fez qualquer distinção legal, fazendo recair o correio aberto e lido no mesmo regime previsto para o restante, sendo que em ambos os casos apenas a autorização judicial legitima a sua apreensão, tal como se dispõe no artigo 17.º. O ponto fulcral reside, pois, em saber se o correio electrónico já recebido e lido deve ser tratado de forma diferente, como um simples documento.

No entendimento de RITA CASTANHEIRA NEVES, foi intenção do legislador conferir ao correio electrónico armazenado uma tutela superior à conferida aos vulgares documentos escritos, "*um plus de protecção a arquivos que já foram comunicação, em nome da salvaguarda da privacidade, em nome da salvaguarda da privacidade da autodeterminação informacional*", razão pela qual é da competência do juiz a autorização ou ordem de apreensão (artigo 17.º da Lei do Cibercrime).[69]

De acordo com a posição sufragada por CONDE CORREIA, o correio electrónico aberto e armazenado será considerado um mero documento, semelhante a uma carta recebida, tornando mais fácil a sua apreensão, e advém precisamente dessa semelhança a convocação das normas gerais, presentes no artigo 17.º da Lei do Cibercrime, de apreensão da correspondência para obter as restantes comunicações. Para o efeito, será então suficiente a intervenção legitimadora do magistrado do Ministério Público, nos termos do disposto no artigo 16.º, da Lei do Cibercrime. "*Invocar o ritualismo da apreensão de correspondência quando já não há correspondência é um contra-senso. Não há nenhuma razão para privilegiar este correio – a pretexto da protecção da vida privada – em relação ao restante. As necessidades de tutela são iguais em ambos os casos, bastando-se com a existência de um controlo judicial posterior (16.º, n.º 3, da Lei n.º 109/2009)*", e continua, alegando que "*a protecção do sigilo das comunicações (sejam elas por correio tradicional ou através dos meios que o progresso disponibilizou) deve terminar quando a mensagem chega ao seu destinatário e*

[67] BENJAMIM SILVA RODRIGUES realça a possível confusão e conflito de normas, resultante da existência de vários diplomas legais aplicáveis ao correio electrónico alegando que tal levará o aplicador do direito a "*uma encruzilhada – e uma nova face oculta – nesta matéria, pois o correio electrónico continuará a fazer o seu constrangedor e confrangedor curso, na doutrina e na jurisprudência, umas vezes como comunicação electrónica (…) a levar ao altar das escutas telefónicas, outra vezes como comunicação electrónica a levar ao altar da correspondência clássica, outras vezes como amálgama de dados a levar ao altar das escutas telefónicas e, por último, enquanto dados a implicar outros de tráfego, e, por isso, a fazer intervir a legislação específica da Lei n.º 32/2008*", *apud*, DIAS VENÂNCIO, Pedro, p. 117.

[68] No Acórdão do TRG, datado de 12.10.2009, Processo n.º 1396/08.1PBGMR-A.G1, com o Relator Tomé Branco e disponível em *dsgi.pt*, afirma-se que a mensagem já recebida mas não lida se distingue da mensagem recebida e lida, evidenciando-se similar ao regime da correspondência do correio tradicional. Pelo contrário, o *e-mail* recebido e lido deverá ter a mesma protecção que as cartas recebidas, abertas e já guardadas. Ainda relativamente a esta temática, revela interesse o Acórdão do TRP, com o Processo n.º 896/07.5JAPRT, com o Relator Artur Vargues e igualmente disponível em *dgsi.pt* "*I - A leitura feita pela PJ de mensagem registada no cartão SIM de um telemóvel que já entrou na esfera de domínio do destinatário, não se configura como intercepção de conversação ou comunicação telefónica para efeitos da aplicação dos artigos 187.º e 188.º, nem lhe é aplicável a extensão enunciada no artigo 189.º, n.º 1, todos do CPP. II - A mensagem via telemóvel já recebida deverá ter o mesmo tratamento da correspondência escrita, que circula através do tradicional sistema postal: recebida mas ainda não aberta pelo destinatário, aplicar-se-á, à respectiva apreensão, o estabelecido no artigo 179º do CPP; recebida, aberta e guardada pelo destinatário, já não beneficiará do regime de protecção da reserva da correspondência e das comunicações, podendo ser apreendida para valer como mero documento escrito.*"

[69] CASTANHEIRA NEVES, Rita, *As ingerências nas comunicações electrónicas em processo penal*, Coimbra, Coimbra Editora (2011), p. 277.

aquele processo de transmissão se encontra concluído. A partir desse momento (conclusão efectiva do processo de transmissão) o destinatário dispõe dos meios necessários a evitar a intromissão estadual" [70].

Concordamos com os fundamentos aduzidos pelo Autor, por ser esta a forma mais coerente na articulação do regime geral com o regime especial e, dada a analogia de situações, o mesmo regime será aplicável à mensagem recebida no telemóvel, que em princípio será lida após recepção, tendo em conta a finalidade do dispositivo móvel e o seu porte pelo visado. Do mesmo modo, à mensagem recepcionada, lida e armazenada em suporte digital, corresponderá a mesma protecção prevista para a correspondência clássica. Consubstanciando simples documentos escritos, não faz sentido que lhes seja atribuído um regime de protecção da reserva da correspondência e das comunicações.

5.7. Intercepção de comunicações

A intercepção[71] de comunicações electrónicas[72] é a medida processual de obtenção de prova digital prevista no artigo 18.º da Lei do Cibercrime[73].

No entendimento de PEDRO VERDELHO[74], a comunicação é uma realidade dinâmica, vai de um lado para o outro, entre um emissor e um receptor. As mensagens de correio electrónico, por exemplo, são uma comunicação enquanto circulam nas redes, entre o computador de origem e o de destino e é precisamente enquanto a comunicação circula nas redes que a intercepção pode ser efectuada.

Saliente-se, como bem refere PEDRO DIAS VENÂNCIO, que, *in casu*, "*falamos da intercepção de mensagens de correio electrónico em tempo real, ou seja, no seu trajecto do computador do emissor para o computador do receptor através da rede de servidores. Ou ainda a intercepção de mensagens trocadas através de processos de comunicação instantânea (usualmente designados serviços de chat).*"[75]

---

[70] CONDE CORREIA, João, ob. cit., p. 41.
[71] Em conformidade com o disposto no artigo 2.º, al. e), da Lei do Cibercrime, a intercepção é "*o acto destinado a captar informações contidas num sistema informático, através de dispositivos electromagnéticos, acústicos, mecânicos e outros*."
[72] A previsão do artigo 18.º satisfaz as exigências dos artigos 20.º e 21.º da Convenção do Cibercrime, que prevê a recolha, em tempo real, de dados de tráfego, e a intercepção de dados de conteúdo de telecomunicações.
[73] Com efeito, o artigo 18.º, da Lei do Cibercrime, que consagra o regime jurídico da intercepção de comunicações, aplica-se a intercepção de dados de conteúdo e dados de tráfego, mas somente enquanto as comunicações ainda estão em curso. Neste sentido veja-se os Acórdãos do TRE, de 06.01.2015, Proc. n.º 6793/11.2TDLSB-A.E1, e de 20.01.2015, Proc. n.º 648/14.6GCFAR-A.E1, ambos disponíveis em *dgsi.pt*. Assim, "*quando o momento do seu recebimento já pertence ao passado, qualquer contacto com a comunicação feita não tem qualquer correspondência com a ideia de intercepção. As mensagens que depois de recebidas, ficam gravadas no receptor deixam de ter a natureza de comunicação em transmissão*", pelo que o regime a aplicar já não será o da intercepção de comunicações. Assim, Acórdão do TRL, de 17.07.2008, Proc. n.º 3453/2008-5, igualmente disponível em *dsgi.pt*.
[74] VERDELHO, Pedro, "*Técnica no Novo C.P.P.: Exames, Perícias e Prova Digital*", Revista CEJ, 1º Semestre 2008, nº 9 – Jornadas sobre a revisão do Código de Processo Penal, p. 164.
[75] DIAS VENÂNCIO, Pedro, *in ob. cit*., p. 117.

O recurso às intercepções telefónicas é, pois, um método oculto de investigação[76], na medida em que os visados com a diligência só dela tomam conhecimento depois de a mesma se encontrar já consumada, o que significa que não tenham qualquer possibilidade de defesa ou reacção contra essa intercepção.

Partindo desta visão, considerando que esta medida "*apresenta um elevado potencial de danosidade social, na medida em que comporta irremediavelmente a restrição de direitos fundamentais*", SÓNIA CRUZ LOPES considera que a mesma só deve ser admitida excepcionalmente, em função da verificação de determinados pressupostos, sob pena de proibição da sua valoração. Como pressupostos indica, então, o princípio da reserva de lei na legitimação desta medida (*cfr*. artigos 18.º, n.º 2, e 165.º, n.º 1, al. c), da Constituição da República Portuguesa), a existência de um "*catálogo*" de crimes que legitimarão a intercepção, a suspeita fundada em factos concretos e medidos a partir de critérios de plausabilidade e probabilidade, a necessidade de se atender ao princípio da subsidiariedade e ao princípio da proporcionalidade, a legitimidade da sua intervenção, salvaguardando a área nuclear da intimidade dos visados e o princípio fundamental da pessoa humana e a reserva de juiz para decretar a medida[77].

No artigo 18.º prevê-se o recurso a intercepções em processos relativos a crimes previstos na Lei do Cibercrime ou cometidos por meio de um sistema informático e ainda para crimes em que a lei processual penal geral admita as escutas telefónicas (artigo 187.º do Código de Processo Penal), ou seja, as intercepções apenas são consideradas com um âmbito de aplicação restrito[78] [79]. Assim sendo, o artigo 18.º aplicar-se-á somente às medidas de intercepção de comunicações em tempo real quanto a crimes previstos na Lei do Cibercrime (falsidade informática, dano relativo a programas ou outros dados informáticos, sabotagem informática, acesso ilegítimo, intercepção ilegítima e reprodução ilegítima de programa protegido), em conformidade com o disposto no artigo 18.º, n.º 1, al. a), da Lei do Cibercrime, e será também aplicável aos crimes previstos no artigo 187.º, n.º 1, do Código de Processo Penal, mas somente quando estes forem cometidos por meio de sistemas informáticos, ou relativamente aos quais seja necessário recolher prova em suporte informático.

[76] Sobre esta problemática, invocando o princípio *nemo tenetur se ipsum accusare*, veja-se LOPES, Sónia Raquel da Cruz, "*Intercepção de comunicações para prova dos crimes de injúrias, ameaças, coacção, devassa da vida privada e perturbação da paz e do sossego cometidos por meio diferente do telefone*", Revista de Concorrência e Regulação, Coimbra, A. 8, n.º 29 (Janeiro-Março 2017), p. 239 e também CASTANHEIRA NEVES, Rita, *in ob. cit*., p. 98. Aliás, este princípio é igualmente invocado pela doutrina quanto à discussão sobre a revelação coactiva da *password*, questão que a Lei do Cibercrime não resolve, mas que, em razão da inexistência de norma habilitante para o efeito e considerando os constrangimentos processuais que tal implica na pessoa do visado, se entende, com fundamento no princípio do *nemo tenetur se ipsum accusare*, que o arguido não deve ser obrigado a contribuir para a sua própria auto-incriminação.

[77] *Idem*, p. 239 a 241.

[78] Sobre a articulação e compatibilização da intercepção das comunicações no quadro constitucional vigente, em especial os artigos 18.º, n.º 2, e 34.º, n.º 4, da Constituição da República Portuguesa e a excepcionalidade deste regime, veja-se LOPES, Sónia*, in ob. cit*., p. 236 e 237.

[79] Note-se que o artigo 34.º, n.º 4, da Constituição da República Portuguesa apenas permite a ingerência das autoridades públicas nas telecomunicações nos processos de natureza penal.

Tal deve-se ao facto deste meio de obtenção de prova, enquanto método oculto de investigação, ser bastante mais restritivo e intrusivo dos direitos fundamentais do que a generalidade dos outros meios de obtenção de prova previstos na Lei do Cibercrime.

Atento o restrito âmbito de aplicação desta disposição legal, uma das questões que se coloca na doutrina é precisamente a de saber se é possível recorrer à intercepção de comunicações previstas no artigo 18.º da Lei do Cibercrime para prova dos crimes de injúria, ameaça, coacção, devassa da vida privada e perturbação da paz e do sossego, quando cometidos por meio diferente do telefone, atento o disposto no artigo 187.º, n.º 1, al. e), do Código de Processo Penal.

Em sentido negativo pronuncia-se, designadamente, RITA CASTANHEIRA NEVES, referindo que tal extensão não parece ser possível "*dada a específica metodologia que deve seguir a interpretação da lei penal e processual penal, atento o respeito ao princípio da legalidade*", defendendo que "*deveria ter sido o legislador a ter a preocupação de logo estabelecer na parte final da agora alínea e) do n.º 1 do artigo 187.º do Código de Processo Penal a expressão quando cometidos através de meio técnico de comunicação. Para além disso, tal interpretação seria in male partem, sendo, por isso, inconstitucional.*"[80]
Em sentido positivo pronuncia-se, desde logo CONDE CORREIA, entendendo que o catálogo de crimes constante do artigo 187.º, n.º 1, do Código de Processo Penal "*deverá, numa interpretação actualista, incluir os crimes de injúria, ameaça, coacção ou devassa da vida privada cometidos através de sistema informático. O que ali é autorizado para os crimes praticados através do telefone é aqui permitido para os crimes cometidos através de um sistema informático*".[81] Também SÓNIA CRUZ LOPES entende que "*poder-se-á recorrer à intercepção de comunicações para prova dos crimes anteriormente referidos quando tais crimes são praticados por meio diferente do telefone, pois tal não violará o princípio da legalidade, uma vez que o próprio artigo 18º, n.º 1, al. b), da LC prevê expressamente essa possibilidade ao dispor que "é admissível o recurso a intercepção de comunicações em processos relativos a crimes cometidos por meio de um sistema informático (…) quando tais crimes se encontrem previstos no artigo 187.º do Código do Processo Penal", não se cingindo, por isso, aos crimes cometidos através do telefone*"[82].

Na verdade, este meio de obtenção de prova, agora adaptado ao ambiente digital, há muito se encontrava previsto no Código de Processo Penal, tanto para as comunicações telefónicas, como para outro tipo de comunicações, designadamente as electrónicas (*cfr*. artigo 189.º do

[80] CASTANHEIRA NEVES, Rita, *in. ob. cit*., p. 167. No mesmo sentido, pronuncia-se CARLOS ADÉRITO TEIXEIRA, *apud*, LOPES, Raquel da Cruz, in ob. cit., p. 248, referindo que "*esta formulação típica não parece consentir a extensão de regime aos (mesmos) crimes cometidos através de outros meios para efeito de se considerarem de catálogo e legitimadores da "intercepção" desses meios para obtenção de prova", devido, sobretudo a duas razões: "por um lado, porque em matéria de restrição de direitos – que uma intercepção sempre representa – não são admissíveis extensões do âmbito do regime que o legislador estabeleceu; por outro lado, não se poderá dizer que a mens legislatoris visaria incluir no catálogo os crimes cometidos através do telefone ou através de "quaisquer outros meios" (a que alude no art. 189.º) porque, em outros lugares do artigo onde se enuncia o catálogo, quando entendeu ser abrangente, usou a expressão "meio de comunicação" (cfr. n.º 4 e n.º 7 do art. 187.º) e não telefone.*"
[81] CONDE CORREIA, João, *in ob. cit*., p. 45.
[82] LOPES, Sónia Raquel da Cruz, *in ob. cit*., p. 252.

Código de Processo Penal.) De notar que este regime não foi revogado com a entrada em vigor da Lei do Cibercrime, continuando por isso, em vigor[83]. Simplesmente, o artigo 18.º instituiu um regime especial, destinado a casos específicos[84].

Estipula o n.º 2 do artigo 18.º, que a intercepção e o registo de transmissões de dados informáticos só podem ser autorizados durante o inquérito, nos casos em que subsistam razões para crer que a diligência se revela indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter, por despacho fundamentado do juiz de instrução e mediante requerimento do Ministério Público.

Por sua vez, no artigo 18.º, n.º 3 da Lei do Cibercrime estabelece que a intercepção tanto pode destinar-se ao registo de dados relativos ao conteúdo das comunicações, como visar apenas a recolha e o registo de dados de tráfego. Todavia, em qualquer dos casos, o despacho do juiz de instrução deverá especificar o respectivo âmbito, de acordo com as necessidades concretas da investigação.

O legislador nacional estabeleceu, assim, em matéria de intercepção e registo de transmissões de dados informáticos, as regras presentes no disposto nos artigos 187.º a 190.º, do Código de Processo Penal (*cfr*. artigo 18.º, n.º 4, da Lei do Cibercrime.) Quer tal significar, conforme se aflorou, que serão aplicáveis os procedimentos e autorizações judiciais previstas para as escutas telefónicas às comunicações electrónicas.

5.8. As acções encobertas

O regime das acções encobertas encontra-se consagrado no artigo 19.º, da Lei do Cibercrime, destinado aos crimes previstos nesse diploma e aos crimes cometidos através de meio informático, sempre que lhes corresponda uma pena de prisão superior a 5 anos, ou inferior, se dolosos e contra a liberdade e autodeterminação sexual quando os ofendidos sejam menores ou incapazes, a burla qualificada, a burla informática e nas comunicações, a discriminação racial, religiosa ou sexual e as infracções económico-financeiras, e ainda os crimes consagrados no título IV do Código do Direito de Autor e crimes conexos[85] [86].

[83] Como bem refere PEDRO VERDELHO "*A verdade é que a extensão do regime das intercepções telefónicas à intercepção de outras comunicações não tinha viabilidade prática quanto aos crimes informáticos, ou a crimes relacionados com a informática, ou ainda a crimes cometidos por computadores. A generalidade deles não está incluída no chamado catálogo de crimes em relação aos quais é permitido proceder a intercepções telefónicas (…) o propósito do artigo 18.º da Lei do Cibercrime é precisamente enquadrar legalmente a realização dessas intercepções de comunicações quando estiverem em investigação crimes considerados neste diploma. Quanto aos demais, limita-se a transpor para o ambiente digital o mecanismo da intercepção de comunicações previsto no Código de Processo Penal. Aliás, parece que deliberadamente remete em bloco para o regime geral e que, portanto, assume que a intercepção de comunicações aqui prevista recorre a toda a regulamentação dos artigos 187.º e 188.º, do CPP. Apenas excepciona desta regra a definição do âmbito material sobre que incide (…) a generalidade dos crimes previsto neste diploma não está incluída no catálogo previsto no artigo 187.º e portanto, a intercepção de comunicações não é permitida por aquele Código quando estão em causa crimes informáticos. Daí se tornar necessário legitimá-la …",* VERDELHO, Pedro, in *A Nova Lei do Cibercrime*, p. 747.

[84] Quanto à articulação dos diversos regimes, veja-se o Acórdão do TRE, datado de 20.01.2015, com o Relator João Gomes de Sousa, Processo n.º 648/14.6GCFAR-A.E1, disponível em *dgsi.pt*.

[85] SILVA RAMALHO elogia esta opção do legislador "*cremos que este passo dado pelo artigo 19.º da Lei do Cibercrime vai no sentido certo, ao reconhecer a necessidade do recurso a métodos de investigação criminal mais*

Ou seja, o artigo 19.º n.º 1 amplia a possibilidade de recurso às acções encobertas, prevendo um conjunto de crimes que não se encontram previstos na Lei nº 101/2001, de 25 de Agosto, isto é, no Regime jurídico das acções encobertas para fins de prevenção e investigação criminal.

Do n.º 2 desta norma resulta a remissão para o regime da intercepção de comunicações (artigo 18.º da Lei do Cibercrime), pelo que aqui serão igualmente aplicáveis os pressupostos do regime das escutas telefónicas dos artigos 187.º a 190.º do Código de Processo Penal.

Como bem refere BENJAMIM SILVA RODRIGUES, "*as acções encobertas, ao nível da Lei do Cibercrime, implicarão a necessidade do respeito pelas regras do regime das escutas telefónicas (artigos 187.º e 190.º do CPP), sempre que elas implicarem o recurso a meios e dispositivos informáticos ligados às tecnologias da informação e comunicação e isso ocorrer por meio das redes electrónicas publicamente acessíveis.*"[87]

6. Cooperação Internacional – breve referência

A Lei do Cibercrime é inovadora no que concerne à vertente internacional, consagrando, nos seus artigos 20.º a 26.º, medidas específicas no domínio da cooperação internacional em matéria de obtenção da prova digital, por referência à Convenção do Cibercrime (artigos 23.º a 35.º.) Todavia, a lei assume, no seu artigo 28.º, como norma, que na cooperação internacional sejam observadas as regras do regime geral previstas na Lei n.º 144/99, de 31 de Agosto (Lei da Cooperação Judiciária Internacional em Matéria Penal), em tudo o que não contrariar as disposições previstas na Lei do Cibercrime.[88]

Estabelece desde logo o artigo 21.º da Lei do Cibercrime a necessidade de organização de um ponto de contacto centralizador e permanente, acessível à cooperação no combate ao crime informático, merecendo esta medida destaque em razão da sua repercussão prática e relevo no âmbito da cooperação internacional urgente. O referido ponto de contacto é a Polícia

agressivos em relação a uma criminalidade que tem beneficiado largamente da ineficácia dos restantes meios disponíveis", *in ob. cit*., pp. 408 a 409. O Autor procura demonstrar, a eficácia das acções encobertas ao âmbito da Dar Web, pelo facto de os seus resultados não encontrarem paralelo em qualquer outro meio de investigação criminal, uma vez que tem a principal vantagem de permitir a descoberta da identidade e localização dos autores dos crimes e respectivas vítimas.

[86] Esta medida tem sido utilizada nos E.U.A., com resultados muito positivos na prevenção e repressão de alguns tipos de cibercriminalidade, em especial no combate à pornografia infantil, à pedofilia *online*, ao tráfico de droga e ao jogo ilegal, SILVA RAMALHO, David, *in ob. cit*., pp. 76 e 77. A União Europeia, através da Directiva 2011/92/EU, do Parlamento Europeu e do Conselho, de 13.12.2011, relativa à luta contra o abuso sexual, exploração sexual de crianças e pornografia infantil, tem vindo a sugerir a sua implementação nas legislações nacionais.

[87] SILVA RODRIGUES, Benjamim, *apud*, DIAS VENÂNCIO, Pedro, p. 123.

[88] Neste aspecto revela todo o interesse atentar na Nota Prática n.º 3/2014, de 12 de Junho de 2014, relativa à cooperação judiciária com os Estados Unidos da América, designadamente à Google, ao Facebook e à Microsoft, com a menção da possibilidade de cooperação informal, através de pedido directo, mediante a apresentação de formulário específico para o efeito, igualmente disponível no SIMP, e elenco das situações em que esse pedido de informação se mostra inviável. A referida nota encontra-se disponível para consulta, em https://simp.pgr.pt/destaques/mount/anexos/3227_nota_pratica_isp_eua.pdf. Veja-se ainda, quanto à mesma matéria, a Nota Prática n.º 4/2014, de 22 de Dezembro de 2014, acessível para consulta em https://simp.pgr.pt/destaques/mount/anexos/3758_nota_pratica_4___pedidos_a_isp_eua_(2).pdf.

Judiciária, através da "*Rede 24/7*"[89], localizada na Secção de Investigação da Criminalidade Informática[90].

Este diploma legal, prevê ainda alguns institutos inovadores em matéria de cooperação internacional, cujo objectivo é o de adequar a cooperação aos novos desafios trazidos pela cibercriminalidade, dos quais importa salientar o disposto nos artigos 22.º e 23.º, referentes, respectivamente, à possibilidade legal de se proceder, em Portugal, à preservação e revelação expeditas de dados informáticos, e motivos da sua recusa. O artigo 24.º estabelece o acesso a dados informáticos em cooperação internacional, prevendo a possibilidade de a autoridade judiciária nacional pesquisar, recolher e divulgar os dados informáticos, quando se trate de "*situação em que a pesquisa e apreensão são admissíveis em caso nacional semelhante*". O artigo 25.º, por sua vez, estipula o acesso transfronteiriço a dados armazenados quando publicamente disponíveis ou com consentimento, e o artigo 26.º consagra a intercepção das comunicações em cooperação internacional, prevendo a autorização pelo juiz da intercepção de transmissão de dados informáticos realizada através de um sistema informático localizado em território português, medida que já resultaria do direito interno[91].

[89] Está disponível 24 horas, 7 dias por semana, através do endereço: contacto24.7@pj.pt.
[90] Em caso de pedido de cooperação de um Estado, o órgão de polícia criminal prestará a assistência prevista no disposto no artigo 21.º, n.º 3, da Lei do Cibercrime, com aconselhamento técnico, através da preservação ou recolha dos dados e localização dos suspeitos. Após, a PJ notificará o Ministério Público de tal pedido, por via do relatório a que alude o artigo 21.º, n.º 4, com a descrição das "*investigações levadas a cabo, os resultados das mesmas, a descrição dos factos apurados e as provas recolhidas*" (artigo 253.º, do Código de Processo Penal.)
[91] Tanto a preservação e revelação expeditas de dados informáticos como o acesso a dados informáticos consubstanciam medidas pouco inovadoras da cooperação internacional, antes traduzindo a adaptação para a cooperação, dos institutos processuais previstos pela Lei do Cibercrime para as investigações no âmbito nacional.

IV. Hiperligações e referências bibliográficas

Hiperligações

https://dre.pt/application/dir/pdf1sdip/2009/09/17900/0635406378.pdf
http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32005F0222
https://simp.pgr.pt/destaques/mount/anexos/4564_nota_pratica_7___retencao_de_dados.pdf
https://simp.pgr.pt/simp_tematicos/documentos/mount/files/1456403096_2016_02_20_nota_pratica_8_pedido_de_info_a_isp.pdf
https://simp.pgr.pt/simp_tematicos/documentos/mount/files/1440687720_nota_pratica_6__jurispridencia_processual.pdf
https://simp.pgr.pt/simp_tematicos/documentos/mount/anexos/1358780904_2013_01_09_nota_pratica___pedido_de_ip.pdf.
https://simp.pgr.pt/simp_tematicos/documentos/mount/files/1365007943_2013_04_03_nota_pratica___jurispridencia_sobre_ip.pdf
www.centroatl.pt/titulos/direito/imagens/excerto-ca-leisdoCibercrime1.pdf
https://simp.pgr.pt/destaques/mount/anexos/3227_nota_pratica_isp_eua.pdf
https://simp.pgr.pt/destaques/mount/anexos/3758_nota_pratica_4___pedidos_a_isp_eua_(2).pdf.

Referências bibliográficas

– ALBUQUERQUE, Paulo Pinto de, "*Comentário do Código de Processo Penal à luz da Constituição da República Portuguesa e da Convenção Europeia dos Direitos do Homem*", 4.ª ed. actualizada, Lisboa, Universidade Católica, 2011;

– CALLEJA, Álvaro Manuel Monge, *A Investigação criminal face à globalização e o cibercrime*, Investigação Criminal, Lisboa, N.º 11 (Fevereiro 2017), p. 170-187;

– CANCELA, Alberto Gil Lima, *A prova digital: os meios de obtenção de prova na Lei do Cibercrime*, Dissertação de Mestrado, Faculdade de Direito da Universidade de Coimbra, 2016;

– CORREIA, João Conde, "*Prova Digital: as leis que temos e a lei que devíamos ter*", Revista do Ministério Público, n.º 139 (Julho-Set 2014);

– LOPES, Sónia Raquel da Cruz, "*Intercepção de comunicações para prova dos crimes de injúrias, ameaças, coacção, devassa da vida privada e perturbação da paz e do sossego cometidos por meio diferente do telefone*", Revista de Concorrência e Regulação, Coimbra, A. 8, n.º 29 (Janeiro-Março 2017);

– MESQUITA, Paulo Dá, (2010) "*Prolegómeno sobre prova electrónica e intercepção de telecomunicações no Direito Processual Penal português – o Código e a Lei do Cibercrime*", in Processo Penal, Prova e Sistema Judiciário, Coimbra, Coimbra Editora;
– MILITÃO, Renato Lopes, *A propósito da prova digital no processo penal*, ROA, 2012 (Ano 72), n.º 1;

– NEVES, Rita Castanheira, "*As Ingerências nas Comunicações Electrónicas em Processo Penal – Natureza e respectivo regime jurídico do correio electrónico enquanto meio de obtenção de prova*", Coimbra; Coimbra Editora, 2011;

– RAMALHO, David Silva, "*A investigação criminal na "Dark Web*", Revista de Concorrência e Regulação, Coimbra, Ano 4, n.º 14-15 (Abril-Setembro 2013);

– VENÂNCIO, Pedro Dias, "*Lei do Cibercrime Anotada e Comentada*", 1.ª ed., Coimbra, Coimbra Editora, 2011;

– VERDELHO, Pedro, "*A nova Lei do Cibercrime*", *Scientia Juridica*, Tomo LVIII, n.º 320, Braga, 2009;

– VERDELHO, Pedro, "*A Convenção sobre Cibercrime do Conselho da Europa – Repercussões na Lei Portuguesa*", Direito da Sociedade da Informação, Vol. VI, Coimbra Editora, 2006;

– VERDELHO, Pedro, "*Apreensão de Correio Electrónico em Processo Penal*", Revista do Ministério Público, Ano 25.º, nº 100, Outubro-Dezembro, 2004, pp. 153-164;

– VERDELHO, Pedro, "*Técnica no Novo C.P.P.: Exames, Perícias e Prova Digital*", Revista CEJ, 1º Semestre 2008, nº 9 – Jornadas sobre a revisão do Código de Processo Penal.

– VERDELHO, Pedro; BRAVO, Rogério; ROCHA, Manuel Lopes, "*Leis do Cibercrime*", Vol. I, 2003, disponível em
http://www.centroatl.pt/titulos/direito/imagens/excerto-ca-leisdocibercrime1.pdf

CENTRO
DE ESTUDOS
JUDICIÁRIOS

4.

Medidas cautelares e de polícia

Enquadramento jurídico, prática e gestão processual

Raul Estêvão Ramos Trancoso

CENTRO
DE ESTUDOS
JUDICIÁRIOS

4. MEDIDAS CAUTELARES E DE POLÍCIA. ENQUADRAMENTO JURÍDICO, PRÁTICA E GESTÃO PROCESSUAL

Raul Estêvão Ramos Trancoso

I. Introdução

As medidas cautelares e de polícia podem ser encaradas como um direito de primeira intervenção, uma vez que permitem a atuação dos órgãos de polícia criminal logo após terem obtido conhecimento da notícia do crime, antecipando a intervenção das autoridades judiciárias. São ainda um espaço de iniciativa própria dos órgãos de polícia criminal, mesmo depois da intervenção das autoridades judiciárias, em que estes podem aplicar medidas que contendem com os direitos fundamentais dos cidadãos. No presente trabalho efetuou-se uma abordagem jurídica das medidas previstas na lei processual penal e na lei do cibercrime, procurando-se aflorar questões de índole prática, quer no relacionamento com os órgãos de polícia criminal quer na abordagem quando da apreciação concreta das medidas por parte do magistrado do Ministério Público.

II. Objetivos

Pretendeu-se elaborar um trabalho com características teórico-práticas, com vista à abordagem da temática medidas cautelares e de polícia, do ponto de vista jurídico-penal mas, todavia, sem deixar de sublinhar questões práticas no que à gestão processual concerne, em particular no relacionamento com os órgãos de polícia criminal e na prática judiciária corrente. Destina-se em especial, aos colegas Auditores de Justiça, com vista criar interesse pela temática e a fomentar o debate.

III. Resumo

No presente trabalho tratam-se questões relacionadas com as medidas cautelares e de polícia. Partindo do seu enquadramento através da abordagem ao conceito de polícia, focando posteriormente a definição da natureza destes atos com o objetivo de chegarmos à sua definição enquanto conceito.

A parte principal do presente trabalho centra-se nas medidas presentes na lei processual penal, discorrendo-se pelas medidas dispostas na lei do cibercrime, sublinhando o seu enquadramento jurídico.

Aborda-se, em jeito de contextualização a relação entre Ministério Público e os órgãos de polícia criminal, enunciando-se algumas práticas que se entendem como relevantes para eficácia da atuação do Ministério Público.

Finaliza-se, enumerando, de forma objetiva, os procedimentos concretos a adotar pelo magistrado do Ministério Público quando confrontado com a atuação cautelar dos órgãos de polícia criminal.

1. Enquadramento das medidas cautelares e de polícia

1.1. As funções da Polícia

A Polícia tem por funções, constitucionalmente definidas, defender a legalidade democrática e garantir a segurança interna e os direitos dos cidadãos (artigo 272.º, nº 1, da Constituição da República Portuguesa (CRP)). A Polícia[1] pode desenvolver a sua atividade abrangendo mais do que uma modalidade, à exceção da Polícia Judiciária (que tem como atribuições a prevenção e a investigação criminal), os órgãos de polícia criminal, como a PSP e a GNR, têm funções de polícia judiciária, de polícia administrativa geral enquanto força de segurança e, ainda, de polícia administrativa especial na medida em que são compostas por unidades com competências específicas, como por exemplo competências de controlo de trânsito.

A atividade policial concretiza-se em três quadrantes[2]:

– Medidas puras de polícia: "*que são ordenadas pela Autoridade de Polícia e promovidas pelos agentes policiais que lhe estão subordinados na função de comando e dependência hierárquica*"[2], à luz da função de garantia de segurança interna, consagrada no nº 1 do artigo 272.º da CRP. Estas podem ser medidas (gerais) de polícia (cfr. artigo 28.º da Lei de Segurança Interna (LSI)) tais como a identificação de pessoas suspeitas que se encontrem ou circulem em lugar público, aberto ao público ou sujeito a vigilância policial; a evacuação ou abandono temporários de locais ou meios de transporte. Ou medidas especiais de polícia (cfr. artigo 29.º

[1] É no âmbito da polícia enquanto "*atividade*" que podemos verificar que é comum fazer-se a tradicional distinção entre "*polícia administrativa*" e "*polícia judiciária*", no que concerne ao conceito amplo de polícia administrativa.
[2] Valente, Manuel Monteiro Guedes - Teoria Geral do Direito Policial, 5.ª Edição, Coimbra, Almedina, 2017, p. 74.

da LSI), por exemplo a realização, em viatura, lugar público, aberto ao público ou sujeito a vigilância policial, de buscas e revistas para detetar a presença de armas, substâncias ou engenhos explosivos ou pirotécnicos; apreensão temporária de armas, munições, explosivos.

– **Medidas preventivas administrativas:** fiscalização de velocidade por meio de radar em determinada via rodoviária e **medidas cautelares administrativas** – por exemplo as que são levadas a cabo no âmbito do ilícito de ordenação social.

– **Medidas cautelares e de polícia**: objeto do nosso estudo e que constituem atos destinados a servir o processo penal, relacionadas diretamente com a atividade de polícia judiciária, previstas na lei processual penal, nos artigos 249.º a 252.º-A do Código de Processo Penal, e em lei avulsa, em específico nos artigos 12.º, n.º 2, 13.º, 16.º, n.º 2 e 22.º, n.º 4, todos da lei do cibercrime (Lei n.º 109/2009, de 15 de setembro).

2. Natureza das medidas cautelares e de polícia

O Código de Processo Penal faz alusão às competências dos órgãos de polícia criminal[3] no artigo 55.º, n.º 1 *(Competência dos órgãos de polícia criminal),* sendo que refere expressamente que estes devem "*coadjuvar as autoridades judiciárias com vista à realização das finalidades do processo*.".

Estamos perante uma relação de cooperação que deve ter em vista servir o processo penal, na concretização da boa decisão da causa, ou seja, da descoberta da verdade, que se materialize na "*decisão sobre a questão da imputação criminal, a questão da determinação das sanções criminais e a questão da responsabilidade civil."* [4].

Em especial, compete aos órgãos de polícia criminal, "*mesmo por iniciativa própria, colher notícia dos crimes e impedir quanto possível as suas consequências, descobrir os seus agentes e levar a cabo os actos necessários e urgentes destinados a assegurar os meios de prova*." - artigo 55.º, n.º 2, do Código de Processo Penal.

A consagração das medidas cautelares e de polícia visa essencialmente acautelar meios de prova, através de tomada de providências por iniciativa dos órgãos de polícia criminal, sem necessidade de qualquer intervenção da autoridade judiciária.

Tal atuação depende dos pressupostos de necessidade e urgência, orientada pelo princípio da eficácia que fundamenta a atuação por iniciativa própria[5].

---

[3] "*todas as entidades e agentes policiais a quem caiba levar a cabo quaisquer actos ordenados por uma autoridade judiciária ou determinados por este Código"* - al. c) do artigo 1.º do Código de Processo Penal; O CPP não baseia a definição de OPC na qualificação institucional de um órgão mas sim na qualidade dos atos que o mesmo pratica, daí como refere Paulo Dá Mesquita, em Repressão Criminal e Iniciativa Própria dos Órgãos de Polícia Criminal, I Congresso de Processo Penal, Coimbra, Almedina, 2005, p. 56., "*a posição jurídico-institucional dos corpos orgânicos designados como Polícia Judiciária, Polícia de Segurança Pública e Guarda Nacional Republicana seja idêntica."*

[4] Albuquerque, Paulo Pinto de, Comentário do Código de Processo Penal, 2.ª edição atualizada, Lisboa, UCE, 2008, p. 164.

[5] Dá, Paulo Mesquita, Direcção do Inquérito e Garantia Judiciária, Coimbra, Coimbra Editora, 2003, p. 131.

Os órgãos de polícia criminal, por iniciativa própria, colhem notícia dos crimes e impedem tanto quanto possível as suas consequências. No entanto, na sequência da aquisição da notícia do crime os órgãos de polícia criminal não podem realizar pré-inquéritos, pois não têm enquadramento jurídico-legal. A notícia do crime determina o dever de comunicação ao Ministério Público, com a consequente obrigação por parte desta autoridade judiciária de abertura do processo penal. Tal dever de comunicação visa a efetivação do controlo sobre todas as atividades investigatórias baseadas em suspeitas de crimes levadas a cabo por órgãos de polícia criminal.[6]

A atividade por iniciativa própria dos órgãos de polícia criminal apresenta quatro características processuais: "obrigatória", "preliminar", "temporária" e "auxiliar"[7].

A atuação dos órgãos de polícia criminal neste âmbito não se confunde com qualquer fase processual, trata-se de uma atividade de recolha de meios de prova por iniciativa própria baseada nos princípios da necessidade e urgência, posteriormente sujeita a controlo judiciário, que se distingue dos atos por encargo de autoridade judiciária pela legitimação *ope legis* fundada no perigo na demora.[8] Este controlo judiciário da repressão criminal visa aferir da legalidade da atuação dos órgãos de polícia criminal e da sua relevância processual, decidindo o Ministério Público quanto à possibilidade da sua integração no processo.

Os atos cautelares praticados pelos órgãos de polícia criminal levados a cabo por iniciativa própria são verdadeiros atos processuais?

Para alguns autores, nomeadamente PAULO DÁ MESQUITA[9] e GERMANO MARQUES DA SILVA, as medidas cautelares e de polícia embora possam vir a integrar o processo, não são no momento da sua prática atos processuais em sentido formal, pelo que a sua integração no processo depende de um ato decisório de apreciação da autoridade judiciária quanto ao conjunto de circunstâncias específicas que pautaram a atuação dos órgãos de polícia criminal.

As medidas cautelares e de polícia tratam-se de "*uma realidade extraprocessual conexa com a processual*"[10], são atos de polícia judiciária, "*praticados pelos funcionários ou autoridades, subsidiariamente às suas funções precípuas, com vista a informar, permitir ou facilitar o exercício da ação penal pelos seus titulares, têm uma natureza material ou melhor oficiosa que, precisam do ponto de vista do processo penal de ser oficializados ou legalizados*"[11].

[6] Veja-se neste sentido Parecer do Conselho Consultivo da PGR n.º 45/2012, relator Paulo Dá Mesquita, disponível em www.dgsi.pt.
[7] Rodrigues, Anabela Miranda, A Fase Preparatória do Processo Penal - Tendências na Europa: o caso português, Revista Brasileira de Ciências Criminais, a. X, n.º 39 (2002), São Paulo: Editora Revista dos Tribunais, p. 25.
[8] Cfr. Dá, Paulo Mesquita, Repressão Criminal e Iniciativa Própria dos Órgãos de Polícia Criminal, Revista do Ministério Público n.º 98, ano 25, abril/junho, 2005, p. 11.
[9] Dá, Paulo Mesquita, Direcção do Inquérito e Garantia Judiciária, Coimbra, Coimbra Editora, 2003, p. 63.
[10] Silva, Germano Marques da, Direito Processual Penal Português, Do Procedimento, Vol. 3, Lisboa, UCE, 2015, p. 61.
[11] Cf. Correia, Eduardo, A Instrução Preparatória em Processo Penal; alguns problemas, BMJ nº 42, 1954, p. 15 e17.

No sentido de que as medidas cautelares e de polícia configuram um verdadeiro ato processual os autores JOSÉ DAMIÃO DA CUNHA[12] e PAULO SOARES[13] realçando a importância das medidas cautelares e de polícia na descoberta da verdade material, o facto de estarem processualmente previstas e a suscetibilidade de virem a ser integradas no processo. O segundo autor realça que apesar de quando da prática das medidas cautelares e de polícia não existir um processo formal, face à importância que assumem na investigação/processo penal, projetando-se neste, não se pode deixar de as considerar como atos processuais. Sublinha ainda que tais atos cautelares para se assumirem como processuais deverão ser materializados em auto, na aceção do disposto no artigo 99.º do Código de Processo Penal.

A nosso ver apesar da importância, indispensabilidade e essencialidade que caraterizam as medidas cautelares e de polícia no âmbito do processo-crime, não podemos deixar de concordar com a visão que caraterizam estes atos cautelares como atos extraprocessuais, cujo marco que assegura a aquisição da natureza processual consiste na apreciação e a necessária validação pela autoridade judiciária competente.

3. Das medidas cautelares e de polícia

3.1. Na Lei Processual Penal

Comunicação da notícia do crime – artigo 248.º do CPP

A iniciativa própria dos órgãos de polícia criminal define-se pela atuação em substituição precária da autoridade judiciária, baseada nos pressupostos de necessidade e de urgência, perante circunstâncias que exigem uma resposta pronta da entidade policial, pautada pelo princípio de eficácia, balizada por pressupostos legais, vinculada ao dever de ser transmitida imediata notícia à autoridade judiciária[14].

Logo que haja conhecimento de notícia de crime por parte do órgão de polícia criminal, recai sobre este a obrigação de a transmitir ao Ministério Público, no mais curto prazo possível, sem exceder os 10 dias, conforme o previsto nos artigos 243.º, n.º 3, 245.º e 248.º, n.º 1, todos do Código de Processo Penal e artigo 2.º, n.º 3, da Lei da Organização da Investigação Criminal (LOIC).

Toda e qualquer *noticia criminis* tem que ser comunicada, mesmo a manifestamente infundada[15] (artigo 248.º, n.º 2, do Código de Processo Penal), até porque é ao titular da ação penal que cabe decidir do fundamento ou não da notícia, e do destino a dar-lhe.

[12] O Ministério Público e os Órgãos de Polícia Criminal no Novo Código de Processo Penal, Porto, 1993, p. 143.
[13] Meios de Obtenção de Prova no Âmbito das Medidas Cautelares e de Polícia,2.ª edição, Coimbra, Almedina, 2017, pp. 95-96.
[14] Mesquita, Paulo Dá , Direcção do Inquérito e Garantia Judiciária, Coimbra: Coimbra Editora, 2003, pp. 120-143.
[15] Toda a notícia em que "*é evidente, patente, notório, que não contém indícios da prática de qualquer crime, concretamente, não contém nenhum dos elementos a que se reporta o artigo 243.º do Código de Processo Penal*." Lobo, Fernando Gama, Código de Processo Penal anotado, Coimbra, Almedina, 2015, p. 460.

A referência ao prazo limite de 10 dias para a comunicação da notícia do crime pelo órgão de polícia criminal surgiu com as alterações introduzidas pela Lei n.º 48/2007, de 29 de agosto, pelo que a anterior redação previa que a comunicação deveria ser feita no mais curto prazo. Alguns autores[16], referem a incompatibilidade do prazo de 10 dias face à Constituição, uma vez que poderá permitir as inconciliáveis ações de investigação criminal pré-processuais pelo órgão de polícia criminal, à margem do titular da ação penal, frustrando a estrutura do processo penal decorrente da dependência funcional do órgão de polícia criminal face ao Ministério Público. Bem como frustrando as garantias de defesa do arguido. Deste modo, tal prazo será inconstitucional por violação dos artigos 32.º, n.º 1 e 219.º, n.º 1, ambos da CRP. Nesse sentido, "*Afora a sua inconstitucionalidade, do ponto de vista prático e actualista, não se percebe o prazo instituído, já que as comunicações tornaram-se mais céleres e eficazes, não se justificando um prazo tão alargado*."[17].

Logo, impõe-se a comunicação imediata da notícia do crime ao Ministério Público, titular da ação penal, permitindo deste modo a direção do inquérito desde o início da investigação, promovendo-se *"o princípio da judiciariedade no âmbito criminal sob o primado jurisdicional*."[18].

Providências cautelares quanto aos meios de prova (Inspeção Judiciária) – artigo 249.º do CPP

Logo após ter conhecimento da possível ocorrência de um crime, ainda antes de obterem quaisquer diretrizes do Ministério Público no sentido de iniciarem as diligências para proceder a investigações, deve o órgão de polícia criminal praticar os atos necessários e urgentes para acautelar os meios de prova (artigo 249.º, n.º 1, do CPP).

O artigo 249.º, n.º 2, do CPP, enumera, de forma exemplificativa (dado a utilização do termo nomeadamente pelo legislador) alguns dos atos necessários e urgentes para acautelar os meios de prova. Entendemos que outros possa haver desde que fora da competência "*reservada da autoridade judiciária*"[19], ou seja, fora do conjunto de atos da competência exclusiva do juiz de instrução, que integram a reserva de juiz ou reserva de competência judicial, e fora do conjunto de atos que a lei expressamente determinar que sejam presididos ou praticados pelo Ministério Público[20].

Esta disposição legal (n.º 2 do artigo 249.º do Código de Processo Penal) prevê a inspeção ao local do crime ou também denominada inspeção judiciária, uma das mais importantes diligências efetuadas no âmbito do inquérito, consubstanciando o primeiro contacto com o evento criminoso que irá influenciar e condicionar a atividade investigatória subsequente[21].

[16] Valente, Manuel Guedes, Teoria Geral do Direito Policial, 5.ª edição, Coimbra: Almedina, 2017, pp. 368-370.
[17] Soares, Paulo, Meios de Obtenção de Prova no Âmbito das Medidas Cautelares e de Polícia,2.ª edição, Coimbra, Almedina, 2017, pp. 130-131.
[18] Expressão de Manuel Guedes Valente, ob. cit., p. 370.
[19] Expressão de Paulo Pinto de Albuquerque, ob. cit., p. 725.
[20] Cfr. Parecer do Conselho Consultivo da PGR n.º 45/2012, relator Paulo Dá Mesquita, disponível em www.dgsi.pt.
[21] Braz, José, Investigação Criminal: a organização, o método e a prova. Os desafios da nova criminalidade, 2.ª edição, Coimbra, Almedina, 2010, p. 202.

Pelo que, compete aos órgãos de polícia criminal[22]:

a) "*Proceder a exames dos vestígios do crime*", de modo a assegurar a preservação daqueles, impedindo que se alterem o estado das coisas e dos lugares. Para isso podem proibir a permanência ou trânsito de pessoas no local do crime bem como a prática de atos suscetíveis de destruir os vestígios. Podem, ainda determinar que uma ou mais pessoas permaneçam no local do crime (artigo 173.º do CPP).

b) "*Colher informações das pessoas*" que tenham presenciado os factos penalmente relevantes ou que por virtude de qualquer relação pessoal tenham conhecimento dos factos, tentando determinar as circunstâncias de modo, tempo e lugar, bem como determinar a identidade do agente do crime, com o objetivo de reconstituir o crime.

c) "*Proceder a apreensões no decurso de revistas ou buscas ou em caso de urgência ou perigo na demora"* de objetos do crime, adequados à sua prática. Deve ainda o órgão de polícia criminal assegurar a conservação ou manutenção dos objetos apreendidos, até à sua entrega à autoridade judiciária (interpretação conjugada do disposto nos artigos 249.º, n.º 2, alínea c) e 178.º, n.º 4, ambos do Código de Processo Penal).

A competência própria dos órgãos de polícia criminal, não se esgota aqui, pois o n.º 3 do mesmo artigo 249.º dispõe que mesmo após a intervenção da autoridade judiciária, devem, de igual modo, assegurar novos meios de prova de que tiverem conhecimento.

Na interpretação desta disposição legal surge a questão de saber se o legislador se quis referir às medidas cautelares e de polícia previstas nos artigos 248.º a 253.º do CPP ou se apenas se refere às medidas previstas no n.º 2 do artigo 249.º do CPP. O legislador também não especifica em que fases processuais se pode recorrer ao n.º 3 do artigo 249.º do CPP. Nesta fase de atuação policial o Ministério Público já teve notícia do crime e já promoveu a ação penal, já está em curso uma investigação de acordo com as regras processuais penais, sob a direção do Ministério Público. Existe a figura do procurador de turno, a quem os órgãos de polícia criminal podem recorrer no imediato quando surge um dado novo na investigação que estão a desenvolver. Pode ser equacionado até que ponto se justifica uma atuação por iniciativa própria, por parte dos órgãos de polícia criminal, já no decorrer do processo.

Aqui não se poderá fazer uma interpretação extensiva do disposto naquele n.º 3 do artigo 249.º, na medida em que estaríamos a admitir que se pretendeu alargar o âmbito da

[22] Considerando que a Polícia Municipal não exerce, em regra, funções de polícia judiciária, nem integra, em princípio, um órgão de polícia criminal, "*De acordo com o disposto no artigo 4.º, n.º 1, alínea f), da Lei n.º 19/2004, e do artigo 249.º, n.ºs 1 e 2, alínea c), do CPP, os órgãos de polícia municipal devem, perante os crimes de que tiverem conhecimento (em situação de flagrante delito) no exercício das suas funções, praticar os actos cautelares necessários e urgentes para assegurar os meios de prova, até à chegada do órgão de polícia criminal competente, competindo-lhes, nomeadamente, proceder à apreensão dos objectos que tiverem servido ou estivessem destinados a servir a prática de um crime, os que constituírem o seu produto, lucro, preço ou recompensa, e bem assim todos os objectos que tiverem sido deixados pelo agente no local do crime ou quaisquer outros susceptíveis de servir a prova (artigo 178.º, n.º 1, do CPP)*." - Parecer do Conselho Consultivo da PGR n.º 28/2008, relator Manuel Matos.

competência própria dos órgãos de polícia criminal, substituindo a autoridade judiciária, assumindo a investigação criminal como competência própria e com independência funcional. Tal situação conduziria a uma "*policialização*" do inquérito [23], representando uma violação do princípio da indisponibilidade das competências, uma vez que os órgãos de polícia criminal acabariam por assumir os poderes funcionais do Ministério Público, nomeadamente o poder funcional de dirigir a ação penal e o inquérito.

A interpretação que aqui deve ser feita, salvo melhor opinião, é no sentido do que for menos oneroso para os direitos e liberdades fundamentais do cidadão, enquanto arguido ou mero suspeito, respeitando o disposto no n.º 2 do artigo 18.º da Constituição da República Portuguesa (interpretação de acordo com o princípio *odiosa sunt restringenda*[24]*).*

Nesse sentido, consideramos que o legislador se quis referir aos meios descritos no n.º 2 do mesmo artigo, isto é, proceder a exames de vestígios do crime, colher informações das pessoas que facilitem a descoberta dos agentes do crime e a sua reconstituição, e proceder a revistas e buscas em caso de urgência ou *periculum in mora*.

Questão particular da recolha de informações junto do suspeito

No âmbito da função cautelar de recolha de informação, logo após a notícia do crime, os órgãos de polícia criminal podem recorrer ao agente do crime, sem conhecimento dessa qualidade, para obterem informação informal (dada a inexistência de inquérito) que vai permitir direcionar a investigação. Serão admissíveis os depoimentos dos órgãos de polícia criminal que recolheram tal informação? Como valorar tal prova?

Alguma jurisprudência[25] entende que as ditas conversas informais provenientes dos suspeitos poderão ser consideradas na fase das medidas cautelares e de polícia, quando ainda não existe inquérito nem arguido constituído, nos termos dos artigos 55.º, n.º 2, 248.º, n.º 1 e 249.º, n.º 1, alínea b), todos do CPP. Todavia, não podem aquelas ser consideradas e reproduzidas na audiência de julgamento, a partir do momento da constituição de arguido, ou seja, quando já foi instaurado inquérito, na justa medida em que a partir deste momento as declarações do arguido só poderão ser valoradas nos estritos termos indicados na lei.

Por outro lado, há jurisprudência que considera que as conversas informais entre arguido e os órgãos de polícia criminal, não têm valor de prova nem antes, nem depois da constituição formal do suspeito como arguido, vejam-se a título exemplificativo os acórdãos: Ac. da Relação de Guimarães, proc. n.º 670/07PBGMR.G1, de 31-05-2010 e Ac. da Relação de Lisboa, proc. n.º 146/09.0PHOER.L1-5, de 03-05-2011[26].

[23] Cfr. Valente, Manuel Guedes, Do Ministério Público e da Polícia - Prevenção Criminal e Acção Penal como Execução de uma Política Criminal do Ser Humano , Lisboa, UCE, 2013, p. 271.
[24] Valente, Manuel Guedes, Do Ministério Público e da Polícia - Prevenção Criminal e Acção Penal como Execução de uma Política Criminal do Ser Humano, Lisboa: UCE, 2013, p. 440.
[25] Em específico Ac. do STJ, proc. n.º 04P902, de 22-04-2004; Ac. do STJ, proc. n.º 06P4593, de 15-02-2007; Ac. do STJ, proc. n.º 886/07.8PSLSB.L1.S1, de 03-03-2010; Ac. da Relação de Coimbra, proc. n.º 370/08.2TACVL.C1, de 30-03-2011, Ac. da Relação de Lisboa, proc. n.º 35/07.2PJAMD.L1-5, de 24-01- 2012, disponíveis em www.dgsi.pt.
[26] Disponíveis em www.dgsi.pt.

Na verdade, entendemos ser de perfilhar a jurisprudência enunciada no Acórdão do Tribunal da Relação de Coimbra de 16-06-2015[27]: "*I. Devendo os órgãos de polícia criminal colher, inter alia, notícias do crime, descobrir os seus agentes e praticar os actos cautelares necessários e urgentes para assegurar os meios de prova (cfr. art.ºs 55.º, n.º 2, 249.º e 250.º do CPP), nada impede que, uma vez assegurados os direitos de defesa do arguido, os mesmos órgãos reproduzam as diligências efectuadas e as conversas tidas, nos referidos âmbitos, em audiência de discussão e julgamento. II. Neste contexto, nem o depoimento é indirecto - os órgãos de polícia criminal apenas relatam em tribunal o que os seus sentidos percepcionam -, nem está abrangido pela proibição de prova do art.º 356.º, n.º 7. III. Tão pouco esse depoimento frustra o direito ao silêncio do arguido*.".

E a do Acórdão do Tribunal da Relação de Coimbra de 15-02-2012[28]: "*1.Não constitui depoimento indirecto - portanto, não enquadrável no art.º 129º, do C. Proc. Penal e, portanto, não constituindo prova proibida -, o depoimento de uma testemunha que relata o que ouviu o arguido dizer, isto mesmo que o arguido não preste declarações na audiência, no exercício do seu direito ao silêncio*.".

O depoimento de órgão de polícia criminal sobre informações colhidas informalmente de alguém que ainda não é suspeito, uma vez que não existe qualquer indício conhecido de que é o agente do crime, é admissível e valorável ao abrigo do princípio da livre apreciação da prova, como qualquer outra prova testemunhal.

O artigo 129.º do Código de Processo Penal proíbe os testemunhos que pretendem ultrapassar o silêncio do arguido e não o relato pelos órgãos de polícia criminal das diligências desenvolvidas durante a pura recolha informal de indícios[29].

Até porque as declarações produzidas neste contexto por qualquer pessoa abordada no decurso de operação policial, não traduzem declarações *stricto sensu* para efeitos processuais, já que não existe verdadeiramente um processo penal a correr os seus termos. São pura e simplesmente medidas cautelares e de polícia, que visam a aquisição e conservação de prova, de modo lícito, dada a sua conformidade com o disposto no artigo 249.º do CPP, e por essa razão não é proibido o seu relato em audiência[30].

Situação oposta é quando a informação tem como fonte o agente do crime, havendo já fundadas suspeitas da sua prática pela fonte de informação. Aqui, uma vez que deve esta pessoa ser constituída arguida, qualquer declaração daquele que já deveria ter sido constituído como arguido não pode ser utilizada como prova, nos termos do disposto do nº 5 do artigo 58º do Código de Processo Penal.

[27] Relatora Cacilda Sena, disponível em www.dgsi.pt.
[28] Relator Paulo Guerra, disponível em www.dgsi.pt.
[29] Neste sentido Acórdão do STJ, de 15.02.2007, Relator Maia Costa.
[30] Neste sentido Acórdão do Tribunal da Relação de Lisboa de 22-06-2017, relatora Filipa Costa Lourenço.

Fundamentando esta tese, seguimos a opinião de PAULO SOARES[31], no sentido de que o disposto no artigo 250.º, n.º 8, do Código de Processo Penal, que a seguir abordaremos, atribui aos órgãos de polícia criminal o poder de solicitarem informações úteis, a qualquer pessoa, inclusive ao suspeito, relativas ao crime e à descoberta e conservação de meios de prova que poderiam perder-se antes da intervenção da autoridade judiciária. No caso do suspeito será de ressalvar o previsto no artigo 59.º do Código de Processo Penal, ou seja, logo que no processo de recolha de informação surjam fundadas suspeitas de que a fonte de informação é o agente do crime, a recolha de informação terá que ser suspensa e essa pessoa constituída arguida, sob pena dessa prova não poder ser valorada.

Identificação de suspeito e pedido de informações – artigo 250.º do CPP

O ato de identificar um qualquer cidadão, titular de direitos fundamentais constitucionalmente consagrados, consiste na limitação do seu direito à liberdade de circulação[32] e uma interferência na sua reserva de identidade. A *"identidade é uma das matérias protegidas da vida privada, podendo, quanto a nós, falar-se numa verdadeira «reserva de identidade». Sem que haja uma obrigação imposta por lei, e esta se situe dentro dos parâmetros constitucionais, ninguém pode ser forçado a declinar e, muito menos, a exibir prova do nome ou de qualquer outro dado de identificação."* [33].

Da conjugação do artigo 250.º do Código de Processo Penal com o 27.º, n.º 3, alínea g), da Constituição da República Portuguesa[34], retira-se que os órgãos de polícia criminal podem proceder à identificação de qualquer pessoa que se encontre em lugar público, aberto ao público ou sujeito a vigilância policial, desde que se reúnam determinados pressupostos. No plano subjetivo (artigo 250.º, n.º 1, do Código de Processo Penal) a existência de fundadas suspeitas:

– Da prática de crime;
– Da pendência de um processo de extradição ou expulsão;
– De que tenha penetrado ou que permaneça de forma irregular em território nacional;
– Ou ainda, que haja contra si um mandado de detenção.

Antes de proceder à identificação, o órgão de polícia criminal deve provar a sua qualidade identificando-se, comunicar ao suspeito as circunstâncias fáctico-jurídicas que fundamentam a obrigação de identificação e por último indicar os meios através dos quais se pode identificar.

A identificação far-se-á através dos meios documentais e testemunhais, sucessivamente, previstos nos n.ºs 3, 4, e 5 do artigo 250.º.

---

[31] Ob. cit., p. 149.
[32] Neste sentido, cfr. Valente, Manuel Guedes, Teoria Geral do Direito Policial, 5.ª edição, Coimbra, Almedina, 2017, p. 377.
[33] Cfr. Pinheiro, Alexandre Sousa e Oliveira, Jorge Menezes de, O bilhete de Identidade e os Controlos da Identidade, Revista do Ministério Público, Ano 15, n.º60, Outubro/Dezembro de 1994, p. 37.
[34] *"3. Exceptua-se deste princípio a privação da liberdade, pelo tempo e nas condições que a lei determinar, nos casos seguintes: g) Detenção de suspeitos, para efeitos de identificação, nos casos e pelo tempo estritamente necessários;"*

A identificação de suspeito de nacionalidade portuguesa deve ser feita através de bilhete de identidade, cartão do cidadão ou passaporte. A identificação de suspeito estrangeiro deve ser feita através da exibição do título de residência, passaporte ou documento que substitua o passaporte – artigo 250.º, n.º 3, do Código de Processo Penal.

Verificada a impossibilidade de apresentação dos documentos referidos no artigo anterior, estatui o n.º 4 do artigo 250.º do mesmo diploma legal que o suspeito se pode identificar apresentando documento original, ou cópia autenticada, que contenha o seu nome completo, a sua assinatura e a sua fotografia.

Se o suspeito não for portador de nenhum documento de identificação, pode fazê-lo mediante comunicação com uma pessoa que apresente os seus documentos, pode deslocar-se, acompanhado pelo órgão de polícia criminal, até ao local onde se encontram os seus documentos ou pode ver a sua identidade reconhecida por uma pessoa que possa ser identificada pelos meios já referidos e que garanta a veracidade dos dados pessoais fornecidos pelo suspeito – artigo 250.º, n.º 5, do CPP.

Se mesmo assim não for possível identificar o suspeito, pode o órgão de polícia criminal de acordo com o disposto no n.º 6 do artigo 250.º, conduzir o mesmo até ao posto policial mais próximo e fazê-lo permanecer nesse local somente pelo tempo estritamente necessário, nunca superior a seis horas. Este prazo de seis horas começa a contar, salvo melhor opinião, desde o momento exato em que o cidadão foi intercetado pelo órgão de polícia criminal, momento em que a sua liberdade fica limitada.[35] Tendo em vista a sua identificação, o suspeito, pode ser levado a realizar provas dactiloscópicas, fotográficas ou de natureza análoga[36] e pode-lhe ser pedido que indique residência através da qual possa ser encontrado e receber comunicações.

Neste âmbito, de relevar a faculdade de o identificando poder contactar com pessoa da sua confiança (artigo 250.º, n.º 9, do Código de Processo Penal), enquanto imperativo essencial e crucial na atuação do órgão de polícia criminal.[37]

Importa, ainda, mencionar que, no âmbito do disposto no n.º 8 do artigo 250.º do Código de Processo Penal, o suspeito (sem prejuízo do disposto no artigo 59.º do CPP, quanto à constituição de arguido) ou qualquer pessoa que esteja em posição de fornecer informações úteis, deve fazê-lo quando solicitado por órgão de polícia criminal, na medida em que estas sejam relevantes e relacionadas com um crime, bem como relacionadas com a descoberta e conservação de meios de prova, que poderiam dissipar-se antes da intervenção da autoridade judiciária.

[35] Neste sentido, Cfr. Valente, Manuel Guedes, Teoria Geral do Direito Policial, 5.ª edição, Coimbra: Almedina, 2017, p. 380.
[36] Não se inclui neste conceito de provas de natureza análoga as perícias que incidam sobre características físicas por força do disposto no artigo 154.º, n.º 3 e 269.º, n.º 1, alínea b), ambos do Código de Processo Penal, na medida em que estamos perante atos de reservados ao juiz de instrução.
[37] Neste sentido, Cf. Valente, Manuel Guedes, Teoria Geral do Direito Policial, 5.ª edição, Coimbra: Almedina, 2017, p. 382.

Perante a recusa de identificação de suspeito para prática do crime que consequências legais podemos retirar?

Alguns autores, designadamente LEAL HENRIQUES e SIMAS SANTOS [38], cominam tal conduta como crime de desobediência, previsto e punido pelo disposto no artigo 348.º, n.º 1, alínea b), do Código Penal, por estarmos perante a violação de um dever de identificação. Também neste sentido Parecer n.º 13/96 do Conselho Consultivo da PGR[39].

No entanto por três fundamentos não entendemos que tal possa acontecer.

Em primeiro lugar, com respeito pelo princípio da tipicidade, se o legislador quisesse que o suspeito que se recusa a identificar incorresse em responsabilidade penal, tê-lo-ia previsto.

A possibilidade de detenção para identificação, como acima se descreveu, afasta a ideia de em caso de recusa de identificação se poder considerar consumado o crime de desobediência, " *a detenção para identificação – em que o OPC tem legitimidade de conduzir um indivíduo para identificação, sendo privado da liberdade – afasta, por completo, a ideia de que a recusa à identificação, mesmo com cominação, consubstancia um crime de desobediência* (…) *a posição doutrinária de que a recusa à identificação gera crime de desobediência mostra-se contrária à ideia de detenção para identificação e não faz sentido que, sendo possível deter para identificar se opte por deter pela prática do crime de desobediência*" [40].

Por outro lado, com a entrada em vigor da redação dada ao artigo 250.º pela Lei n.º 59/98, de 25 de agosto, que visou resolver as dificuldades de conjugação da sua previsão anterior com o estipulado na Lei n.º 5/95, de 21 de fevereiro, assim se eliminando as incertezas e ambiguidades numa matéria que se prende diretamente com direitos fundamentais, revogou tacitamente esta lei (n.º 5/95), que no seu artigo 2.º, n.º 1, veio estabelecer a obrigatoriedade do porte de documento de identificação. Neste sentido se pronunciou o Parecer nº 161/2004 do Conselho Consultivo da PGR[41].

Refira-se que o texto final daquele artigo 1.º da Lei nº 5/95, de 21 de fevereiro, que instituiu a obrigatoriedade do porte do documento de identificação (que como acima o dissemos, norma que se mostra, assim, tacitamente revogada com a alteração do artigo 250.º, n.º 1, do CPP, introduzida pela citada Lei n.º 59/98), resultou de o Tribunal Constitucional, em sede de apreciação preventiva, ter declarado a inconstitucionalidade das normas conjugadas do artigo 1.º, n.º 1 e 3.º, n.º 1, constante da anterior Decreto nº 161/VI da Assembleia da República, enquanto autorizavam que uma pessoa insuspeita da prática de qualquer crime e em local não frequentado habitualmente por delinquentes, pudesse ser sujeita a identificação policial, com base na invocação de razões de segurança interna, através de procedimento susceptível de o vir a privar da liberdade, por um período até seis horas, por violação do disposto no artigo

[38] Apud Soares, Paulo, Meios de Obtenção de Prova no Âmbito das Medidas Cautelares e de Polícia, 2.ª edição, Coimbra, Almedina, 2017′ p. 181.
[39] Publicado no Diário da República, II série, n.º 286, de 12 de dezembro de 1997.
[40] Cf. Valente, Manuel Guedes, Teoria Geral do Direito Policial, 5.ª edição, Coimbra: Almedina, 2017, p. 380.
[41] Publicado no DR II Série de 11.01.2008, com a retificação nº 198/2008 (quanto ao número do parecer), publicada no DR II Série de 6.02.2008.

27.º, n.ºs 1, 2 e 3 da Constituição - Acórdão do TC nº 479/94, de 7 de julho, publicado no DR. Iª Série A, de 28.08.1994.

Podemos então concluir que apesar de existir a obrigação de identificação por parte de pessoa encontrada em lugar público, aberto ao público ou sujeita a vigilância policial, sempre que sobre ela recaiam fortes suspeitas da prática de crime, da pendência de processo de extradição ou de expulsão, de que tenha penetrado ou permaneça irregularmente no território nacional ou de haver contra si mandado de detenção, a sua recusa em identificar-se não legitima o recurso, por parte dos órgãos de polícia criminal, à ordem de identificação e, consequentemente, à cominação de a mesma incorrer na prática de crime de desobediência, devendo antes, nessa eventualidade, serem desencadeados os procedimentos previstos no artigo 250.º do CPP, tendo em vista a identificação do suspeito.

Uma outra questão emerge, esgotadas todas as diligências previstas no artigo 250.º e mantendo-se a recusa de identificação do suspeito haverá aqui incriminação dessa conduta com tipo legal desobediência?

Esta questão foi levantada no parecer n.º 28/2008 do Conselho Consultivo da PGR, relator Manuel Matos[42], que nos esclarece: *"Consideramos também que um eventual recurso ao mecanismo compulsório facultado pelo artigo 250.º do CPP não impede a incriminação daquela conduta. Os procedimentos aí previstos podem, de resto, revelar-se ineficazes para o apuramento da identidade. Assim, como também se pondera naquele parecer* (n.º 13/96*), «tal não impede, a nosso ver, que esgotados sem êxito os meios compulsórios referidos [naquele preceito] e reiterada a ordem de identificação, o indivíduo renitente não venha a cometer o crime de desobediência*» *"*.

Revistas e Buscas Cautelares – artigo 251.º do CPP

A revista[43] enquanto medida cautelar e de polícia apenas pode ser efetuada, nos casos previstos no n.º 1 do artigo 251.º do CPP: alínea a) deve ser levada a cabo em caso de fuga iminente ou caso tenha ocorrido a detenção dos visados, sendo que tem como pressupostos a existência de fundadas suspeitas de que o suspeito ou o detido oculta em si mesmo objetos relacionados com o crime e que podem servir de prova e que, de outra forma, se poderiam perder; e a alínea b) prevê a revista cautelar (ou de segurança) como meio de prevenção de práticas criminosas durante atos processuais ou nos casos em que o suspeito deva ser conduzido ao posto policial.

A busca[44] pode revestir um carácter cautelar e de urgência, também por via do artigo 251.º, n.º 1, alínea a), do Código de Processo Penal, impondo-se como pressupostos: não seja busca domiciliária; que deve recair sobre suspeito em caso de fuga iminente ou sobre o detido; que terá de existir fundada razão de que naquele local se ocultam objetos relacionados com o

[42] Disponível em www.dgsi.pt.
[43] As revistas consistem em proceder à inspeção minuciosa de uma pessoa, a qualquer hora do dia ou da noite, para se verificar se a mesma oculta ou não objetos relacionados com o crime ou que possam servir de prova daquele.
[44] Medida a ser desenvolvida por órgão de polícia criminal no intuito de obter indícios probatórios, que se realiza em locais reservados ou não livremente acessíveis ao público, suscetíveis de servirem de prova em processo penal.

crime; que esses objetos têm de ser suscetíveis de servirem de prova; que se a busca não se efetivasse aqueles poder-se-iam perder, ou seja, a utilidade da diligência desapareceria.

O artigo 251.º, n.º 1, alínea a), do Código de Processo Penal é uma disposição processual de natureza eminentemente cautelar, voltada para situações de emergência em que a suspeita de existência de prova de um crime não se compadece com demoras sob pena da sua evaporação, a sua aplicação tem de bastar-se com tal suspeita, seja ela anterior ou concomitante à intervenção da autoridade judiciária, desde que suportada em fundamento razoável e que, pela natureza das coisas, nem sequer carece de ser isenta de toda a dúvida.

Uma nota para a alínea b) deste artigo 251.º do Código de Processo Penal, que apesar da sua localização sistemática, trata-se de uma medida preventiva que visa estabelecimento de segurança em determinado local e não o acautelamento de meio de prova, e por isso também denominada por revista de segurança.

A execução destas medidas cautelares deve ser comunicada de imediato ao juiz de instrução nos termos do n.º 6 do artigo 174.º do CPP, conforme resulta do n.º 2 do artigo 251.º, significando assim que está sujeita a controlo jurisdicional.

Como refere GERMANO MARQUES DA SILVA[45], tal validação pelo juiz de instrução não deixa de ser "*anómala*", considerando que cabe ao Ministério Público ordenar revistas e buscas não domiciliárias.

Segundo PAULO PINTO DE ALBUQUERQUE[46] este n.º 2 deve sofrer uma interpretação restritiva no sentido de que a fiscalização das diligências urgentes realizadas por órgão de polícia criminal apenas ser da competência do juiz na fase de instrução e em virtude de que a remissão desta disposição legal excede o espirito da lei, "*que consiste em deferir ao Ministério Público a competência, na fase de inquérito, para ordenar essas diligências (artigo 270.º, n.º2, d)).*"[47].

Apreensão de correspondência – artigo 252.º do CPP

A apreensão de correspondência prevista no artigo 252.º, n.º 1, do Código de Processo Penal, consagra a regra de que a apreensão de correspondência só poder ter lugar quando o juiz autorizar ou ordenar. E o juiz que autorizou ou ordenou apreensão de correspondência pelos órgãos de polícia criminal, deve recebê-la intacta tornando-se assim a primeira pessoa a conhecer o conteúdo da correspondência, tal como previsto no artigo 179.º do mesmo Código.

Perante a necessária autorização do juiz para que o órgão de polícia criminal possa apreender correspondência parece-nos não ser adequada a integração deste preceito no âmbito das

[45] Cfr. Do Processo Penal Preliminar, Lisboa,Univ. Católica Portuguesa, Faculdade de Direito, 1990, p. 120.
[46] Comentário do Código de Processo Penal, 4.ª edição, pp. 692-693.
[47] Gaspar, António Henriques; Cabral, José António Henriques dos Santos; E outros., Código de Processo Penal comentado, 2.ª Edição, Almedina, 2015, p. 894.

medidas cautelares e de polícia, pois não se tratam de atos pré-processuais e de competência originária, tratando-se assim de um ato ordenado ou autorizado por autoridade judiciária[48].

O órgão de polícia criminal pode, por sua iniciativa própria, informar o juiz da existência de fundadas razões para crer que determinadas encomendas ou valores fechados, possam conter informações úteis para a investigação de um crime ou conduzir à sua descoberta e que cuja utilidade se pode perder em caso de demora (artigo 252.º, n.º 2, do Código de Processo Penal), o qual pode autorizar a abertura imediata da correspondência.

Esta iniciativa dos órgãos de polícia criminal surge com fundamento no perigo resultante da demora e nos critérios de necessidade e urgência, estando sujeita a posterior apreciação e validação judicial.

Para MANUEL GUEDES VALENTE o preceituado no n.º 2 do artigo 252.º do CPP não é uma verdadeira medida cautelar e de polícia pois "*o n.º 2 do art.º 252.º do CPP se correlaciona e entrelaça com o n.º 1 do mesmo preceito, i.e., a abertura de correspondência nos termos do n.º 2 do art.º 252.º do CPP – acto exclusivo do juiz [n.º 1 do art.º 179.º do CPP e al. b) do n.º1 do art.º 269.º do CPP ex vi do n.º 4 do art.º 32.º da CRP] – só pode cingir-se à abertura por ordem daquele e à correspondência apreendida por ordem ou autorização do mesmo*"[49].

O órgão de polícia criminal pode, por sua iniciativa, proceder à suspensão da remessa de qualquer correspondência nas estações de correios e de telecomunicações, com base em fundadas razões para crer que estes possam conter informações úteis para a investigação de um crime ou conduzir à sua descoberta e cuja utilidade se pudesse perder em caso de demora – artigo 252.º, n.º 3, do CPP.

A atuação do órgão de polícia criminal terá que ter em consideração os requisitos cumulativos previstos nas alíneas a) a c) do n.º 1 do artigo 179.º do Código de Processo Penal, isto é, a correspondência suspensa ter sido expedida pelo suspeito ou lhe ser dirigida, mesmo que sob nome diverso ou através de pessoa diversa; Estar em causa crime punível com pena de prisão superior, no seu máximo, a 3 anos; e a diligência se revelar de grande interesse para a descoberta da verdade ou para a prova.

Esta suspensão tem de ser convalidada por despacho fundamentado do juiz, no prazo de quarenta e oito horas, sob pena de ser remetida ao destinatário.

A lei é clara no sentido de não poder ocorrer apreensão de correspondência sem prévia intervenção do juiz, apenas sendo legalmente permitida a medida cautelar de suspensão da sua remessa.

A apreensão realizada fora dos trâmites deste artigo 252.º, é nula por força do disposto no artigo 179.º, n.º 1, do Código de Processo Penal. Trata-se de nulidade atinente a meio de

[48] Neste sentido Cf. Valente, Manuel Guedes, Teoria Geral do Direito Policial, 7.ª edição, Coimbra: Almedina, 2017, pp. 260-261.
[49] Cf. Valente, Manuel Guedes, Teoria Geral do Direito Policial, 5.ª edição, Coimbra: Almedina, 2017, p. 261.

prova, não segue o regime do artigo 122.º do Código de Processo Penal, mas antes dos artigos 125.º e 126.º, n.º 3, ambos do Código de Processo Penal que proíbem as provas obtidas mediante intromissão na correspondência sem consentimento do titular e fora da previsão dos referidos preceitos que delimitam os casos em que pode ser realizada a sua apreensão.

Localização celular – artigo 252.º-A do CPP

O artigo 252.º-A, introduzido com a reforma de 2007, dispõe que as autoridades judiciárias e as autoridades de polícia criminal[50], mediante um critério de necessidade, podem obter informações sobre localização celular quando esta se mostre necessária para acautelar bens jurídicos fundamentais, como são a vida e a integridade física grave (n.º 1).

Os dados de localização celular, conforme a definição dada pelo artigo 2.º, n.º 1, alínea e), da Lei n.º 41/2004, de 18 de agosto, são *"quaisquer dados tratados numa rede de comunicações eletrónicas ou no âmbito de um serviço de comunicações eletrónicas que indiquem a posição geográfica do equipamento terminal de um utilizador de um serviço de comunicações eletrónicas acessível ao público*;" estes dados fazem parte dos denominados por dados de tráfego, definidos pelo disposto no artigo 2.º, n.º 1, alínea d), do mesmo diploma legal, constituindo elementos funcionalmente necessários ao estabelecimento e à direção da comunicação.

São elementos inerentes à própria comunicação permitindo identificar, em tempo real ou à *posteriori*, a localização do equipamento de telecomunicação.

Em conformidade com a Diretiva n.º 2002/58/CE, a Lei n.º 41/2004 considera os dados de localização que fornecem a posição geográfica do equipamento terminal como dados de tráfego apenas na medida em que sejam estritamente tratados pela rede móvel para permitir a transmissão de comunicações, ficando fora desta classificação os dados de localização que são mais precisos do que o necessário para a transmissão das comunicações e que são utilizados para a prestação de serviços de valor acrescentado, tais como serviços que prestam aos condutores informações e orientações individualizadas sobre o tráfego (artigos 2.º, alíneas d), e) e f), 6.º e 7.º)[51].

A localização celular cautelar supõe a existência de um perigo para a vida ou para a integridade física grave de quem está, pode estar, ou pode vir a ser vítima de um ato ilícito criminal, associado à criação de um risco de morte ou grave lesão da integridade física e seja ou se suponha ser detentor de um dispositivo móvel de comunicação detetável por localização celular.
O caso paradigmático será o rapto ou sequestro, com ou sem pedido de resgate, mas sempre com existência de ameaça, de perigo para a vida ou integridade física.

[50] Conforme definido no artigo 1.º, alínea d), do Código de Processo Penal: "*os directores, oficiais, inspectores e subinspectores de polícia e todos os funcionários policiais a quem as leis respectivas reconhecerem aquela qualificação*;".
[51] Veja-se Acórdão do Tribunal Constitucional n.º 486/2009, publicado em Diário da República n.º 215/2009, Série II de 2009-11-05, disponível em http://www.tribunalconstitucional.pt/tc/acordaos/.

Supõe-se para a aplicação do artigo 252.º-A do Código de Processo Penal, a existência de uma "*vítima*" no sentido da alínea c) do nº 4 do artigo 187.º do Código de Processo Penal, a existência de um perigo (em sentido amplo, risco, ameaça, situação potenciadora de violação da vida e integridade física) para a vida e a integridade física grave desse alguém e a possibilidade de a localização celular obviar à concretização desse perigo.

Não se exige a existência de um processo nem a definição de um suspeito dos supostos crimes. Nem tão pouco se supõe existente um crime concreto já consumado, mas apenas a simples mas séria possibilidade da sua existência e da existência de uma "*vítima*", cujo perigo para a sua vida ou integridade física não se tenha concretizado.

Os sistemas de comunicações de redes móveis "*assentam numa estrutura celular que consiste na instalação de emissores para assegurar a cobertura de uma determinada área geográfica e utilizam tecnologia digital designada por rede GSM (Global System for Mobile communications). Os equipamentos de uma rede GSM desempenham várias funções, designadamente, a gestão da mobilidade dos terminais. A zona de influência de uma rede GSM está dividida em várias áreas designadas por células que correspondem à área servida por uma antena e que são identificadas por um identificador, CGI (Cell Global Identity). Essas células são agregadas em áreas de localização, LA (Location Area), que têm o seu identificador, LAI (Location Area Identity). A estação móvel é composta pelo equipamento móvel e pelo SIM (Subscriber Identity Module), o qual, basicamente, é um cartão que permite a identificação do cliente perante a rede através do IMSI (Internacional Mobile Subscriber Identity). Os próprios equipamentos terminais (telemóveis) têm um identificador único conhecido pela sigla IMEI (International Mobile Equipment Identity) que permite identificar a sua utilização numa rede GSM. A área de localização (LA) é utilizada para localizar o terminal móvel, pois a informação que está registada sobre o estado de atividade do terminal indica qual a área de localização em que o IMEI foi detetado. Durante a fase de arranque, a estação móvel inicia uma acção de actualização de localização, enviando a sua identificação para a rede. Quando se desloca para uma nova área, ocorre uma atualização de localização (location update) e a identificação da nova área é fornecida para a rede. A localização celular dispensa a realização de chamadas telefónicas, bastando para o efeito que o equipamento móvel esteja ligado e, portanto, conectado à rede. A localização celular dos equipamentos móveis, ao permitir a gestão dos equipamentos que acedem à rede, constitui condição indispensável para o estabelecimento e transmissão das comunicações, quer durante a fase de arranque da estação móvel, quer quando ocorre uma mudança de área. Os dados de localização celular podem incidir sobre a latitude, a longitude e a altitude do equipamento terminal do utilizador, a identificação da célula de rede em que o equipamento terminal está localizado em determinado momento e sobre a hora de registo da informação de localização. De tudo isto decorre que a localização celular revela, por via da observação da sua ligação à rede telefónica móvel, a localização de um detentor de um determinado aparelho telefónico e, portanto, permite conhecer o percurso físico que fez ou está a fazer, ou então revela a sua mobilidade ou permanência num determinado local. Por isso se pode dizer que, em certa medida, a localização celular tem uma finalidade probatória semelhante à das tradicionais vigilâncias policiais sobre pessoas."* – vide Acórdão do Tribunal da Relação do Porto, Processo 2063/14.2JAPRT-A.P1, Relator Neto de Moura.

Importa saber que tipos legais legitimam a utilização desta medida cautelar de localização celular, da leitura do preceito parece-nos que o legislador quis limitar a sua utilização ao catálogo de crimes contra as pessoas, em específico contra a vida e contra a integridade física. Enquadrando-se neste catálogo os crimes de sequestro, rapto, escravidão, tráficos de pessoas, e contra a liberdade e autodeterminação sexual, mas a cláusula aberta perigo para a vida ou

de ofensa à integridade física grave poderão incluir crimes que também afetem estes bens jurídicos, quer de forma direta ou indireta, como seja o terrorismo[52].

Este artigo tem duas partes distintas, que PAULO PINTO DE ALBUQUERQUE[53] carateriza como matéria de processo penal, no caso do n.º 2, e matéria de prevenção criminal, no caso do n.º 3.

O n.º 2 do artigo 252.º-A do CPP diz-nos que caso se trate de uma localização celular referente a um processo em curso, a sua obtenção deve ser comunicada ao juiz no prazo máximo de quarenta e oito horas.

Por outro lado, o n.º 3 do artigo 252.º-A do CPP faz alusão aos dados sobre a localização celular que não se referem a nenhum processo em curso, cuja comunicação deve ser feita ao juiz da sede da entidade competente para a investigação criminal.

O mesmo autor defende a inconstitucionalidade do n.º 3 do artigo 252.º-A, por violação do disposto no n.º 4 do artigo 34.º da Constituição da República Portuguesa ("*é proibida toda a ingerência das autoridades públicas na correspondência, nas telecomunicações e nos demais meios de comunicação, salvos os casos previstos na lei em matéria de processo criminal* "). Considerando que para a localização celular ser utilizada tem de existir já um processo em curso, nunca antes da sua existência, e não pode ser utilizada para fazer "*pura prevenção criminal*".

Por outro lado, PAULO SOARES[54] defende que apenas os dados de localização associados a uma comunicação efetivada ou tentada, entre pessoas, goza da tutela da inviolabilidade das comunicações eletrónicas, constitucionalmente tutelado pelo artigo 34.º, n.º 1 e 4. Considera ainda que no caso da localização celular existe apenas uma comunicação entre máquinas, entre o telemóvel e os lacetes locais das redes de telecomunicações móveis. Logo, tal medida não se inclui no âmbito tutela da inviolabilidade das comunicações eletrónicas mas constitui uma restrição do direito à reserva da intimidade da vida privada e familiar (artigo 26.º, n.ºs 1 e 2, da CRP), constitucionalmente legitimada pelo artigo 18.º, n.ºs 2 e 3, uma vez que se trata de uma medida prevista na lei e se demonstra necessária, adequada e proporcional à salvaguarda da vida e da integridade física.

Por último, a consequência jurídica para a obtenção de dados de localização em violação do disposto no artigo 252.º-A, n.ºs 1 a 3, é a nulidade, constituindo uma proibição de prova, prevista no artigo 32.º, n.º 8, da Constituição da República Portuguesa e 126.º, n.º 3, do Código de Processo Penal, no entanto pode ser suprida pelo consentimento do respetivo titular[55].

[52] Neste sentido Cf. Valente, Manuel Guedes, Teoria Geral do Direito Policial, 5.ª edição, Coimbra, Almedina, 2017, pp. 399-400.
[53] Cf. Paulo Pinto de Albuquerque, ob. cit., p. 671.
[54] Meio de Obtenção de Prova no Âmbito das Medidas Cautelares e de Polícia, 2.ª edição, Coimbra, Almedina, 2017, p. 278.
[55] Ver neste sentido Cf. Paulo Pinto de Albuquerque, ob. cit, p. 673 e Manuel Guedes Valente, ob. cit., p. 403.

3.2. Na Lei do Cibercrime

A prova digital[56] é altamente volátil, por vezes basta um simples premir de tecla ou execução de programa para a fazer desaparecer. Alguns tipos de dados informatizados são armazenados por curtos períodos de tempo, e noutras situações se as provas não forem colhidas rapidamente, tal poderá originar prejuízos significativos para pessoas e bens.

A Lei do Cibercrime (LC) consagra um regime processual penal potencialmente dirigido a todos os crimes[57], no entanto não existe qualquer capítulo dedicado em exclusivo às medidas cautelares e de polícia, tal como sucede no Código de Processo Penal, mas da leitura das normas depreendemos da existência das seguintes medidas:

– Preservação expedita de dados, artigo 12.º, n.º 2;
– Revelação expedita de dados de tráfego, artigo 13.º;
– Apreensão de dados informáticos, artigo 16.º, n.º 2; e
– Preservação e revelação expeditas de dados informáticos em cooperação internacional, artigo 22.º, n.º 4.

Preservação expedita de dados[58] – artigo 12.º, n.º 2, da LC

A preservação expedita de dados visa essencialmente impedir a perda, destruição ou modificação de dados informáticos[59], não a obtenção de dados informáticos em si mesmo, mas apenas impõe a obrigação de quem tem acesso e controlo desses dados a preservá-los por um determinado período de tempo. Tal processo também é denominada por "*quick freeze*"[60], obrigando os fornecedores a "congelarem" os dados perante essa notificação. Não quer com isto dizer que os operadores tornem os dados inacessíveis, mas o seu acesso se fará apenas de acordo com as especificações que foram estabelecidas na ordem[61].

---

[56] *«[a] prova electrónico-digital pode definir-se como qualquer tipo de informação, com valor probatório, armazenada [em repositório electrónico-digitais de armazenamento] ou transmitida [em sistemas e redes informáticas ou redes de comunicações electrónicas, privadas ou publicamente acessíveis], sob a forma binária ou digital» (cfr.* RODRIGUES, Benjamim Silva Rodrigues, Direito Penal. Parte Especial, I, "Direito Penal Informático-Digital", Coimbra, Coimbra Editora, 2009, p. 39.)

[57] O âmbito material de aplicação das medidas cautelares tem alcance a nível dos crimes informáticos, cometidos por meio de um sistema informático ou em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico (artigo 11.º, n.º 1, da Lei do Cibercrime).

[58] Quanto a esta matéria de especial relevância a nota prática n.º 8/2016, de 18 de fevereiro, do gabinete de cibercrime da PGR.

[59] Definidos no artigo 2.º, alínea b), da Lei do cibercrime: "*qualquer representação de factos, informações ou conceitos sob uma forma susceptível de processamento num sistema informático, incluindo os programas aptos a fazerem um sistema informático executar uma função.*" Podemos estar perante documentos eletrónicos (art. 2.º, alínea a) do DL n.º 290/99, de 02/08), programa de computador (DL n.º 252/94, de 20/10), dados pessoais (art. 3.º, alínea a), da Lei n.º 67/98, de 26/10), dados de tráfego e dados de localização (artigo 2.º, n.º 1, alíneas c) e e), da Lei n.º 41/2004, de 18/08, respetivamente).

[60] RODRIGUES, Benjamim Silva, Da Prova Penal – Tomo IV, Da Prova Electrónico-Digital e da Criminalidade Informático-Digital, 1-ª Ed. Rei dos Livros, 2011, pág. 522.

[61] Relatório explicativo da Convenção do Cibercrime, ponto 159, disponível em https://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Documents/Convention%20and%20protocol/ETS_185_Portugese-ExpRep.pdf.

O órgão de polícia criminal por iniciativa própria, pode ordenar a preservação de dados, incluindo dados de tráfego, quando haja urgência ou perigo na demora.

Os visados com esta medida cautelar são qualquer entidade, designadamente fornecedor de serviço[62], que tenha a disponibilidade ou o controlo de dados informáticos específicos armazenados num sistema informático.

A ordem de preservação discrimina, sob pena de nulidade, a natureza dos dados, a sua origem e destino, bem como o período de preservação.

Sendo notificado desta obrigação, o fornecedor deverá preservar os dados, garantindo a confidencialidade da aplicação da medida (artigo 12.º, n.º 4, da LC).

O órgão de polícia criminal não deverá ter acesso aos dados, limitando-se, apenas e exclusivamente, a ordenar a quem detenha a disponibilidade destes dados que os preserve.

Esta ordem terá que ser posteriormente apreciada com vista a validação pela autoridade judiciária competente.

Os dados serão preservados pelo período máximo de três meses, prorrogáveis por períodos não superiores a três meses, desde que se verifiquem os requisitos de admissibilidade, até ao limite máximo de um ano, por ordem de autoridade judiciária (artigo 12.º, n.ºs 3, alínea c) e 5, da LC).

O órgão de polícia criminal que ordenar a preservação de dados terá que dar notícia imediata do facto à autoridade judiciária e transmitir-lhe relatório, nos moldes do disposto no artigo 253.º do Código de Processo Penal.

Revelação expedita de dados de tráfego – artigo 13.º da LC

Esta medida processual surge no decurso de uma ordem de preservação de dados emitida pelo OPC, sendo acessória desta uma vez que se destina a garantir a sua eficácia. Consiste na obrigação de o fornecedor de serviço indicar ao órgão de polícia criminal quais os outros fornecedores através dos quais determinada comunicação, cuja preservação tenha sido ordenada, tenha sido efetuada, permitindo que seja dada ordem de preservação de dados a esses outros fornecedores. Não deve ser confundida com revelação de dados de tráfego.
Esta informação é essencial na reconstrução do percurso informático de determinada comunicação com interesse para um futuro processo penal, e que visa determinar a sua origem ou o seu destino. Está dependente da informação fornecida por cada um dos fornecedores de serviço por onde a comunicação passou, sendo a obtenção célere e em tempo útil de tal informação essencial para o sucesso da investigação.

[62] Noção dada pelo artigo 2.º, alínea d), da Lei do Cibercrime: "*qualquer entidade, pública ou privada, que faculte aos utilizadores dos seus serviços a possibilidade de comunicar por meio de um sistema informático, bem como qualquer outra entidade que trate ou armazene dados informáticos em nome e por conta daquela entidade fornecedora de serviço ou dos respectivos utilizadores*.".

Para melhor perceber a razão de ser desta medida temos que atender ao próprio funcionamento da rede, o IP define o modo como os dados informáticos são enviados através da rede, atribuindo um endereço numérico a cada sistema informático ligado à Internet (o endereço de IP) e fragmentando se necessário os dados que irão ser transmitidos em pacotes de dados, onde está incluída a informação relativa aos dados de comunicação, a origem e o destino da comunicação, sendo que cada pacote de dados poderá seguir um caminho diferente.

Sendo usual que seja mais do que um fornecedor de serviço a intervir na transmissão de uma comunicação, acabando por cada um deles deter dados de tráfego relacionada com a transmissão da comunicação especificada. Esta informação revelada é essencial na reconstrução do percurso informático de determinada comunicação especificada, transmitida por mais do que um fornecedor de serviço. No fundo cada um dos fornecedores de serviço detém uma parte de um puzzle, que após examinada, poderá levar à deteção da origem ou o destino de determinada comunicação.

Apreensão *cautelar* de dados informáticos[63] – artigo 16.º, n.º 2, da LC

O órgão de polícia criminal pode efetuar apreensões, por iniciativa própria, quando haja urgência ou perigo de não se assegurar ou perder a prova, legitimamente ordenada, se conclua que determinados dados ou documentos informáticos servem ou serviram à prática de ilícitos criminais - Artigo 16.º, n.º 2, da LC.

Estas apreensões estão sujeitas a comunicação e validação pela autoridade judiciária, no prazo de 72 horas (16.º, n.º 4, da LC), sob pena de irregularidade[64].

De relevar que quando se tratem de conteúdos suscetíveis de revelar dados pessoais ou íntimos, que possam pôr em causa a privacidade do respetivo titular ou de terceiro, deverão ser apresentados ao juiz, sob pena de nulidade, que ponderará a sua junção aos autos tendo em conta os interesses do caso concreto (artigo 16.º, n.º 3, da LC).

A lei não ignora que os computadores pessoais são o local onde são guardados documentos escritos, fotografias, filmes ou gravações sonoras que são suscetíveis de revelar segredos e que são manifestações da vida íntima ou privada do seu dono. Trata-se de um regime que visa salvaguardar a intimidade e a privacidade do titular dos dados ou documentos informáticos, ou de terceiro, valores constitucionalmente consagrados no artigo 35.º da CRP. Acrescentamos, que estes elementos deverão ser levados ao juiz em envelope fechado, sendo

[63] Quanto a esta matéria de especial relevância a nota prática n.º 12/2017, de 2 de novembro, do Gabinete Cibercrime da PGR.
[64] O artigo 178.º *ex vi* 28.º da LC não estabelece qualquer cominação para a falta de validação (ao contrário, por exemplo, do artigo 179.º, relativo à apreensão de correspondência, que comina com nulidade as circunstâncias aí previstas), nem essa falta consta do elenco dos artigos 119.º e 120.º do CPP. Por tal motivo, a falta de validação da apreensão terá, nos termos do artigo 118.º, n.º 2, do CPP, de ser considerada mera irregularidade, tendo que ser arguida no próprio ato ou nos três dias subsequentes à primeira notificação ou intervenção processual que se lhe seguir (cfr. artigo 123.º, n.º 1 do CPP).

este o primeiro a tomar conhecimento do seu conteúdo, evitando-se assim a exposição do titular ou de terceiros perante outros agentes da justiça.

O artigo 16.º, n.º 7, da LC consagra a necessidade de serem satisfeitos os princípios da proporcionalidade e da adequação da apreensão tendo em vista os interesses do caso concreto. Define ainda as diferentes formas de apreensão de dados informáticos, podendo: ser apreendido o "*suporte onde está instalado o sistema ou (…) estão armazenados os dados informáticos, bem como os dispositivos necessários à respetiva leitura*" (alínea a)); realizar-se uma "*cópia dos dados, em suporte autónomo*", (alínea b)); preservar-se a integridade dos dados, "*por meios tecnológicos (…) sem realização de cópia nem remoção dos mesmos*" (alínea c)); ou eliminar-se de forma não reversível ou bloquear-se o acesso aos dados (alínea d)).

O legislador consagrou, ainda, a imposição de os dados apreendidos serem certificados através de uma assinatura digital, que se trata uma medida de preservação e garantia da integridade dos dados apreendidos relativamente a alterações posteriores à apreensão – artigo 16.º, n.º 8, da LC. Este artigo impõe ainda que se a apreensão for realizada através de cópia dos dados em suporte autónomo seja feita em duplicado.

DIAS RAMOS[65] propõe a alteração da palavra "*cópia*" por expressões como "*clonagem*" ou "*cópia de imagem*", por existirem equipamentos e ferramentas informáticas forenses para o efeito, que através da criação de resumo digital (código *hash*) permite certificar que a prova não sofreu alterações, não permitindo que se ponha em causa a valoração da prova em sede de julgamento.

Preservação expedita de dados informáticos em cooperação internacional[66] – artigo 22.º, n.º 4, da LC

A eficácia da recolha da prova digital está diretamente relacionada com a rapidez da intervenção, e tais objetivos apenas poderão ser atingidos com recurso ao auxílio mútuo em matéria de medidas cautelares e à cooperação policial, que permitem fazer face aos desafios colocados pela criminalidade desenvolvida na era informática.

Esta medida visa a preservação de dados informáticos armazenados, efetuada nos moldes dos artigos 12.º, n.º 2, da lei do cibercrime, em sistema informático localizado em Portugal. Impedindo que os dados sejam alterados, removidos ou eliminados durante o período de tempo necessário à preparação, transmissão, e execução de um pedido de assistência mútua para fins de obtenção dos dados.

Trata-se de uma medida cautelar, que a Polícia Judiciária pode ordenar, quando haja urgência ou perigo na demora, perante solicitação de autoridade judiciária estrangeira, com vista à futura apresentação de um pedido de auxílio judiciário para fins de pesquisa, apreensão e

[65] Ramos, Armando Dias, A prova digital em processo penal: o correio electrónico, 1.ª edição, Lisboa, Chiado Editora, Novembro 2014, p. 101, nota de rodapé 145.
[66] Quanto a esta matéria de especial relevância as notas práticas n.º 3/2014, de 12 de junho, e 4/2014, de 22 de dezembro, do Gabinete Cibercrime da PGR.

divulgação de dados informáticos. Esta solicitação de autoridade judiciária estrangeira é apresentada via "*ponto de contacto 24.7*", que providencia por imediata assistência.

A Convenção do Cibercrime, no seu artigo 35.º, prevê o estabelecimento de um serviço de contacto, denominado "*ponto de contacto 24.7*", transposto para ordem jurídica pelo artigo 21.º, n.º 1, da lei do cibercrime, baseado na experiência adquirida por uma rede já implementada e criada por iniciativa dos países mais industrializados do mundo.

De muito importante relevância prática, trata-se de um ponto de contacto operacional permanente a funcionar durante 24 horas por dia, 7 dias por semana. Ao contrário de outras ordens jurídicas, como a Holandesa que pertence ao Ministério Público, o ponto de contacto 24:7 está sob alçada da Polícia Judiciária, na Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica (UNC3T) – cfr. artigo 29.º, da Lei do Cibercrime e artigo 9.º-A, n.º 2, do DL n.º 42/2009, de 12 de Fevereiro - tendo como objetivo a rápida obtenção de elementos de prova aquando da criminalidade transnacional. Uma das características da prova informática é a sua volatilidade, pelo que recorrendo aos instrumentos tradicionais, a emissão e cumprimento de uma carta rogatória, a preservação e posterior recolha de prova poderá demorar uma eternidade ou mesmo não ser possível. Desta forma o contacto 24.7 pretende dar resposta mais eficiente e rápida de modo a ultrapassar os formalismos internacionais. O ponto de contacto pode ser contactado por via do endereço contacto24.7@pj.pt.

A Polícia Judiciária sempre que aplique tais medidas cautelares dará notícia imediata do facto ao Ministério Público e remete-lhe o relatório previsto no artigo 253.º do Código de Processo Penal (artigo 21.º, n.º 4, da Lei do Cibercrime).

Relatório – 253.º do Código de Processo Penal

Os órgãos de polícia criminal devem elaborar um relatório, sempre que levarem a cabo a aplicação das medidas cautelares e de polícia. Este relatório deve conter, conforme o disposto no n.º 1 do artigo 253.º do CPP:

– As investigações levadas a cabo: consiste num resumo das diligências efetuadas;
– Os resultados obtidos com as mesmas, nomeadamente resultado da inspeção judiciária, se há detidos, suspeitos identificados, quais os indícios recolhidos;
– A descrição dos factos apurados;
– As provas recolhidas, quanto ao(s) agente(s) do crime, à(s) vítima(s), à(s) testemunha(s), ao(s) objeto(s) da prática do(s) crime(s).

Em síntese, trata-se de um documento policial que materializa a descrição e análise das diligências efetuadas (meios de prova e de obtenção de prova), correlação do resultado das mesmas e a síntese quanto aos factos apurados.

Este relatório, em regra, deverá ser remetido à autoridade judiciária competente, Ministério Público se a atividade cautelar teve lugar em fase pré-processual ou durante o inquérito, ou ao Juiz de instrução se atividade cautelar teve lugar em fase de instrução, com vista à apreciação, controlo e validação da atividade do órgão de polícia criminal.

4. Prática e Gestão Processual

O Ministério Público e os Órgãos de Polícia Criminal - breve contextualização

Compete ao Ministério Público "*exercer a acção penal orientada pelo princípio da legalidade*" – artigo 219.º, n.º 1, da Constituição da República Portuguesa e artigo 3.º, n.º 1, alínea c), do Estatuto do Ministério Público (EMP).

No âmbito do exercício da ação penal, cabe ao Ministério Público a direção do inquérito (artigo 3.º, n.º 1, alínea h), do EMP) que consiste na orientação da investigação criminal através da emissão de diretivas, acompanhamento e fiscalização dos vários atos, delegação ou solicitação de diligências, presidir ou assistir a certos atos e avocar o inquérito.

Colocando o relacionamento entre o Ministério Público e os órgãos de polícia criminal "*no preenchimento dos conceitos de «assistência», «directa orientação» e «dependência funcional» (…) numa lógica de coadjuvação*[67] *dos órgãos de polícia criminal face ao Ministério Público, criando-se uma «relação de supremacia sem hierarquia» (…)*[68]".

O modelo de relacionamento entre os órgãos de polícia criminal e o Ministério Público baseia-se num sistema de dependência funcional, e de independência ao nível orgânico, preservando assim a autonomia técnica e tática das polícias, conforme o disposto no artigo 2.º, n.º 5, da Lei de Organização e Investigação Criminal. É, também, no n.º 6 do referido artigo que vem consagrada a distinção entre autonomia técnica – que "*assenta na utilização de um conjunto de conhecimentos e métodos de agir adequados*" e autonomia táctica – que "*consiste na escolha do tempo, lugar e modo adequados à prática dos actos correspondentes ao exercício das atribuições legais dos órgãos de polícia criminal*.".

O conceito de dependência funcional "*visa fundamentalmente pôr em relevo o esquema organizatório que preside ao relacionamento entre autoridades judiciárias e órgãos de polícia criminal*"[69], determinando que haja um respeito mútuo entre os diferentes operadores judiciários: os órgãos de polícia criminal coadjuvam as autoridades judiciárias e cumprem as diligências por elas determinadas (pois são elas que dirigem as diferentes fases processuais); e as autoridades judiciárias respeitam a autonomia técnica e táctita dos órgãos de polícia criminal no domínio da investigação criminal quando tal se revele necessário para o cumprimento das suas atribuições.
O princípio da coadjuvação não significa, porém, que haja uma transferência das competências do Ministério Público (ou de outra autoridade judiciária, nas fases que superintendem) para os órgãos de polícia criminal. Estes já possuem essas competências, que lhes são conferidas precisamente pela sua natureza de órgãos auxiliares da Administração da Justiça, quando atuam na veste de polícia judiciária, mas só as exercem a partir do momento em que têm conhecimento da prática de um ilícito criminal e/ou após o respetivo despacho de delegação

[67] Vide artigo 55.º, do Código de Processo Penal.
[68] Gaspar, Jorge, Titularidade da Investigação Criminal e Posição Jurídica do Arguido, Revista do Ministério Público, ano 22, jul/set, 2001, n.º 87, p. 35.
[69] Cfr. Cunha, José Damião da - O Ministério Público e os Órgãos de Polícia Criminal: No Novo Código de Processo Penal. Porto, Universidade Católica Portuguesa, 1993, p. 114.

de competências para procederem à investigação criminal do facto criminal em concreto. Partilhamos da visão de MANUEL GUEDES VALENTE que afirma que "*o princípio da coadjuvação não significa derrogação de competência, mas o respeito integral pelo princípio da inderrogabilidade de competências*"[70].

A Polícia não depende hierarquicamente do Ministério Público[71], não deixa, no entanto, de necessitar de aprovação deste para realizar atos no decorrer do Inquérito. Mesmo quando actua *a priori* da intervenção do Ministério Público, no âmbito das medidas cautelares e de polícia, quando a urgência ou o perigo *in mora* assim o justifiquem, a Polícia tem de submeter toda a sua actuação à apreciação do Ministério Público (ou do JIC, quando estejam em causa direitos, liberdades e garantias fundamentais). Só após verificação cuidada é que a autoridade judiciária competente se pronuncia pela validação das medidas adotadas pelos órgãos de polícia criminal, passando estas a integrar o Processo.

A dependência funcional dita que os órgãos de polícia criminal, no decorrer do processo, atuem sob orientação das autoridades judiciárias competentes em cada fase processual. No entanto, o que se verifica no sistema nacional é que o Ministério Público emite um despacho genérico de delegação de competências a um dado órgão de polícia criminal, conferindo-lhe autonomia técnica e táctica para desenvolver a investigação criminal de acordo com os princípios e o conhecimento técnico e científico de que o mesmo dispõe nessa matéria. Uma das críticas que por vezes se coloca é precisamente o facto de o Ministério Público delegar a investigação criminal no órgão de polícia criminal limitando-se a verificar *a posteriori* o que foi feito e se está conforme os princípios e as regras do Processo Penal, deixando assim de ser o "*diretor do inquérito*" para ser um "*receptor do inquérito*". Para solucionar a questão, concordamos que se procure uma maior aproximação entre Ministério Público e polícias, para que haja um diálogo constante entre ambos, de forma a evitar que haja uma "*policialização do inquérito*".

O poder de orientação do Ministério Público "*não pode ser entendido estaticamente, mas, pelo contrário, como um processo dinâmico que se baseia num processo de informação, tanto quanto possível constante*"[72] e que lhe permita decidir convenientemente sobre o rumo da investigação.

O âmbito de atuação da Polícia, no campo das medidas cautelares e de polícia, ocorre maioritariamente numa fase pré-processual, logo que obtenham notícia do crime, mas ainda antes da abertura do inquérito. Mas essa prerrogativa de poder aplicar estas medidas por autonomia própria subsiste durante a primeira fase processual, onde os órgãos de polícia criminal passam a ter associada uma competência delegada.

[70] Valente, Manuel Guedes, Do Ministério Público e da Polícia - Prevenção Criminal e Acção Penal como Execução de uma Política Criminal do Ser Humano, Lisboa, UCE, 2013, p. 105.
[71] A "*hierarquia das policias deve ser salvaguardada como meio de assegurar as suas coesão e disciplinas internas, factores da própria eficácia das missões*"- Rodrigues, Cunha, A Posição Institucional do Ministério Público e das Polícias de Investigação Criminal, *in* BMJ, 337, junho, 1984, p. 39.
[72] Cunha, José Damião da - O Ministério Público e os órgãos de polícia criminal: No novo código de processo penal. Porto: Universidade Católica Portuguesa, 1993, p. 133.

O Código de Processo Penal atribui à magistratura do Ministério Público a competência constitucional para a direção do inquérito, que envolve igualmente competências de investigação criminal e, sobretudo, um papel estruturante da intervenção policial.

Se se pretende evitar a designada "*policialização*" do processo penal, o Ministério Público não pode ser um mero gestor de papéis, pelo contrário, deve ser dotado de condições que lhe permitam intervir/acompanhar o trabalho das forças policiais, só assim podendo ser responsabilizado pelos resultados obtidos.

Os órgãos de polícia criminal ou as autoridades de polícia criminal não podem substituir o papel das autoridades judiciárias, sob pena se colocar em causa o sentido do princípio da investigação sob garantia judicial.

Este acompanhamento próximo da atuação policial, que se deve verificar mesmo no exercício da atividade cautelar, pelo Ministério Público consiste na aplicação da prerrogativa legal de fiscalizar a todo o tempo o modo de atuação do órgão de polícia criminal no âmbito da investigação criminal, prevista pelo disposto no artigo 263.º do Código de Processo Penal e artigo 2.º da LOIC. No exercício da atividade cautelar a intervenção dos órgãos de polícia criminal não escapa à responsabilidade funcional do Ministério Público, considerando que são atos que integram a tramitação processual concreta após avaliação do titular de ação penal.

No fundo a atuação do Ministério Público, consiste em dar uma base jurídica às primeiras intervenções policiais que é uma das atribuições basilares do Ministério Público[73].

Formação em investigação criminal

Para a constante melhoria da eficácia do Ministério Público, é fundamental a otimização ao nível da divulgação da informação sobre a intervenção na investigação criminal, onde a consciencialização da especificidade das tarefas de cada um dos intervenientes é fundamental.

A investigação criminal, como ciência auxiliar do direito penal, deve ser alvo de estudo e divulgação adequadas junto Ministério Público. Uma vez que não se trata de uma atividade exclusiva dos órgãos de polícia criminal, sendo orientada e partilhada pelo Ministério Público. A ministração de conhecimentos especializados aos magistrados do Ministério Público no domínio da investigação criminal demonstra-se essencial para facilitar uma definição clara das "*fronteiras*" da intervenção dos vários órgãos e autoridades, com reflexos positivos na sua eficácia de atuação.

Até porque a investigação criminal/direção do inquérito/exercício da ação penal definem o Ministério Público como magistratura.[74] E por acima de tudo para se fazer fazer é necessário saber fazer.

[73] Mesquita, Paulo Dá, Direcção do Inquérito Penal e Garantia Judiciária, Coimbra, Coimbra Editora, 2003, p. 133.
[74] Moura, Souto, O inquérito e as relações M.P./PJ, 1.º Congresso de Investigação Criminal - Modelos de Polícia e Investigação Criminal, edição: ASFIC / PJ, junho de 2006, p. 146.

Fomentar uma "cultura de proximidade" entre os agentes do sistema de justiça

Não podemos descurar a importância do estabelecimento de relações interpessoais e interprofissionais fortes. Só desta forma se poderá promover o relacionamento são entre magistrados e polícias, imprescindível na tarefa (que é de todos) de servir o interesse público.

Comunicação imediata da atividade realizada por iniciativa própria pelo OPC

A atuação por iniciativa própria dos órgãos de polícia criminal integra-se dentro da competência de coadjuvação do Ministério Público. Neste sentido, como escreve DAMIÃO DA CUNHA[75]: "(…)*as medidas cautelares em sentido estrito (…) não correspondem, em termos jurídico-organizatórios, a qualquer figura nova, portanto não fundamentam qualquer competência específica, em termos processuais penais. Antes são apenas a concretização da competência de coadjuvação e, só por isso, não justificariam qualquer tratamento legislativo autónomo*.".

Apesar de estarmos dentro de atos de iniciativa própria dos órgãos de polícia criminal, estamos ainda perante atos que se encontram na dependência funcional das autoridades judiciárias isto porque, embora não tenha existido intervenção destas, os órgãos de polícia criminal atuam como órgãos auxiliares da Administração da Justiça. Tanto assim é que estes atos só passam a ser considerados atos processuais e por conseguinte a integrar o processo se o Ministério Público assim o decidir.

A função de controlo do Ministério Público, enquanto competência funcional, deve recair, em primeira linha, sobre a atividade policial pré-processual, esta função consiste na análise da legalidade da atuação e na integração no processo das diligências respeitadoras das normas legais. E por outro lado, deve permitir a concretização de uma atividade processual articulada com o órgão de polícia criminal, tão importante para eficácia da atividade investigatória.

Segundo PAULO DÁ MESQUITA[76] o único limite à autonomia do órgão de polícia criminal nos atos por iniciativa própria consiste na obrigação de comunicação imediata da atividade realizada, através do cumprimento da obrigatoriedade de elaboração e remessa de relatório pelo órgão de polícia criminal.

Mesmo no caso da existência de medidas que apenas podem ser autorizadas ou ordenadas pelo Juiz, na fase de inquérito, o relatório sobre as medidas cautelares e de polícia deverá ser enviado ao Ministério Público, o qual apenas deve submeter a validação judicial se entender que no caso concreto a atuação respeitou as regras legais. Caso entenda que a atuação policial

[75] Cfr. Cunha, José Damião da - O Ministério Público e os Órgãos de Polícia Criminal: No Novo Código de Processo penal, Porto, Universidade Católica Portuguesa,1993, p. 139.
[76] Dá, Paulo Mesquita, Repressão Criminal e Iniciativa Própria dos Órgãos de Polícia Criminal, Revista do Ministério Público n.º 98, ano 25, abril/junho, 2005, p. 12.

não pode ser validada não a deve submeter a apreciação judicial, assinalando eventuais infrações tendo em vista a sua repressão penal ou disciplinar[77].

Esta atuação deve prevalecer pelo respeito pela competência funcional exclusiva do Ministério Público, que enquanto titular da ação penal, assume, no inquérito, a primeira palavra, através da promoção processual quanto à integração ou não integração dos atos cautelares desenvolvidos por iniciativa própria policial.

Emissão de regras de conduta genéricas para o futuro

No âmbito de intervenção por iniciativa própria dos órgãos de polícia criminal pode verificar-se o seu exercício deficiente, e até irrecuperável. Quando desta intervenção emirjam atos com estas caraterísticas deve o Ministério Público emitir regras de conduta futuras que eliminem tais deficiências irrecuperáveis. Tal poder é exercido com fundamento no poder de fiscalização da atividade processual dos órgãos de polícia criminal, previsto no disposto pela alínea n) n.º 1 do artigo 3.º do EMP, não se confundindo com o poder de orientação exercido na tramitação de um concreto processo penal[78].

4.2 Da atuação concreta do magistrado do Ministério Público no âmbito das medidas cautelares e de polícia

Como já referimos, ao longo trabalho, o Ministério Público no âmbito das medidas cautelares tem funções a jusante da intervenção dos órgãos de polícia criminal. A sua função passa pelo controlo da atividade policial, que consiste na apreciação, validação ou promoção da validação dos atos cautelares tendo em vista a integração de tais atos no processo penal, levando à sua convolação em atos processuais.

Nesta parte pretende-se, de uma forma sintética e objetiva, abordar as medidas cautelares e de polícia e indicar qual a atuação que o magistrado do Ministério Público deve considerar.

Comunicação da notícia do crime

Os órgãos de polícia criminal estão obrigados a comunicar no mais curto prazo possível, e face aos meios de comunicação atuais pode ser feito quase em tempo real, os crimes de que tenham conhecimento direto, indireto ou por denúncia ao Ministério Público (artigo 248.º do Código de Processo Penal). O início imediato das diligências policiais não pode afastar esta obrigação, até porque nesta fase pré-processual apenas deve consistir nos atos que se afigurem urgentes e necessários até intervenção do Ministério Público[79].

[77] Neste sentido Paulo Dá Mesquita, Direcção do Inquérito e Garantia Judiciária, Coimbra, 2003, p. 135. No sentido de que quando o ato de natureza cautelar caiba na reserva judicial, o relatório policial para apreciação e validação deve ser entregue ao Juiz de Instrução. Germano Marques da Silva, Do Processo Penal Preliminar, p. 65.
[78] Cfr. Cunha, José Damião da, O Ministério Público e os Órgãos de Polícia Criminal: No Novo Código de Processo Penal, Porto, Universidade Católica Portuguesa,1993, p. 276.
[79] Valente, Manuel Monteiro Guedes - Teoria Geral do Direito Policial, 5.ª Edição, Coimbra, Almedina, 2017, pp. 488 e 493.

A necessidade de transmissão do auto de notícia e denúncia ao Ministério Público no mais curto espaço de tempo têm a finalidade de que este assuma as suas responsabilidades funcionais.

A comunicação de notícia de crime (auto de notícia/denúncia) é alvo de registo e distribuição (vide artigos 247.º, n.º 5 e 262.º, n.º 2, do Código de Processo Penal).

O seu registo e distribuição são efetuados de acordo com o previsto na Ordem de Serviço da PGR n.º 4/2015[80], que estabelece regras nacionais uniformes de registo da atividade do Ministério Público, bem como implementa uma tabela única de distribuição de inquéritos criminais.

Uma nota para as denúncias anónimas que apenas são registadas como inquérito se, analisado o expediente, se concluir dever haver lugar à sua efetiva abertura, para os efeitos consignados no artigo 262.º do Código de Processo Penal, o que apenas deverá ocorrer quando se mostrem verificadas as condições constantes do nº 6 do artigo 246.º do Código de Processo Penal, ou seja, se retirem da denúncia indícios da prática de crime ou constituir crime.

Providências Cautelares quanto aos meios de prova

No âmbito da inspeção judiciária os órgãos de polícia criminal procedem ao exame de vestígios do crime (artigo 249.º, n.º 2, alínea a), do CPP) e à sua recolha para posterior análise pericial. Caberá ao magistrado do Ministério Público, recebido o relatório do órgão de polícia criminal, emitir despacho a ordenar a efetivação de perícia aos vestígios, nos termos do artigo 154.º do Código de Processo Penal (artigo 270.º, alínea a) do mesmo código), caso essa faculdade não esteja delega em autoridade de polícia criminal, nos termos do disposto do n.º 3 do mesmo artigo. E caso não se trate de perícia cuja ordem ou autorização seja da competência do juiz de instrução (vide artigo 154.º, n.º 3, *ex vi* do artigo 269.º, n.º 1, alínea a) do CPP), sendo que neste caso o procedimento a ser adotado passará pela promoção de apreciação e decisão tendo vista a ordem ou autorização de efetivação da perícia.

A recolha de informação (artigo 249.º, n.º 2, alínea b), do Código de Processo Penal) pode originar a identificação do suspeito, e havendo fundada suspeita da prática do crime por este, a sua constituição na qualidade de arguido. Nesta sede caberá ao magistrado do Ministério Público a apreciação e validação deste ato, conforme o previsto no artigo 58.º, n.º 2, do Código de Processo Penal. A comunicação do órgão de polícia criminal deverá fornecer os elementos necessários para o magistrado fazer um juízo de apreciação sobre os pressupostos da constituição de arguido, designadamente do n.º 1 do artigo 58.º do Código de Processo Penal.

No âmbito destas providências cautelares o órgão de polícia criminal efetua apreensões no decurso de revistas ou buscas ou em caso de urgência ou perigo na demora (artigo 249.º, n.º 2, alínea c), do CPP), após comunicação de tais apreensões, através do envio pelo órgão de polícia criminal de relatório e do auto de apreensão, o magistrado do Ministério Público

[80] Disponível em http://www.ministeriopublico.pt/sites/default/files/documentos/pdf/os_4_2015.pdf.

deverá apreciar a existência dos pressupostos que levaram a tais apreensões bem como da sua relevância para o futuro inquérito, tendo em vista a sua validação (vide artigo 178, n.º 5, do Código de Processo Penal).

Identificação do suspeito e pedido de informações

Em particular de acordo com o n.º 8 do artigo 250.º, no âmbito da sua atividade cautelar e por iniciativa própria pode pedir ao suspeito (sem prejuízo do disposto no artigo 59º do CPP, quanto à constituição de arguido) ou qualquer pessoa informações úteis, relevantes e relacionadas com um crime, bem como relacionadas com a descoberta e conservação de meios de prova, que poderiam dissipar-se antes da intervenção da autoridade judiciária.

Daqui pode resultar a sua constituição na qualidade de arguido, pelo que ao magistrado do Ministério Público cabe a apreciação e validação deste ato, conforme o previsto no artigo 58.º, n.º 2, do Código de Processo Penal.

Revistas e Buscas cautelares

Estas revistas e buscas não domiciliárias, conforme o previsto do artigo 174.º, n.º 6 *ex vi* do artigo 251.º, n.º 2, do Código de Processo Penal, são comunicadas ao juiz de instrução e por este apreciadas em ordem à sua validação. Este ato cautelar urgente do órgão de polícia criminal está sujeito a homologação do juiz de instrução. Nesta sede o magistrado do Ministério Público deverá tomar a iniciativa de promover tal ato jurisdicional.
Pelo que o relatório sobre as medidas cautelares e de polícia, com os respetivos autos de revista e/ou busca deverá ser enviado ao Ministério Público, o qual apenas deve promover a validação judicial se entender que no caso concreto a atuação respeitou as regras legais, sublinhando-se, deste modo, que ao Ministério Público, em fase de inquérito ou anterior, cabe a primeira intervenção pós atuação policial.

Apreensão de correspondência

O órgão de polícia criminal pode, por sua iniciativa, proceder à suspensão da remessa de qualquer correspondência nas estações de correios e de telecomunicações, com base em fundadas razões para crer que estes possam conter informações úteis para a investigação de um crime ou conduzir à sua descoberta e que cuja utilidade se pudesse perder, em caso de demora – artigo 252.º, n.º 3, do CPP.

Na fase de inquérito ou quando a atuação cautelar ocorra antes desta fase, o órgão de polícia criminal deverá comunicar ao Ministério Público a suspensão da correspondência, integrando tal comunicação relatório e cópia do auto que ordenou a suspensão, para que o Ministério Público possa efetuar despacho fundamentado a promover a convalidação da ordem de suspensão ao juiz de instrução de criminal. De notar a celeridade que se exige na efetivação desta promoção atendendo ao prazo de 48 horas em que suspensão cautelar de correspondência pode ser mantida.

Localização Celular

Na fase de inquérito ou quando a atuação cautelar ocorra antes desta fase, a comunicação da efetivação desta medida cautelar deverá ser efetuada ao Ministério Público, em concreto ao procurador titular do inquérito caso haja processo em curso ou ao procurador de turno da sede da entidade competente para a investigação criminal caso não haja processo em curso (vide artigos 252.º-A, n.º 2 e 3, do CPP). Esta comunicação terá que ser instruída com relatório, solicitação efetuada pela autoridade de polícia criminal ao operador de telecomunicações, bem como com a resposta dada por este operador, cabendo ao Ministério Público promover, no prazo máximo de 48 horas desde a obtenção dos dados, o controle judicial da medida, caso tenham sido cumpridos os pressupostos legais.

Preservação expedita de dados

O órgão de polícia criminal que ordenar a preservação de dados terá que dar notícia imediata do facto à autoridade judiciária e transmitir-lhe relatório, nos moldes do disposto no artigo 253.º do Código de Processo Penal.

A atuação do magistrado do Ministério Público passa pela apreciação da verificação dos pressupostos, já analisados em sede própria (vide artigo 12.º, n.º 1, 2 e 3, da LC), que legitimem a atuação por iniciativa própria do órgão de polícia criminal, tendo em vista a sua validação.

Apreensão cautelar de dados informáticos

O órgão de polícia criminal pode efetuar apreensões, por iniciativa própria, quando haja urgência ou perigo de não se assegurar ou perder a prova, desde que no decurso de pesquisa informática, legitimamente ordenada, se conclua que determinados dados ou documentos informáticos servem ou serviram à prática de ilícitos criminais.
Como já verificamos, estas apreensões estão sujeitas a comunicação e validação pela autoridade judiciária, no prazo de 72 horas (16.º, n.º 4, da LC).

Nesta sede, em fase de inquérito ou anterior, a adoção do procedimento pelo magistrado do Ministério Público depende do tipo de dados apreendidos.

Se verificarmos que os dados são pessoais ou íntimos, que possam pôr em causa a privacidade do respetivo titular ou de terceiro, deverá promover-se a apresentação destes elementos ao juiz, que ponderará a sua junção aos autos tendo em conta os interesses do caso concreto (artigo 16.º, n.º 3, da LC).

Não se tratando de dados com estas características, o magistrado do Ministério Público fará a apreciação dos pressupostos de urgência ou perigo na demora da apreensão que legitimaram a atuação cautelar do órgão de polícia criminal, tendo em vista a validação da sua atuação e a junção dos dados aos autos.

Preservação expedita de dados informáticos em cooperação internacional.

O órgão de polícia criminal que ordenar a preservação de dados terá que dar notícia imediata do facto à autoridade judiciária e transmitir-lhe relatório, nos moldes do disposto no artigo 253.º do Código de Processo Penal.

A atuação do magistrado do Ministério Público passa pela apreciação da verificação dos pressupostos da medida cautelar decorrente de pedido de auxílio internacional, já analisados em sede própria (vide artigo 22.º, n.º 1, 2 e 4, da LC), que legitimem a atuação por iniciativa própria do órgão de polícia criminal, tendo em vista a sua validação.

IV. Referências bibliográficas

- ALBUQUERQUE, Paulo Pinto de, Comentário do Código de Processo Penal à luz da Constituição da República Portuguesa e da Convenção Europeia dos Direitos do Homem, 2.ª edição, Lisboa, Universidade Católica Editora, 2008.
- BRAZ, José, Investigação Criminal: a organização, o método e a prova. Os desafios da nova criminalidade, 2ª edição, Coimbra, Almedina, 2010.
- CORREIA, Eduardo, A Instrução Preparatória em Processo Penal; alguns problemas, BMJ nº 42, 1954.
- CUNHA, José Damião da, O Ministério Público e os Órgãos de Polícia Criminal, No Novo Código de Processo Penal, Porto, Universidade Católica Portuguesa, 1993.
- GASPAR, António Henriques, CABRAL, José António Henriques dos Santos, E outros., Código de Processo Penal comentado, 2.ª Edição, Coimbra, Almedina, 2015.
- GASPAR, Jorge, Titularidade da Investigação Criminal e Posição Jurídica do Arguido, Revista do Ministério Público, ano 22, jul/set, 2001, n.º 87, p. 7-62.
- GASPAR, Jorge, Titularidade da Investigação Criminal e Posição Jurídica do Arguido, Revista do Ministério Público, ano 22, Out/Dez, 2001, n.º 88, p. 101-136.
- LOBO, Fernando Gama, Código de Processo Penal anotado, Coimbra, Almedina, 2015.
- MESQUITA, Paulo Dá, Direcção do Inquérito Penal e Garantia Judiciária, Coimbra, Coimbra Editora, 2003.
- MESQUITA, Paulo Dá, Repressão Criminal e Iniciativa Própria dos Órgãos de Polícia Criminal, Revista do Ministério Público n.º 98, ano 25, abril/junho, 2005, p. 7-36.

- MOURA, Souto, O Inquérito e as Relações M.P./PJ, Actas do 1.º Congresso de Investigação Criminal - Modelos de Polícia e Investigação Criminal edição: ASFIC / PJ, junho de 2006.

- PINHEIRO, Alexandre Sousa e OLIVEIRA, Jorge Menezes de, O Bilhete de Identidade e os Controlos da Identidade, Revista do Ministério Público, Ano 15, n.º60, Outubro/Dezembro de 1994, p. 11-100.

- RODRIGUES, Anabela, A Fase Preparatória do Processo Penal – Tendências na Europa. O Caso Português, Revista Brasileira de Ciências Criminais, Ano 10, n.º 39, São Paulo: Editora Revista dos Tribunais (Julho/Setembro 2002), pp. 9-27.

- RODRIGUES, Benjamim Silva Rodrigues, Direito Penal. Parte Especial, I, Direito Penal Informático-Digital, Coimbra, Coimbra Editora, 2009.

- RODRIGUES, Benjamim Silva, Da Prova Penal – Tomo IV, Da Prova Electrónico-Digital e da Criminalidade Informático-Digital, 1-ª Ed. Rei dos Livros, 2011.

- RODRIGUES, Cunha, A Posição Institucional do Ministério Público e das Polícias de Investigação Criminal, in BMJ, 337, junho, 1984, p. 15-43.

- SOARES, Paulo, Meios de Obtenção de Prova no Âmbito das Medidas Cautelares e de Polícia, 2.ª edição, Coimbra, Almedina, 2017.

- SILVA, Germano Marques da, Do Processo Penal Preliminar, Lisboa, Univ. Católica Portuguesa. Faculdade de Direito, 1990.

- SILVA, Germano Marques da, Direito Processual Penal Português, Do Procedimento, Vol. 3, Lisboa, UCE, 2015.

- VALENTE, Manuel Guedes, Teoria Geral do Direito Policial, 7.ª edição, Coimbra, Almedina, 2017.

- VALENTE, Manuel Guedes, Do Ministério Público e da Polícia - Prevenção Criminal e Acção Penal como Execução de uma Política Criminal do Ser Humano, Lisboa, UCE, 2013.

- VENÂNCIO, Pedro, Lei do Cibercrime Anotada e Comentada, Coimbra, Coimbra Editora, 2011.

CENTRO
DE ESTUDOS
JUDICIÁRIOS

5.

Apreensão, exame ou perícia, e utilização processual de meios de prova existentes em material informático (documentos, correio eletrónico, memorandos pessoais, fotografias, registos, áudio, etc.) - enquadramento jurídico, prática e gestão processual

Rui Miguel dos Santos Real

CENTRO
DE ESTUDOS
JUDICIÁRIOS

5. APREENSÃO, EXAME OU PERÍCIA, E UTILIZAÇÃO PROCESSUAL DE MEIOS DE PROVA EXISTENTES EM MATERIAL INFORMÁTICO (DOCUMENTOS, CORREIO ELECTRÓNICO, MEMORANDOS PESSOAIS, FOTOGRAFIAS, REGISTOS, ÁUDIO, ETC.. ENQUADRAMENTO JURÍDICO, PRÁTICA E GESTÃO PROCESSUAL

Rui Miguel dos Santos Real

1. Prova digital – âmbito

O presente trabalho, desenvolvido no âmbito do 2.º Ciclo do 32.º Curso Normal de Formação para Magistrados nos Tribunais Judiciais – Ministério Público, versa sobre alguns aspectos respeitantes à obtenção de prova em dispositivos informáticos, com particular enfoque nos exames, perícias, pesquisas e apreensões.

O tema reveste-se de manifesta actualidade e pertinência, uma vez que a ubiquidade do mundo digital trouxe consigo a ubiquidade dos dados informáticos como elementos com interesse probatório no âmbito de procedimentos criminais, atinentes não apenas a crimes exercidos sobre sistemas informáticos, mas antes à integralidade do universo criminal.

Apesar desta ubiquidade, a temática relativa à obtenção e uso de dados informáticos para efeitos probatórios continua a ser pouco dominada pelos agentes do mundo judiciário, circunstância a que não é obviamente alheia a intrincada e complexa teia legislativa existente, mas para a qual contribui sobretudo uma ainda disseminada iliteracia tecnológica, agravada pela constante mutação do universo digital e pela difícil compreensibilidade da linguagem técnica utilizada.

O presente trabalho constitui um esforço modesto e superficial de análise de algumas problemáticas que frequentemente se apresentam ao aplicador do Direito nesta sede, partindo primordialmente da perspectiva e posicionamento de um Magistrado do Ministério

Público em sede de inquérito criminal, com pontuais alusões à posterior participação em audiência de julgamento.

O trabalho encontra-se dividido em quatro grandes capítulos (sendo o último conclusivo), no primeiro dos quais se introduzirão alguns aspectos básicos dos dados informáticos enquanto prova e dos antecedentes da Lei do Cibercrime, que continua a constituir o diploma central neste âmbito.

O segundo capítulo conterá uma análise do regime legal aplicável aos meios de obtenção de prova digital de uso mais frequente, abordando-se alguns dos problemas práticos que tais meios suscitam. Principiar-se-á pela análise das medidas cautelares previstas na LC, para posteriormente se abordar a tríade constituída pela detecção de prova digital (injunção para apresentação ou concessão de acesso a dados e pesquisa de dados informáticos), sua preservação à ordem de um processo (apreensões) e análise posterior da mesma (exames e perícias).

De fora, ficarão as intercepções de comunicações (art. 18.º da LC) e as acções encobertas (art. 19.º da LC), por se tratar de meios de obtenção de prova com menor expressão estatística e por suscitarem problemas que imporiam um trabalho de outra envergadura.

O terceiro capítulo conterá algumas apreciações em matéria de gestão processual, que derivarão directamente dos aspectos de regime que merecerão enfoque nos capítulos antecedentes. Será neste capítulo que se adiantarão algumas orientações genéricas para a condução do inquérito e preparação da audiência de julgamento e que se farão algumas considerações sobre realidades que reputamos deverem ser conhecidas pelo aplicador do Direito, como as medidas anti-forenses e *software* forense.

2. Prova digital e Lei do Cibercrime

2.1. Dados informáticos e prova digital

A análise das problemáticas colocadas pela obtenção de prova em ambiente digital convoca o uso frequente das expressões “dados informáticos” e “prova digital”, a primeira das quais contendo definição legal, contrariamente à segunda, ainda assim referida em profusa doutrina e jurisprudência.

Principiando pelo conceito de “prova digital”, sabe-se que o vocábulo “prova” é de natureza polissémica, podendo significar, consoante o contexto de utilização:

(i) Meio de prova, ou seja realidade susceptível de atestar ou indiciar a verificação histórica de um facto juridicamente relevante;
(ii) Actividade probatória, ou seja procedimento tendente à reconstrução histórica de um facto juridicamente relevante; e

(iii) Resultado probatório, ou seja, juízo de verosimilhança da verificação histórica de facto juridicamente relevante[1]. Para a presente exposição, releva apenas a noção de prova como meio de prova.

Relativamente à noção de digital, tratando-se também de palavra polissémica, interessa-nos particularmente o sentido de digital como algo "*que apresenta dados, resultados ou indicações sob forma numérica, por oposição a analógico*", ou como "*representação da informação de forma abstracta (intocável), a qual pode ser manipulada por meio de dispositivos digitais, ou a forma de representação por valores lógicos e exactos, de qualquer tipo de dado*"[2].

Ressaltam destas definições dois aspectos que cremos serem essenciais para a caracterização de dada realidade como digital: representação sob forma numérica e a susceptibilidade de manipulação através de dispositivos electrónicos. O digital tem assim uma linguagem própria (binária, ou seja uma sequência de zeros e uns), cuja descodificação e conversão em significado apreensível para o utilizador corrente dependem do uso de dispositivos com aptidão para esse efeito.

Ensaiando uma definição perfunctória de "prova digital", dir-se-á assim que se trata do conjunto das realidades com representação através de uma linguagem numérica (binária) e susceptíveis de manipulação, análise e conservação através de dispositivos electrónicos, que manifestam interesse para a reconstituição da verdade histórica, no âmbito da actividade judiciária.

A Lei do Cibercrime (Lei n.º 109/2009, de 15 de Setembro, doravante designada como LC), não acolheu qualquer definição de prova digital, centrando-se antes na definição de "dados informáticos", aí entendidos como "*qualquer representação de factos, informações ou conceitos sob uma forma susceptível de processamento num sistema informático, incluindo os programas aptos a fazerem um sistema informático executar uma função*". Verifica-se assim uma certa aproximação entre esta noção e aquela que demos e prova digital.

Mesmo perante noções tão amplas de prova digital e de dados informáticos, é possível excluir do seu âmbito várias realidades probatórias, designadamente aquelas que tenham existência corpórea ou sejam representáveis por outra linguagem que não a numérica. Dando dois exemplos significativos, ficam fora deste âmbito as comunicações telefónicas (às quais falta a linguagem binária, sendo antes comunicações de discurso oral por rede fixa ou através de satélite) e as impressões físicas de páginas de Internet ou mensagens de correio electrónico (que correspondem a simples prova documental)[3].

Ainda assim, a amplitude é suficientemente significativa para que possamos afirmar que praticamente todas as realidades susceptíveis de documentação física possam aqui estar

[1] Neste sentido, GERMANO MARQUES DA SILVA, *Curso de Processo Penal, Volume II*, Editorial Verbo, 2002, p. 96.

[2] Definições extraídas, respectivamente, do Dicionário Priberam da Língua Portuguesa e consultável em https://www.priberam.pt/dlpo/digital, e da *Wikipedia*, consultável em https://pt.wikipedia.org/wiki/Dados_digitais.

[3] Discordamos por isso da posição assumida pelo TRP, em Acórdão datado de 13 de Abril de 2016, proferido no proc. n.º 471/15.0T9AGD-A.P1 e disponível em www.dgsi.pt, onde se parece sustentar que a simples impressão física de uma página de Facebook deve também ser sujeita aos termos da Lei do Cibercrime.

abrangidas na sua manifestação digital (em elenco não exaustivo, podemos falar de mensagens de correio electrónico, páginas de Internet, programas informáticos, livros, vídeos, gravações áudio, arquivos, fotogramas, mapas, plantas arquitectónicas, documentação contabilística e financeira, etc.).

Ao nível dos dispositivos electrónicos susceptíveis de conter ou processar dados informáticos com interesse probatório há a considerar um longo espectro, que inclui computadores pessoais, discos externos, *pen drives*, telemóveis, *tablets*, cartões de memória, DVD's, CD's, disquetes, redes informáticas, câmaras de filmar, câmaras fotográficas, relógios digitais, dispositivos de geolocalização e até robôs ou microchips subcutâneos.

Perante tão ampla profusão de realidades digitais, fácil é perceber que a eventual utilidade probatória de dados informáticos em processos criminais é virtualmente ilimitada, não sendo assim de surpreender que o art. 11.º da LC preveja que os meios de obtenção de prova regulados na mesma (com excepção da intercepção de comunicações e das acções encobertas), se apliquem aos processos relativos, não apenas aos crimes previstos nessa lei, mas também àqueles que sejam cometidos por meio de sistema informático ou relativamente aos quais haja de se proceder à recolha de prova em suporte electrónico (em suma, a todos os crimes[4]).

Os dados informáticos apresentam várias características que justificam grande parte do regime aplicável aos meios de obtenção de prova digital e que devem sempre estar presentes na mente dos actores do mundo judiciário, na medida em que definirão igualmente o sucesso ou insucesso de estratégias processuais. Não pretendendo oferecer-se um catálogo de todas as particularidades da prova digital, dir-se-á que as características mais comumente identificadas são as seguintes[5]:

a) Incorporeidade – os dados informáticos não têm uma existência corpórea, não sendo assim apreensíveis pelos sentidos humanos e antes dependendo da mediação de uma máquina que os converta para uma linguagem compreensível para os seres humanos.

b) Fragilidade – diferentemente do que sucede com meios de prova corpóreos, os dados informáticos são facilmente destrutíveis através da mera inserção de um conjunto de comandos na máquina que os processe ou armazene, havendo ainda o risco adicional que representa o curto tempo de vida útil dos suportes digitais (agravado num quadro de obsolescência programada).

c) Corruptibilidade – os dados informáticos são também facilmente adulteráveis, mesmo de forma acidental e não intencional, podendo essa adulteração resultar inclusivamente dos processos de obtenção, análise e utilização processual desses dados. Esta alterabilidade,

[4] Neste sentido, PAULO DÁ MESQUITA, "Prolegómeno Sobre Prova Electrónica e Intercepção de Telecomunicações no Direito Processual Penal Português – O Código e a Lei do Cibercrime", *Processo Penal, Prova e Sistema Judiciário*, Coimbra Editora, 2010, pp. 108-111.

[5] Para maiores desenvolvimentos, embora com algumas diferenças em relação às características da prova digital aqui enunciadas, veja-se DAVID SILVA RAMALHO, *Métodos Ocultos de Investigação Criminal em Ambiente Digital*, Almedina, 2017, pp. 102-108.

muitas vezes imperceptível ao olho não treinado, é suficiente para poder provocar a irreversível perda de valor probatório dos dados informáticos[6].

Além destas características, que cremos serem inerentes a todos os dados informáticos, podem ainda encontrar-se outras particularidades tendenciais, como sejam a dispersão geográfica (por ocorrer armazenamento em servidores sitos em diferentes jurisdições) ou a permanente evolução técnica (surgimento de novos formatos digitais e obsolescência de formatos antigos).

2.2. A Lei do Cibercrime – generalidades e definições legais

Em matéria de prova digital em processos criminais, a Lei do Cibercrime constitui o diploma central, pese embora a tortuosa necessidade de a conjugar com outros diplomas, designadamente o CPP, a Lei n.º 41/2004, de 18 de Agosto, ou a Lei n.º 32/2008, de 17 de Julho[7].

O aludido diploma revogou a Lei n.º 109/91, de 17 de Agosto (Lei da Criminalidade Informática), e teve como fontes principais a Decisão-Quadro 2005/22/JAI do Conselho, de 24 de Fevereiro de 2005, e a Convenção sobre Cibercrime do Conselho da Europa, de 23 de Novembro de 2001[8], vulgarmente designada como Convenção de Budapeste[9], razão pela qual estes instrumentos internacionais constituem elementos interpretativos relevantes para compreender o alcance de algumas soluções legislativas acolhidas.

Em termos sistemáticos, a LC divide-se em cinco capítulos autónomos, agregando matérias substantivas e adjectivas, a saber:

(i) Capítulo I, contendo a identificação do objecto do diploma e as definições legais aplicáveis (arts. 1.º e 2.º);

(ii) Capítulo II, no qual se contêm os tipos incriminadores e demais disposições de natureza substantiva (arts. 3.º a 10.º);

---

[6] É comum falar-se, a este respeito, na preservação da cadeia de custódia forense (*forensic chain of custody*) para expressar a ideia da necessidade de manutenção da integridade da prova digital obtida, através de um registo circunstanciado de todos os acessos aos dispositivos que contêm prova digital – neste sentido veja-se o *Electronic Evidence Guide*, do Conselho da Europa, de 3 de Fevereiro de 2013 p. 14, consultável em https://www.coe.int/en/web/cybercrime/home.

[7] A conjugação e dilucidação do âmbito de aplicação do art. 189.º do CPP, da Lei do Cibercrime, da Lei n.º 41/2004, de 18 de Agosto, e da Lei n.º 32/2008, de 17 de Julho, são matérias que extravasam o âmbito do presente trabalho, mas não deixaremos de referir que nos parece essencialmente correcto o esforço interpretativo desenvolvido no Acórdão do TRE, datado de 20 de Janeiro de 2015, proferido no processo n.º 648/14.6GCFAR-A.E1 e disponível em www.dgsi.pt.

[8] Aberta à assinatura em 23 de Novembro de 2001 e com entrada em vigor em 1 de Julho de 2004, na sequência da verificação do mínimo de cinco ratificações exigidas para o efeito (art. 36.º, n.º 3, da Convenção).

[9] Para uma análise mais desenvolvida dos antecedentes da Lei do Cibercrime, veja-se PEDRO VERDELHO, "A nova Lei do Cibercrime", *Scientia Ivridica*, Tomo LVIII, n.º 320 – Outubro/Dezembro de 2009, Universidade do Minho e "A Convenção sobre Cibercrime do Conselho da Europa – Repercussões na Lei Portuguesa", *Direito da Sociedade da Informação – Volume VI*, Coimbra Editora 2006, pp. 257-276.

(iii) Capítulo III, no qual se inclui, sob a menção de "disposições processuais", o conjunto de dispositivos que regulamentam os meios de obtenção de prova em ambiente digital (arts. 11.º a 19.º);

(iv) Capítulo IV, no qual estão vertidas as disposições respeitantes à cooperação judiciária internacional (arts. 20.º a 26.º) e

(v) Capítulo V, contendo as disposições finais e transitórias.

Esta sistemática revela que o diploma em causa acaba por ser uma agregação, algo desconexa, de matérias de natureza diversa, cujo único ponto comum parece ser a ligação a ambientes digitais. No fundo, é como se o legislador tivesse reunido num único diploma extravagante disposições que poderiam pertencer ao Código Penal, ao Código de Processo Penal e à Lei da Cooperação Judiciária Internacional em Matéria Penal, por serem matérias ainda novas e que sofreriam modificações futuras (embora, paradoxalmente, a LC mantenha inalterada a redacção originária).

É também de notar que a LC não veio oferecer resposta a todas as interrogações que se colocam relativamente a meios de obtenção de prova em ambiente digital, como sejam as buscas *online* (sem conhecimento do visado e eventualmente através de uso de técnicas de *hacking* ou de *malware*) ou a localização de viaturas através de GPS[10]. Por outro lado, não esgota o âmbito das diligências probatórias que respeitem a prova digital, aplicando-se as normas gerais do CPP designadamente ao nível dos exames e perícias.

A LC contém um elenco de definições legais no seu art. 2.º, as quais condicionam o sentido e alcance de várias das soluções legais adoptadas nesse diploma, destacando-se, além da noção de dados informáticos, já acima abordada, as noções de:

a) Sistema informático, definido latamente como qualquer dispositivo ou conjunto de dispositivos interligados ou associados, que desenvolva um tratamento automatizado de dados informáticos, bem como as redes que suportem comunicações entre dispositivos e o conjunto de dados de que depende o funcionamento, utilização, protecção e manutenção desses dispositivos (art. 2.º, alínea a), da LC).

b) Dados de tráfego, definidos para efeitos deste diploma[11] como sendo os dados informáticos relacionados com uma comunicação efectuada por um sistema informático e gerados pelo mesmo como elemento de uma cadeia de comunicação, os quais indicam a origem, destino, trajecto, data, hora, tamanho e duração da comunicação ou qualquer tipo de serviço subjacente (art. 2.º, alínea c), da LC).

[10] Sobre estas questões, veja-se CONDE CORREIA, "Prova digital: as leis que temos e a lei que devíamos ter", *Revista do Ministério Público*, n.º 139, pp. 42-44 e 56-58.
[11] Esta precisão é importante, porquanto não se trata da única definição legal de dados de tráfego, como se alcança do confronto com o teor do art. 2.º, n.º 1, alínea d), da Lei n.º 41/2004, de 18 de Agosto.

c) Fornecedor de serviço, latamente definido como toda a entidade pública ou privada que faculte aos utilizadores dos seus serviços a possibilidade de comunicar por meio de um sistema informático ou que trate ou armazene dados informáticos em nome e por conta da prestadora de serviço ou dos seus utilizadores (art. 2.º, alínea d), da LC).

3. Obtenção e análise de prova digital

3.1. As medidas cautelares previstas na LC

A LC prevê, nos seus arts. 12.º e 13.º, que colhem inspiração dos arts. 16.º e 17.º da Convenção de Budapeste, dois mecanismos que correspondem, rigorosamente, a medidas cautelares, por se limitarem a permitir a conservação de dados informáticos por quem tenha a sua disponibilidade, tendo em vista um eventual pedido posterior para a sua disponibilização.

Principiando pela preservação expedita de dados, prevista no art. 12.º da LC, a mesma consiste num "congelamento" de dados informáticos armazenados em dado sistema informático, por período circunscrito. Efectua-se através de uma ordem, emanada da autoridade judiciária competente e dirigida ao fornecedor de serviço, e funda-se na existência de um receio de perda, alteração ou indisponibilidade desses dados (art. 12.º, n.ºs 1 e 4). A referida ordem poderá ser igualmente veiculada por órgão de polícia criminal, mediante prévia autorização da autoridade judiciária ou em caso de urgência (art. 12.º, n.º 2). Em qualquer caso, a ordem de preservação terá, imperativamente e sob pena de nulidade, de discriminar a natureza, origem e destino dos dados e o período de preservação, que não poderá ultrapassar três meses, sem prejuízo de eventuais prorrogações por igual período e até a uma duração global de um ano (art. 12.º, n.ºs 3 e 5).

Já a revelação expedita de dados de tráfego, prevista no art. 13.º da Lei do Cibercrime, traduz-se numa operação acessória de identificação de outros fornecedores de serviço que tenham participado no circuito de dada comunicação, a realizar por parte do fornecedor de serviço intimado, habilitando assim a autoridade judiciária ou órgão de polícia criminal a solicitarem, também a estes, a preservação dos dados correspondentes.

A razão de ser das referidas medidas cautelares assenta, não apenas na já referida fragilidade e corruptibilidade dos dados informáticos, mas também e sobretudo na existência de prazos máximos de preservação de determinados dados informáticos, essencialmente por razões de protecção de dados pessoais[12], como sucede com aqueles previstos no art. 6.º, n.º 3, da Lei n.º 41/2004, de 18 de Agosto (aplicável aos dados de base de comunicações electrónicas), e no art. 6.º da Lei n.º 32/2008, de 17 de Julho (aplicável aos dados de tráfego e de localização,

[12] A jurisprudência firmada pelo TJUE, no caso Digital Rights Ireland (processos n.ºs C-293/12 e C-594/12, acórdão datado de 8 de Abril de 2014), declarando inválida a Directiva n.º 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de Março de 2006, que foi transposta pela Lei n.º 32/2008, de 17 de Julho, veio lançar algumas interrogações quanto ao futuro desse regime legal. Chamado a pronunciar-se sobre a questão, o Tribunal Constitucional, no Acórdão n.º 420/2017, decidiu no sentido da não inconstitucionalidade do regime nacional, sopesando os argumentos expendidos pela jurisprudência europeia. Cremos ser esta a posição correcta, fazendo igualmente nossa a linha de raciocínio desenvolvida na Nota Prática n.º 7/2015 do Gabinete Cibercrime da Procuradoria-Geral da República, disponível no SIMP.

gerados por comunicações electrónicas)[13]. Quanto às categorias de dados a que aludem estes dois últimos diplomas, a ordem de preservação deverá ser obviamente enviada ao fornecedor de serviço antes do término do prazo máximo de conservação de dados. Por outro lado, e em qualquer caso, a diligência probatória que permita o acesso definitivo aos dados deverá ser realizada antes do termo do prazo máximo de vigência da ordem de preservação.

3.2. A injunção para apresentação ou concessão de acesso a dados

A injunção para apresentação ou concessão de acesso a dados, prevista no art. 14.º da LC, é um meio de obtenção de prova de génese anglo-saxónica (onde as *injunctions* são de uso bastante disseminado) e que tem como fonte principal o art. 18.º da Convenção de Budapeste. No essencial, corresponde a uma ordem emanada por autoridade judiciária, para apresentação ou acesso a dados informáticos, e dirigida a quem tenha a disponibilidade do sistema informático onde se encontram os mesmos, sendo o incumprimento considerado crime de desobediência (art. 14.º, n.ºs 1 a 3).

A referida injunção pode ser dirigida a todo o tipo de entidades[14], incluindo fornecedores de serviços (unicamente para obtenção de dados de base, pois a obtenção de dados de tráfego e conteúdo é objecto de regime diverso), mas excluindo suspeitos ou arguidos (por força do direito à não auto-inculpação) e sistemas informáticos utilizados para o exercício da advocacia, actividades médicas, bancárias ou jornalísticas (por força dos regimes de segredo profissional correspondentes[15]), aplicando-se o regime previsto no art. 182.º do CPP (art. 14.º, n.ºs 4 a 7).

Ao nível da obtenção de dados relativos a comunicações electrónicas (que não esgotam o âmbito de aplicação da injunção, que abrange todo o tipo de dados informáticos), alguns operadores de serviços, após o recebimento aludida injunção, têm assumido a posição de que a obtenção de dados relativos a determinado endereço IP (*Internet Protocol*) não poderá ser ordenada pelo Ministério Público, tendo antes de o ser pelo Juiz de Instrução Criminal, por se tratar de dados de tráfego e não de base[16].

[13] Sobre a conjugação dos diversos prazos de conservação legalmente previstos, veja-se a Nota Prática n.º 8/16, de 18 de Fevereiro de 2016, do Gabinete Cibercrime da Procuradoria-Geral da República, devendo ainda considerar-se o prazo máximo de 90 (noventa dias) de conservação de dados de tráfego que é habitualmente respeitado pelos operadores norte-americanos.

[14] Como refere PEDRO VERDELHO, "A nova Lei do Cibercrime", *Scientia Ivridica*, Tomo LVIII, n.º 320, p. 739, além dos fornecedores de serviços, também as estruturas empresariais onde suspeitos exerçam funções, e em cujos sistemas possa existir prova digital das suas actividades ilícitas, serão destinatários paradigmáticos da injunção.

[15] Nestes casos, caberá ao Juiz de Instrução Criminal determinar que seja fornecido acesso aos aludidos dados informáticos, sopesando os interesses do segredo em causa e do exercício do poder punitivo. Veja-se a este propósito o Acórdão do TRP, datado de 7 de Dezembro de 2016, proferido no proc. n.º 1689/16.4JAPRT-A.P1, e disponível em www.dgsi.pt.

[16] Esta posição encontra-se ancorada numa corrente jurisprudencial minoritária, de que constituem exemplos o Acórdão do TRE, proferido no proc. n.º 1276/09.3TAPTM-B.E1 e datado de 27 de Janeiro de 2011, e o Acórdão do TRC, proferido no proc. n.º 84/11.6JAGRD-A.C1 e datado de 3 de Outubro de 2012, ambos disponíveis em www.dgsi.pt.

Seguindo de perto o entendimento constante do Parecer do Conselho Consultivo da PGR de 28 de Agosto de 2000, e da maioria da jurisprudência[17], diremos que, ao nível de dados necessários ou gerados por comunicações electrónicas, as categorias de dados de base, tráfego e conteúdo se diferenciam essencialmente nos seguintes termos:

a) Dados de base são aqueles necessários para que o utilizador aceda à rede, como sejam a identificação do utilizador, morada e todas as credenciais de acesso. Em termos simplistas, poderá dizer-se que os dados de base são os elementos nucleares de estabelecimento de um ponto de comunicação, através do qual se pode aceder a uma rede.

b) Dados de tráfego são aqueles que permitem identificar a existência de uma comunicação entre dois utilizadores, abrangendo a direcção, destino, trajecto e duração dessa comunicação. Através destes dados, é possível saber que ocorreu uma comunicação electrónica entre dois sistemas informáticos e quais as suas particularidades, com excepção do correspondente conteúdo.

c) Dados de conteúdo são aqueles que correspondem ao teor da comunicação, permitindo determinar se a mesma se traduziu numa conversação em texto, áudio ou vídeo, qual o significado e sentido dessa comunicação, se a mesma foi acompanhada de outros elementos ou ficheiros e qual a natureza dos mesmos, etc.

No que concerne ao endereço IP, dir-se-á, de forma simplista e sem pretensão de grande rigor técnico, que se trata de um número de acesso atribuído a cada dispositivo electrónico que se ligue à Internet, aparentado com o número de telefone para as telecomunicações. Na sua versão actual (IPv4), o endereço IP é composto por uma sequência de quatro números, compreendidos entre 0 e 255, separados por pontos, sendo os endereços geridos globalmente por uma organização sem fins lucrativos, designada *Internet Corporation for Assigned Names and Numbers* (ICANN).

Dada a finitude das combinações possíveis de números que compõem o endereço IP na sua versão actual e a desproporção em relação ao número de utilizadores, existem endereços IP dinâmicos, utilizados indiferenciadamente pelos vários dispositivos electrónicos que se vão ligando à rede e ficando disponíveis para uso por outros, logo que cesse a conexão à rede.

Pelo conhecimento do endereço IP (e, no caso de se tratar de IP dinâmico, também da data e hora em que o mesmo terá sido utilizado), é apenas possível identificar o ponto através do qual foi estabelecida a ligação à rede, mais concretamente a identificação do contratante do serviço de Internet e a sua morada. Os dados obtidos através da revelação do titular de um endereço IP correspondem assim unicamente a dados de base, uma vez que nada revelam quanto à direcção, destino, trajecto e duração de uma comunicação, e muito menos quanto ao seu conteúdo.

[17] A título exemplificativo refiram-se o Acórdão do TRL, datado de 18 de Janeiro de 2011 e proferido no proc. n.º 3142/09.3PBFUN-A.L1-5, e o Acórdão do TRP, datado de 10 de Setembro de 2014 e proferido no proc. n.º 1953/00.4JAPRT-B.P1, ambos disponíveis em www.dgsi.pt

Por esse motivo, e em face do teor do art. 14.º, n.º 4, da LC, impõe-se concluir que o Ministério Público é competente para solicitar directamente aos fornecedores de serviço que providenciem essa informação, mostrando-se desnecessária a intervenção do Juiz de Instrução Criminal[18] (além de injustificada, por não haver direitos fundamentais que hajam de ser acautelados no caso vertente).

No respeitante aos dados de tráfego e de localização associados a comunicações electrónicas, aí sim caberá ao Juiz de Instrução Criminal determinar a sua transmissão para efeitos de investigação criminal, nos termos do art. 9.º da Lei n.º 32/2008, de 17 de Julho, e desde que esteja em causa crime de catálogo. No atinente aos dados de conteúdo, não existe norma que habilite qualquer conservação dos mesmos pelos fornecedores de serviços, pelo que a sua obtenção apenas poderá ser obtida por outros meios, como sejam a pesquisa de dados informáticos ou a intercepção de comunicações.

Tem sido igualmente frequente, no contacto do Ministério Público com Google, Facebook, Microsoft e outros grupos multinacionais[19], uma certa falta de colaboração destas entidades com as autoridades portuguesas[20], umas vezes escondida por detrás de repetidas exigências de informações adicionais e outras vezes mais abertamente traduzida em recusas polidas, fundadas em argumentos vários, que vão desde a inexistência de incriminação equivalente na sua jurisdição, até à invocação de argumentos economicistas.

Sobre esta questão, cremos que a postura de um certo fatalismo ou resignação que parece ser adoptada por alguns titulares de inquéritos não poderá ser o caminho. A verdade é que, independentemente de as referidas entidades se encontrarem sedeadas no estrangeiro, as mesmas desenvolvem actividade que abrange o espaço territorial português e aqui obtêm ganhos avultados, pelo que terão de se acomodar ao cumprimento das leis portuguesas. Aos Magistrados caberá darem uso aos instrumentos que se encontram ao seu dispor, designadamente abrindo os correspondentes inquéritos para investigação da prática do crime de desobediência[21], que constitui a cominação para a falta de colaboração imposta pelo art. 14.º, n.ºs 1 e 3, da LC, e promovendo a condenação dessas entidades em multa processual, por falta de colaboração, nos termos do disposto no art. 521.º do CPP, tudo sem prejuízo da eventual necessidade de negociação de protocolos ou procura de soluções políticas.

[18] Chegamos assim à mesma conclusão que o Gabinete Cibercrime da Procuradoria-Geral da República, constante das Notas Práticas n.ºs 1/2012 e 2/2013, ambas disponíveis no SIMP, onde a questão é abordada de modo mais desenvolvido, com alusão ao normativo da Convenção de Budapeste que constitui fonte essencial do art. 14.º da LC e ao sentido dado ao mesmo no *Explanatory Report to the Convention of Cybercrime*, disponível em https://rm.coe.int/16800cce5b.

[19] O Ministério Público português estabeleceu canais informais de comunicação por via electrónica com Google, Microsoft, Facebook e Instagram, tendo em vista agilizar a interacção com essas entidades, encontrando-se os correspondentes formulários disponíveis no SIMP.

[20] Sobre a (parca) colaboração prestada pelos fornecedores de serviços baseados nos EUA é eloquente o relatório elaborado pelo Gabinete Cibercrime da Procuradoria-Geral da República, datado de 22 de Dezembro de 2014, e disponível no SIMP: vários operadores evidenciam taxas de respostas positivas bastante baixas. Não se poderá assacar todas as recusas às deficiências de preenchimento dos formulários por parte dos Magistrados.

[21] Não haverá contudo crime quando a recusa de colaboração seja fundada numa interpretação razoável e fundada da lei – neste sentido veja-se o Acórdão do TRE, proferido no proc. n.º 3506/15.3T9FAR.E1, datado de 02-05-2017 e disponível em www.dgsi.pt.

3.3. A pesquisa de dados informáticos

A pesquisa de dados informáticos, que se encontra regulada no art. 15.º da LC, é vulgarmente vista como uma espécie de "busca"[22] em ambiente virtual, não surpreendendo assim a remissão constante do n.º 6 desse normativo para o regime das buscas.

Ao nível dos pressupostos materiais de utilização da pesquisa de dados informáticos, constantes do art. 15.º, n.º 1, da LC, são de destacar a necessidade para a descoberta da verdade de dados informáticos específicos e determinados, e o seu armazenamento em determinado sistema informático.
Esta forma de redigir o normativo em causa parece evidenciar que a realização da pesquisa depende de uma prévia identificação de dados informáticos com relevo probatório e de um sistema informático onde os mesmos se encontrem. Cremos, contudo, que basta uma identificação relativamente difusa mas minimamente concretizada dos sistemas informáticos visados e dos dados informáticos pretendidos, para que encontre justificação o uso deste meio de obtenção de prova.

Ao nível da competência para a determinação da realização da diligência, a regra geral, prevista no n.º 1 do art. 15.º, é a de que a mesma cabe à autoridade judiciária competente, a qual será sempre o Ministério Público em sede de inquérito. Admite-se contudo, como se alcança do disposto nos n.ºs 3 e 4 do art. 15.º, que o órgão de polícia criminal proceda à pesquisa sem prévia autorização da autoridade judiciária competente, em circunstâncias excepcionais, como sejam o consentimento (documentado) prestado por quem tenha a disponibilidade do sistema informático ou a verificação de iminência de crime que coloque em risco a vida ou integridade física de qualquer pessoa, em contexto de terrorismo, criminalidade violenta ou altamente organizada. Fora destes casos, a pesquisa realizada sem prévio despacho de autoridade judiciária será nula, nos termos do art. 126.º, n.º 3, do CPP[23].

Importa ainda ter presente a remissão do art. 15.º, n.º 6, para os regimes das buscas previstos no CPP e no Estatuto do Jornalista, dos quais resultam diversas situações especiais ao nível da competência para a determinação da realização da diligência e da necessidade de participação de representantes de determinadas classes profissionais, por razões de sigilo profissional. Em termos sintéticos, esta remissão, que será para os arts. 177.º, n.º 6, do CPP e 11.º, n.º 6, do Estatuto do Jornalista, implica que a diligência seja presidida pelo Juiz de Instrução Criminal e se encontre presente representante da classe profissional do visado.

Em termos formais, o despacho que ordene a pesquisa de dados informáticos tem a validade máxima de 30 dias, sob pena de nulidade (art. 15.º, n.º 2, da LC), exigindo-se, quando não haja prévio despacho, a validação da mesma pela autoridade judiciária (art. 15.º, n.º 4, da LC). Embora a LC não estabeleça um prazo concreto para a validação da pesquisa informática, parece-nos que a remissão para o regime das buscas, constante do art. 15.º, n.º 6,

[22] Note-se que o art. 19.º da Convenção de Budapeste fala expressamente em busca e apreensão de dados informáticos, tendo o legislador português optado por diversa terminologia.
[23] Veja-se o Acórdão do TRE, proferido no proc. n.º 445/10.8JAFAR.E2, datado de 2 de Maio de 2017 e disponível em www.dgsi.pt.

contemplará o disposto nos arts. 174.º, n.º 6 e 251.º, n.º 2, do CPP, com a inerente necessidade de comunicação imediata à autoridade judiciária. A diferença radicará aqui na concreta autoridade judiciária competente para a validação: no caso das buscas, prevê-se que será o Juiz de Instrução Criminal a proceder à validação, ao passo que na LC se prevê a validação pela autoridade judiciária competente, que será o Ministério Público durante o inquérito.

O n.º 5 do art. 15.º da LC prevê um regime de extensão da pesquisa de dados informáticos, admitindo que a mesma possa contemplar o acesso a sistema informático diverso do pesquisado, sempre que o mesmo seja legitimamente acessível a partir deste. Esta extensão encontra-se dependente de autorização ou ordem da autoridade competente, razão pela qual este aparente regime de extensão acaba afinal por se traduzir numa mera ordem de realização de nova pesquisa informática, apresentando como única especificidade a realização da mesma por via remota, ou seja a partir do primeiro sistema pesquisado.

Esta norma suscita várias dúvidas de natureza interpretativa e prática, designadamente ao nível do que deva entender-se por acesso legítimo, e às especificidades que coloca a realização de pesquisa de dados informáticos por via remota, quando o correspondente sistema informático se encontre em país estrangeiro ou opere em nuvem.
Relativamente à noção de acesso legítimo, o significado deste último vocábulo aponta no sentido de o legislador ter pretendido incluir, com alguma amplitude, todos os acessos que não sejam proibidos por lei. Aqui se incluirão, além das pesquisas expressamente consentidas pelo titular dos dados informáticos constantes do sistema acessível remotamente, aquelas que incidam sobre sistemas informáticos de acesso público ou que possam ser acedidos através de credenciais que se encontrem introduzidas no sistema informático originariamente pesquisado[24].

Alguma doutrina discute ainda se a prevista extensão é legitimadora de pesquisas de dados informáticos que se encontrem armazenados em sistemas informáticos situados no estrangeiro, havendo quem conclua em sentido negativo[25], objectando que tal consubstanciaria uma violação da soberania do Estado onde o servidor se encontra.

Embora se trate de tema dotado de complexidade justificativa de um tratamento mais aprofundado, diremos sinteticamente que não vislumbramos razão para se negar que a extensão da pesquisa informática possa contemplar sistemas informáticos fisicamente sitos no estrangeiro, desde que se mostre viável o acesso remoto aos mesmos a partir de território nacional.

Cremos até que o legislador pretendeu, precisamente, contemplar essas situações (pense-se na situação de, no decurso da pesquisa informática, se descobrir que o visado utilizava o sistema pesquisado para aceder ao Facebook, Google Drive, Instagram ou qualquer outro

[24] Como sucede com a conta de correio electrónico do visado, que poderá ser acedida por esta via. Neste sentido, veja-se PEDRO VERDELHO, "A nova Lei do Cibercrime", *Scientia Ivridica*, Tomo LVIII, n.º 320, p. 742.
[25] É o caso de DAVID SILVA RAMALHO, *Métodos Ocultos de Investigação Criminal em Ambiente Digital*, pp. 87-91.

servidor estrangeiro, e que as credenciais de acesso se encontravam já introduzidas ou memorizadas no aparelho pesquisado).

No que concerne a eventuais conflitos de soberania, diremos que, atendendo às modalidades de apreensões de ficheiros informáticos descritas no art. 16.º, n.º 7, da LC, o acesso remoto dificilmente permitirá fazer mais do que uma cópia dos ficheiros que sejam encontrados no sistema remotamente acedido. Essa cópia, em princípio (e idealmente, sob pena de não ser probatoriamente fidedigna), deixará intocados os ficheiros originais, pelo que o acesso remoto será inócuo para a integridade do sistema informático remotamente acedido, não se vislumbrando assim qualquer actuação que possa ser tida como invasiva da soberania alheia.

Cumpre ainda lembrar que, a partir do momento em que um Estado admite que sejam prestados serviços de Internet no seu território, está a abrir uma margem de liberdade para que os seus cidadãos acedam a dados existentes em sistemas situados no estrangeiro e vice-versa. Daí que os acessos legítimos realizados por autoridades policiais ou judiciárias de países estrangeiros, integrados nesta margem de liberdade consentida, se contenham dentro dos limites do respeito da soberania alheia.

Por fim, refira-se que a adopção de uma espécie de princípio da territorialidade em matéria de pesquisa de dados informáticos se mostra de todo incompatível com os desafios concretamente suscitados pela cibercriminalidade em geral[26] e pelos sistemas de computação em nuvem[27] em particular, dado que a localização territorial dos dados informáticos é fluida e constantemente mutável, com especial intensidade neste último caso.

Exigir-se que se dê uso aos mecanismos de cooperação judiciária internacional, com a sua morosidade intrínseca, implicará abrir uma ampla margem de impunidade, ao tornar impossível a obtenção de prova em grande parte das situações, e afrontará flagrantemente o espírito da LC (e da Convenção de Budapeste), de onde ressalta uma intencionalidade de obstar à existência de espaços livres de jurisdição penal, e de que é exemplo lapidar a amplitude de aplicação da lei no espaço e da competência internacional dos tribunais portugueses, prevista no art. 27.º da mesma.

Uma palavra ainda para a eventual possibilidade de uso de *malware*[28] para efectivação da pesquisa de dados informáticos (designadamente para efeitos da já aludida busca *online*, à

[26] Sobre estes desafios, veja-se ÁLVARO MANUEL MONGE CALLEJA, "A Investigação criminal face à Globalização e o Cibercrime", *Investigação Criminal*, n.º 11, ASFICPJ, Fevereiro de 2017, pp. 170-187.
[27] A complexidade do funcionamento dos sistemas de computação em nuvem torna particularmente difícil avançar com uma definição facilmente apreensível pelo leigo. De forma assumidamente simplista e tecnicamente imprecisa, diremos que se trata de uma plataforma de serviços, explorada por uma entidade que utiliza e mantém diversos dispositivos electrónicos de processamento e armazenamento de dados, ligados à rede, a qual disponibiliza essa capacidade de armazenamento a terceiros, que poderão transferir dados informáticos para esses servidores, gratuitamente ou a troco de uma remuneração.
[28] Vocábulo anglo-saxónico de uso corrente entre nós, que resulta da aglutinação dos vocábulos "*malicious*" e "*software*", e que corresponde a uma designação abrangente de todos os programas informáticos de natureza lesiva ou intrusiva, instalados num sistema informático contra a vontade do seu titular e propiciando que esse sistema realize certas actividades à revelia da vontade do dito titular. Para maiores desenvolvimentos e compreensão das categorias mais frequentes de *malware*, veja-se DAVID SILVA RAMALHO, *Métodos Ocultos de Investigação Criminal em Ambiente Digital*, pp. 318-324.

revelia do conhecimento do buscado). A lei não prevê essa possibilidade, e cremos que a mesma se mostra incompatível com o regime previsto para a pesquisa de dados informáticos, mormente por esta pressupor a entrega do despacho que ordena a diligência a quem tenha a disponibilidade do sistema informático, afigurando-se assim como um meio de obtenção de prova cuja realização é conhecida pelo visado, o que nos parece de difícil conciliação com o uso de *software* oculto ou dissimulado (o que não prejudica o uso de *malware* no contexto dos meios ocultos de obtenção de prova digital).

3.4. Apreensões de dados informáticos e de correio electrónico

A apreensão, que contém o seu regime geral nos arts. 178.º a 186.º do CPP, corresponde, sinteticamente, à manutenção física e temporária de determinado objecto na esfera de domínio das autoridades estaduais, e na dependência de um processo judicial para cuja resolução esse objecto revela interesse, designadamente por poder servir de prova ou por poder vir a ser declarada a sua perda a favor do Estado.

Por regra, a apreensão pressuporá assim uma actuação física das autoridades estaduais sobre uma realidade corpórea, a qual se traduz na sua retirada do âmbito de disponibilidade dos seus titulares, e na sua colocação na esfera de domínio estadual, de onde não poderá ser movida até existir decisão da autoridade competente para o efeito.

A LC, nos seus arts. 16.º e 17.º, prevê modalidades especiais de apreensão, respectivamente relativas a dados informáticos e a correio electrónico. Dada a imaterialidade destas realidades e a tendencial corporeidade das realidades para as quais foi pensado o regime geral das apreensões, é natural que o legislador tenha considerado necessária a criação de um regime especial, com vista a lidar com as idiossincrasias da prova digital.

Principiando pela apreensão de dados informáticos, prevista no art. 16.º, a mesma pressupõe uma prévia pesquisa informática ou acesso legítimo a um sistema informático, no decurso do qual ocorra a descoberta de dados informáticos com relevância probatória para processo criminal pendente (art. 16.º, n.º 1), sendo assim evidente que a apreensão surge como passo logicamente posterior à realização de diligência de obtenção de prova digital[29].

Ao nível da competência, incumbe à autoridade judiciária competente em cada fase processual determinar a realização da apreensão de dados informáticos, razão pela qual será ao Ministério Público que assistirá tal prerrogativa durante o inquérito (art. 16.º, n.º 1).

Admite-se contudo que o órgão de polícia criminal possa realizar as apreensões, sem prévio despacho da autoridade judiciária, quando a mesma ocorra no decurso de uma pesquisa informática ordenada nos termos do art. 15.º ou quando exista perigo ou urgência na demora

[29] Não se inclui aqui e, consequentemente, não corresponde à apreensão de dados informáticos, a mera cópia de dados que se encontrem publicamente acessíveis na Internet, como seja a informação que alguém publicita em mural de Facebook, sem qualquer restrição de acesso. Neste sentido, veja-se o Acórdão do TRP, datado de 5 de Abril de 2017, proferido no proc. n.º 671/14.0GAMCN.P1 e disponível em www.dgsi.pt.

(art. 16.º, n.º 2). Estes dois desvios à regra geral de competência justificam-se por motivos diversos: no primeiro caso, por já existir uma pesquisa informática licitamente ordenada e executada, pode afirmar-se ter já sido sopesado o inconveniente que daí advirá para o titular dos dados informáticos; no segundo caso, e à semelhança do que sucede com outros regimes especiais, a salvaguarda da pretensão do poder punitivo estadual é justificação bastante para que as formalidades habituais sejam afastadas. Seja como for, as apreensões realizadas nestes termos não dispensam a posterior necessidade de validação pela autoridade judiciária, como resulta do disposto no art. 16.º, n.º 4.

O art. 16.º, n.º 3, da LC prevê um regime específico para a apreensão de dados ou documentos informáticos cujo conteúdo corresponda a dados pessoais ou íntimos, exigindo, sob pena de nulidade, que os mesmos sejam apresentados ao Juiz de Instrução Criminal, a quem incumbirá decidir a pertinência da junção dos mesmos aos autos, sopesando os interesses da perseguição criminal e da integridade dos direitos fundamentais potencialmente atingidos.

Embora a lei não refira um prazo para que tais dados sejam levados ao conhecimento do Juiz, parece-nos imperioso concluir que a apresentação deverá ocorrer logo que sejam descobertos dados informáticos dessa natureza, sob pena de frustração da finalidade da norma que é, precisamente, evitar que a vida privada e íntima dos cidadãos possa ser devassada, com a difusão da informação correspondente por terceiros.

Ciente das especificidades da apreensão da prova digital, designadamente ao nível dos procedimentos a adoptar para a sua conservação, o legislador fez constar do art. 16.º, n.º 7, da LC um conjunto exemplificativo de formas de efectivação da apreensão. Acabou, contudo, por fazê-lo de forma deficiente, confundindo actuações que são materialmente apreensões, com outras que são estranhas a essa realidade[30].

Assim, as duas primeiras modalidades previstas (apreensão do suporte onde está o sistema ou os dados informáticos e dispositivos necessários à sua leitura, e realização de cópia de dados em suporte autónomo) são indubitavelmente formas de efectivação da apreensão, na medida em que pressupõem que os dados informáticos correspondentes fiquem na esfera de domínio das autoridades estaduais.

O mesmo não sucede com a mera preservação da integridade dos dados, sem cópia ou remoção, pois a mesma não implica essa transmissão de disponibilidade e não dispensa uma posterior operação para efectivação da apreensão. Já quanto à eliminação não reversível ou o bloqueio de acesso a dados parece-nos ser uma realidade inteiramente estranha à apreensão, dado que pressupõe uma destruição dos dados que seriam apreensíveis. Admitimos que o legislador terá pretendido deixar alguma abertura para legitimar as autoridades a suprimirem ou tornarem inacessíveis certos dados informáticos com potencial lesivo de direitos (como ficheiros relativos a pornografia de menores ou susceptíveis de facilitar actividades

[30] Embora se observe que a própria Convenção de Budapeste contém essa parificação no art. 19.º, n.º 3, cremos que o legislador português poderia ter acolhido as diversas matérias aí constantes com diferente sistematização e sem perda de rigor técnico.

terroristas). Contudo, embora a intenção se compreenda, a inserção sistemática desta prerrogativa numa listagem de modalidades de apreensão não foi certamente a mais feliz.

Em complemento desta listagem de modalidades de apreensão, o legislador fez constar do art. 16.º, n.º 8, da LC, um conjunto de procedimentos técnicos a serem observados quando a apreensão seja efectivada através da cópia dos dados em suporte autónomo, designadamente a realização da cópia em duplicado, com uma das cópias a ser confiada ao secretário judicial e a certificação dos dados apreendidos por meio de assinatura digital.

Compreende-se a preocupação do legislador em garantir a fidedignidade da cópia realizada e a sua fiel correspondência ao original copiado e a integridade dos dados apreendidos, dada a tendencial fragilidade e corruptibilidade da prova digital. Voltamos aqui à ideia da preservação da cadeia de custódia, devendo existir um registo de todas as ocasiões e pessoas que manuseiam os aparelhos electrónicos onde se encontrem os dados informáticos com relevo probatório.

Os n.ºs 5 e 6 do art. 16.º contêm remissões para aspectos do regime geral das apreensões, mais concretamente para as disposições que versam sobre os regimes protectivos do segredo profissional das actividades médica, jornalística e de advocacia, bem como para os regimes de segredo profissional e de Estado que o CPP prevê ao nível das apreensões.

Assim, à apreensão de dados informáticos em escritório de advogado ou em consultório médico é aplicável o disposto no art. 180.º do CPP, exigindo-se que a diligência seja presidida pelo Juiz de Instrução Criminal e proibindo-se a apreensão de documentos abrangidos pelo segredo profissional, excepto quando os próprios constituam objecto ou elemento do crime.

Tratando-se de apreensão de dados informáticos em estabelecimento bancário, é aplicável o disposto no art. 181.º do CPP, devendo a diligência ser igualmente presidida por Juiz, o qual pode examinar correspondência ou documentação bancária e deve realizar pessoalmente o exame dos elementos a apreender, embora com possibilidade de coadjuvação por técnicos qualificados ou órgão de polícia criminal, ficando todos sujeitos ao dever de segredo quanto aos factos de que tomem conhecimento e não revistam interesse probatório.

Ao nível do segredo profissional ou de funcionário e de segredo de Estado, é aplicável o disposto no art. 182.º do CPP, que remete em grande medida para o regime dos correspondentes segredos e modo de levantamento ou quebra dos mesmos.

No respeitante aos jornalistas, o art. 11.º, n.ºs 7 e 8, do Estatuto do Jornalista estabelece regras especiais que se aplicam à apreensão de dados informáticos utilizados por jornalistas no exercício da profissão, exigindo-se mandado de Juiz para a sua apreensão e prevendo-se a sua utilização probatória apenas quando seja ordenada a quebra do segredo profissional.

Encontrando-se as remissões para o regime das apreensões circunscritas aos casos indicados, vislumbramos com alguma dificuldade que as demais normas constantes do CPP e reguladoras desta matéria possam ser transponíveis para o âmbito digital. Será este o caso dos normativos

respeitantes às cópias e certidões (art. 183.º do CPP), aposição e levantamento de selos (art. 184.º do CPP), apreensão de coisas sem valor ou perecíveis, perigosas ou deterioráveis (art. 185.º do CPP) ou restituição dos objectos apreendidos (art. 186.º do CPP), cujo desenho claramente orientado para lidar com realidades corpóreas, dificilmente se compatibiliza com a imaterialidade dos dados informáticos. Serão contudo, e sem qualquer dúvida, aplicáveis aos dispositivos electrónicos onde os dados informáticos se encontrem.

À semelhança do que sucede com o regime geral das apreensões, previsto no CPP, a LC estabelece uma regulamentação específica para a correspondência electrónica, prevista no art. 17.º, e contendo um formalismo mais exigente, dada a necessidade de tutela do direito à inviolabilidade da correspondência, extensível também à correspondência de natureza digital.

Diferentemente contudo do que sucede quanto ao regime da apreensão de correspondência previsto no art. 179.º do CPP, o qual incide apenas sobre correspondência fechada (a correspondência aberta é mera prova documental sujeita ao regime geral), a LC não estabelece qualquer diferenciação entre mensagens de correio electrónico abertas ou fechadas (*rectius*, lidas ou não lidas, para usar a terminologia corrente nos serviços de correio electrónico), pelo que o correspondente regime se aplica indiferenciadamente a ambas as situações[31].

A lei parece assim estabelecer um regime mais protector e restritivo para a correspondência electrónica do que para a correspondência física, o que se revela dificilmente justificável. Embora aceitemos que, na correspondência electrónica, a tomada de conhecimento do seu teor depende de um acto de prática tendencialmente exclusiva pelo destinatário, traduzido na introdução das credenciais de acesso à caixa de correio electrónico, temos alguma dificuldade em ver neste acto um qualquer paralelismo com a abertura de correio fechado. No respeitante às mensagens de correio electrónico que possam simplesmente estar gravadas no disco rígido do computador, nem sequer vislumbramos qualquer esboço de analogia com a correspondência fechada.

A LC alude a "*correio electrónico e registos de comunicações de natureza semelhante*", o que indica que o regime em causa, além de ser aplicável aos serviços tradicionais de correio electrónico, incluirá igualmente plataformas de mensagens, como o Facebook Messenger ou o WhatsApp, e ainda as próprias SMS e MMS armazenadas em telemóveis. O critério decisivo será aqui de aproximação à realidade-padrão do correio electrónico, importando aferir se está em causa uma comunicação entre dois indivíduos, que utilizam meios informáticos para esse efeito e concretamente um programa informático que propicie essa comunicação e o eventual armazenamento da mesma para consulta futura[32].

[31] Especialmente crítico desta solução é CONDE CORREIA, "Prova digital: as leis que temos e a lei que devíamos ter", *Revista do Ministério Público*, n.º 139, p.40-41.

[32] Em qualquer caso, falamos apenas em comunicações electrónicas que não sejam livremente disponibilizadas pelo emissor ou receptor, uma vez que, havendo essa disponibilização voluntária, inexiste qualquer potencial violação de Direitos Fundamentais que exija o correspondente juízo de proporcionalidade em face do exercício do poder punitivo. Neste sentido vejam-se, exemplificativamente, o Acórdão do TRP, datado de 20 de Janeiro de 2016, proferido no proc. n.º 1145/08.4PBMTS.P1, e o Acórdão do TRG, datado de 15 de Outubro de 2012 e proferido no proc. n.º 68/10.1GCBRG.G1, ambos disponíveis em www.dgsi.pt. Fora estarão também, segundo cremos, os

Como se depreende do teor do art. 17.º da LC, a apreensão de correio electrónico ou registos de comunicações de natureza semelhante é um meio de obtenção de prova que surge na sequência de uma pesquisa informática ou outro acesso legítimo a um sistema informático, que permitam revelar a existência desse tipo de dados informáticos.

A apreensão propriamente dita depende de autorização ou ordem de Juiz, no sentido de serem apreendidos à ordem do processo aqueles que se afigurem ser de grande interesse para a descoberta da verdade ou para a prova. A menção a um "grande interesse" ao invés do mero "interesse" parece apontar no sentido de o Juiz dever sopesar cuidadosamente as necessidades da investigação criminal em face do previsível dano que se gerará para os direitos fundamentais do visado.

Tirando estas sumárias menções, o art. 17.º da LC efectua uma remissão em bloco para o regime da apreensão de correspondência previsto no art. 179.º do CPP, devendo considerar-se que a mesma não contempla o art. 179.º, n.º 1, do CPP, onde se regulam especificamente as matérias dos pressupostos e autorização judicial necessária, já reguladas na LC, e cujo teor parece estranho à dinâmica do correio electrónico, onde as mensagens potencialmente relevantes surgirão previsivelmente no decurso de uma pesquisa informática já ordenada por autoridade judiciária.

Serão contudo aplicáveis os n.ºs 2 e 3, do art. 179.º do CPP, razão pela qual o correio electrónico trocado entre arguido e advogado só poderá ser apreendido no caso de haver razões para crer que constitua objecto ou elemento do crime, e devendo o Juiz ser sempre o primeiro a tomar conhecimento do conteúdo da correspondência apreendida, determinando qual deverá ser junta ao processo e ficando vinculado ao dever de segredo quanto ao teor das comunicações excluídas do processo.

É precisamente na remissão para o art. 179.º, n.º 3 do CPP que se encontra a principal dificuldade prática de aplicação do regime da apreensão do correio electrónico: considerando que a mesma pressupõe uma prévia pesquisa informática ou outro acesso legítimo a um sistema informático, no qual sejam encontradas mensagens de correio electrónico ou registos semelhantes, parece-nos inevitável que a entidade que realiza aquela pesquisa ou acesso legítimo venha a ser a primeira a tomar conhecimento do teor das mensagens de correio electrónico.

Aliás, cremos até que apenas dessa forma se poderão identificar os dados informáticos dessa natureza e discerni-los dos demais dados que hajam de ser apreendidos nos termos do art. 16.º da LC – com efeito, pode suceder que ao abrir um simples documento Word ou PDF, armazenado no disco rígido de um computador, venham a encontrar-se aí gravadas diversas conversas mantidas através de correio electrónico. Acresce que, sendo normalmente o órgão de polícia criminal quem realizará os referidos acessos ao sistema, os resultados dessas diligências serão comunicados ao Ministério Público, o que levará a que este também tome conhecimento prévio do teor do correio electrónico.

rascunhos de mensagens de correio electrónico, mesmo quando sejam usados como meio de comunicação entre pessoas que possuam as credenciais de acesso à mesma conta de correio electrónico.

Por outro lado, as necessidades da investigação criminal, dada a fragilidade e corruptibilidade dos dados informáticos, a que o correio electrónico não é também alheio, imporão, o mais das vezes, que se proceda imediatamente à preservação do correio electrónico que venha a ser encontrado, de modo a obstar a eventuais acções destrutivas por parte dos visados ou investigados.

Todas estas necessidades práticas mostram-se inconciliáveis com a intencionalidade legislativa de fazer com que o Juiz seja o primeiro a tomar conhecimento do teor das mensagens de correio electrónico ou registos de comunicações de natureza semelhante. Para que tal fosse possível e viável, seria necessário que o Juiz acompanhasse toda e qualquer pesquisa informática ou acesso legítimo a sistema informático, tomando imediatamente conhecimento do teor de quaisquer dados informáticos que tivessem essa natureza, o que é obviamente incomportável.

Em termos práticos, o que se vem observando na prática judiciária é uma preservação das mensagens de correio electrónico e registos de comunicações semelhantes por parte do órgão de polícia criminal, que entrega os correspondentes suportes no Ministério Público, o qual efectua posteriormente a promoção ao Juiz de Instrução Criminal, para que seja ordenada a apreensão das mensagens de correio electrónico relevantes que venham a ser encontradas. Isto significa que, no momento em que é solicitada ao Juiz de Instrução Criminal a apreensão, os dados informáticos em causa já se encontram num estado de "apreensão de facto", por se encontrarem guardados à ordem de determinado processo judicial.

A jurisprudência, embora exigindo sempre uma intervenção de Juiz para a efectivação da apreensão de correio electrónico ou registos de comunicações semelhantes, vem admitindo que esta intervenção não seja necessariamente prévia à realização dos actos materiais de apreensão, que consubstanciariam uma apreensão provisória a ser posteriormente objecto de validação[33]. É contudo notório que a questão não seria suscitada não fosse a manifesta deficiência do regime legal vigente.

Esta deficiência de regime tem-se igualmente evidenciado ao nível da própria decisão do Juiz de Instrução Criminal, o qual tem frequentemente emitido uma mera autorização genérica, remetendo para o órgão de polícia criminal e o Ministério Público a tarefa de discernir quais as mensagens de correio electrónico com interesse para a investigação[34].

Não surpreende que assim seja: contrariamente ao que sucede no âmbito da apreensão física, em que o Juiz de Instrução Criminal tenderá a ser confrontado com um número circunscrito e pouco significativo de cartas ou outro tipo de correspondência, no âmbito do correio electrónico haverá que proceder a uma análise de um número elevadíssimo de mensagens de

[33] Veja-se o Acórdão do Tribunal da Relação de Guimarães, datado de 29 de Março de 2011, proferido no processo n.º 735/10.0GAPTL-A.G1, e disponível em www.dgsi.pt. Em sentido idêntico se pronuncia PEDRO VERDELHO, "A nova Lei do Cibercrime", *Scientia Ivridica*, Tomo LVIII, n.º 320, p. 743-744.
[34] O que configurará nulidade, como se sustenta no Acórdão do TRL, datado de 6 de Março de 2018, proferido no processo n.º 1950/17.0T9LSB-A.L1-5 e disponível em www.dgsi.pt, embora tenhamos algumas dúvidas em reconduzir a situação ao art. 120.º, n.º 2, alínea d), do CPP.

correio electrónico, o que só poderá ser feito por quem tenha o domínio da investigação, e não por quem tenha participações fragmentárias na mesma, enquanto "juiz das liberdades".

3.5. Exames e perícias informáticas

É frequente observar na prática judiciária algum equívoco no respeitante às diferenças e âmbitos da pesquisa de dados informáticos, exames e perícias informáticas (surgindo até frequentemente uma quarta figura híbrida, apelidada de "exame pericial"). De forma sintética, e remetendo em parte para o que acima se disse quanto à pesquisa de dados informáticos diremos que[35]:

a) A perícia distingue-se do exame e da pesquisa de dados informáticos, por se traduzir num meio de prova, diferentemente dos demais que são meios de obtenção de prova. Tal significa que a perícia, enquanto juízo técnico, científico ou artístico sobre factos é elemento susceptível, por si só, de permitir elucidar a verdade histórica dos factos sob investigação, diferentemente das demais figuras, que constituem instrumentos para recolha de prova.

b) A pesquisa de dados informáticos e o exame, sendo ambos meios de obtenção de prova, diferenciam-se pela natureza coerciva do primeiro, evidenciada pelo regime legal previsto na Lei do Cibercrime e pela remissão para o regime das buscas, a qual não é partilhada pelo segundo, onde a eventual coerção de pessoa não colaborante surge como situação especial (art. 172.º do CPP)[36], bem como pela própria natureza das operações necessárias à efectivação de um e do outro, com o primeiro a circunscrever-se à já referida "busca em ambiente digital".

Tendo já anteriormente analisado a pesquisa de dados informáticos, importa agora passar aos exames e perícias que serão, tendencialmente, operações posteriores à injunção ou pesquisa de dados informáticos (que permitem obter esses dados) e à apreensão dos mesmos.

Os exames não dispõem de regime especial na LC (a qual, de resto e como se disse, não esgota a regulamentação dos meios de obtenção de prova em ambiente digital), sendo assim aplicável o regime geral constante do CPP, e previsto nos arts. 171.º a 173.º desse diploma, com a inerente competência do Ministério Público para determinação dos mesmos, nos termos aí previstos[37].

Trata-se de um meio de obtenção de prova traduzido na inspecção aos vestígios que o crime possa ter deixado e aos indícios relativos às circunstâncias em que o mesmo foi praticado (art. 171.º, n.º 1, do CPP). Estando em causa prova digital, os vestígios ou indícios em causa

[35] Acompanhamos aqui no essencial PEDRO VERDELHO, "Técnica no novo C.P.P.: Exames, Perícias e Prova Digital", *Revista do CEJ*, 1.º Semestre 2008, Número 9 (Especial), Jornadas sobre a revisão do CPP, pp. 145-171.
[36] Em sentido similar veja-se PEDRO VERDELHO, "A nova Lei do Cibercrime", pp. 740-741.
[37] No mesmo sentido, veja-se o Acórdão do TRE, datado de 7 de Abril de 2015, proferido no proc. n.º 13/15.8PAOLH-A e disponível em www.dgsi.pt.

corresponderão aos dispositivos electrónicos de processamento e armazenamento de dados informáticos, bem como aos dados informáticos propriamente ditos.

Ao nível dos procedimentos tendentes à efectivação do exame, são de salientar a adopção de quaisquer medidas que se mostrem necessárias à preservação dos vestígios ou indícios deixados pelo crime, designadamente a proibição de entrada ou trânsito de pessoas estranhas ao local (art. 171.º, n.º 2, do CPP), e também a procura de reconstituição do estado pré-existente dos indícios, quando sejam detectadas a adulteração ou desaparecimento dos mesmos (art. 171.º, n.º 3, do CPP).

Transplantando estes procedimentos para o âmbito digital, diremos que alguns procedimentos de preservação que tipicamente se verifiquem poderão traduzir-se na selagem dos dispositivos electrónicos encontrados, na manutenção dos mesmos no estado de ligados (para garantir que são preservados os dados da concreta sessão em que os mesmos se encontravam) ou na utilização de software apropriado para prevenir a adulteração dos dados em causa.

No respeitante à descoberta de indícios de adulteração ou desaparecimento de indícios do crime, parece-nos evidente que o desaparecimento dos dispositivos electrónicos propriamente ditos impossibilitará o trabalho de reconstituição da base indiciária pré-existente (excepto se os dados forem acessíveis por outra via, designadamente por se encontrarem *online*), pelo que só em caso de serem encontrados dados informáticos adulterados ou destruídos, se mostrará possível o recurso às ferramentas que permitam a sua reconstituição, como seja *software* de recuperação de ficheiros apagados ou de análise do código dos ficheiros adulterados.

A prática de actos urgentes por parte de qualquer agente da autoridade, prevista no art. 171.º, n.º 4, do CPP, deverá ser perspectivada com alguma cautela, uma vez que a já referenciada fragilidade e corruptibilidade dos dados informáticos obriga a um manuseamento cuidadoso, preferivelmente por quem tenha conhecimentos especializados na área. Diremos assim que estes actos deverão circunscrever-se ao mínimo de impedir que indivíduos acedam aos dispositivos electrónicos encontrados no local do crime.

Por fim, ao nível da sujeição a exame contra vontade do visado, apenas poderemos obviamente conjecturar situações de recusa em facultar coisa que deva ser examinada, designadamente os aparelhos onde se mostre possível o processamento ou armazenamento de dados informáticos e que sejam encontrados no local do crime. Nesse cenário, o regime previsto no art. 172.º, n.º 1, do CPP aplicar-se-á sem especificidades particulares, com a consequente possibilidade de compulsão do visado a providenciar a coisa para exame, através de decisão da autoridade judiciária. Quanto às especificidades previstas nos n.ºs 2 e 3 do art. 172.º do CPP, cremos que as mesmas são alheias às realidades digitais.

O resultado do exame será plasmado em relatório, o qual apresentará, no caso concreto da prova digital, a identificação do aparelho electrónico examinado, com indicação das suas características e especificações técnicas, a identificação dos ficheiros informáticos com relevo probatório que sejam aí encontrados e seu conteúdo, e a explicitação dos procedimentos

tendentes à realização desse exame, de modo a permitir que os sujeitos processuais possam conhecer os termos em que foi efectivado o exame e obtidos os correspondentes resultados.

Nesta sede, mostra-se igualmente importante a existência de um registo da cadeia de custódia, onde sejam indicados todos os acessos ao dispositivo electrónico objecto de exame, com identificação da data, hora, local e identidade do examinador. É importante que os sujeitos processuais saibam onde se encontrou o aparelho a cada momento, e se ocorreram eventos susceptíveis de fazer duvidar da fidedignidade e integridade dos dados que aí se encontrem.

No respeitante às perícias, não falamos aqui das diligências plasmadas nos chamados "relatórios de exame pericial", usualmente elaborados pelo Laboratório de Polícia Científica da PJ, os quais verdadeiramente se reconduzem a meros exames, não obstante a alusão a "pericial" e a circunstância de serem realizados por especialistas nas correspondentes áreas de conhecimentos. É importante relembrar que os exames podem igualmente ser realizados por pessoas dotadas de especiais conhecimentos técnicos, científicos ou artísticos, sem que por isso a correspondente diligência probatória se transmute em perícia.

A lei processual penal não contém uma definição de prova pericial, podendo contudo extrair-se a sua natureza do disposto nos arts. 151.º e 152.º do CPP: trata-se da percepção ou apreciação de factos por parte de pessoa ou equipa multidisciplinar, dotadas de especiais conhecimentos técnicos, científicos ou artísticos. Podemos dizer, sem correr grande risco de imprecisão, que se trata assim de um meio de prova indirecto, na acepção de que não assenta num conhecimento imediato dos factos com relevância probatória, correspondendo antes a uma análise especializada, da qual são extraídas conclusões.

O regime legal da prova pericial, previsto nos arts. 151.º e 163.º do CPP é aplicável também no âmbito digital, dado que a LC não contém quaisquer dispositivos reguladores deste meio de prova. Impõem-se contudo algumas precisões, derivadas das especificidades próprias da recolha e análise de prova em meio digital.

No respeitante à realização da perícia, o art. 152.º, n.ºs 1 e 2, do CPP aponta para a preferência por estabelecimento, laboratório ou serviço oficial apropriado, e como critérios subsidiários de escolha as listas oficiais de peritos existentes na comarca ou a indicação de pessoa idónea.

No caso das perícias informáticas, o Laboratório de Polícia Científica da PJ continua a ser a instituição de referência. Contudo, verifica-se desde há muito um certo estrangulamento desta instituição, em face do incremento exponencial de solicitações, desacompanhada do proporcional aumento de meios técnicos e humanos. Ciente disso, a Procuradoria-Geral da República celebrou protocolos com algumas instituições de Ensino Superior, tendo em vista a participação das mesmas na realização de perícias informáticas . A intenção é louvável, mas a utilização destes protocolos é ainda marginal , devendo por isso ser promovida, de modo a obstar aos atrasos tantas vezes verificados por força do já referido excesso de solicitações do LPC.

A perícia deverá ser ordenada por despacho da autoridade judiciária competente, com indicação do objecto da perícia, dos quesitos a serem respondidos e da entidade que deverá realizar a perícia (art. 154.º, n.º 1, do CPP), devendo ser transmitida a esta última toda a informação e elementos necessários para a efectivação da mesma (art. 154.º, n.º 2, do CPP). Cremos que a notificação do despacho a que aludem os n.ºs 4 e 5 do 154.º do CPP poucas vezes poderá ter lugar em sede de perícia informática, dada a facilidade com que o arguido poderá proceder à destruição ou adulteração de dados. Ao nível do procedimento para a realização da perícia, realização de relatório pericial, pedidos de esclarecimentos e nova perícia, previstos nos arts. 156.º a 158.º do CPP, não se vislumbram particulares especificidades no contexto digital.

O art. 161.º do CPP permite que possa ser autorizada a destruição, alteração ou comprometimento grave da integridade de qualquer objecto, para efectivação da perícia. Dada a virtualmente ilimitada capacidade de multiplicação de cópias dos dados informáticos, não vemos em que medida este dispositivo se poderá aplicar em sede de perícia informática. Pelo contrário: para assegurar a integridade e fidedignidade da prova digital recolhida, haverá que assegurar a existência permanente de uma cópia original e intocada (clonada), prevenindo assim adulterações frequentes aquando da análise da mesma.

Uma palavra, por fim, quanto ao valor da prova pericial, que se presume subtraída à livre apreciação do julgador e que obriga o mesmo a um especial esforço de fundamentação da discordância quanto às conclusões da mesma (art. 163.º, n.ºs 1 e 2, do CPP). A prática judiciária parece demonstrar uma certa tendência de seguidismo quase acrítico das conclusões dos peritos, o que acaba por produzir o efeito perverso de transmissão da decisão judicial para os ombros do perito. Cremos que a eventual falta de domínio de certas áreas de saber por parte do jurista não o desculpabiliza, nem o isenta, de realizar um esforço de compreensão dessas áreas e de saber interpretar e analisar criticamente o produto da análise pericial. Sem esse esforço, bastante mais fácil de encetar actualmente, dada a profusão ilimitada de fontes de consulta *online*, o jurista ficará desamparado na discussão da causa e demitir-se-á daquela que é sua função judiciária, além de, no caso do Magistrado do Ministério Público, não ser capaz de refutar as considerações expendidas por peritos ou consultores técnicos apresentados pela defesa[38].

[38] Parafraseando PEDRO VERDELHO, "Técnica no novo C.P.P.: Exames, Perícias e Prova Digital", *Revista do CEJ*, p. 146: "*Nas modernas perícias sobre crimes informáticos ou financeiros, por vezes, o técnico do direito só arduamente consegue apreender as conclusões, sendo ainda mais difícil descodificar as razões que levaram a elas. Os casos que manifestam estas circunstâncias impõem reflexão e colocam questões que têm que ser resolvidas, para evitar que o sistema seja subvertido, isto é, para que a verdadeira decisão deixe de ser tomada pelo Magistrado, para ser antecipada pelas conclusões do perito*".

4. Problemas de gestão processual

4.1. Orientações breves sobre gestão de inquérito e utilização processual da prova digital em fases posteriores

A indicação de critérios gerais de gestão processual é sempre uma tarefa difícil, dado que cada realidade processual é única e dotada de idiossincrasias, forçando a um constante esforço de adaptação e reponderação das práticas e quadros mentais pré-existentes.

Não obstante essa assumida dificuldade, muito do que foi dito nos capítulos antecedentes permite avançar com algumas (breves) orientações para a gestão processual, quando esteja em causa a obtenção e utilização de prova digital, sempre com vista à maximização das hipóteses de sucesso da investigação criminal e da obtenção de condenação em julgamento posterior.

Em sede de inquérito, diremos que a palavra de ordem é celeridade: como se viu, a prova digital caracteriza-se por uma certa fragilidade e corruptibilidade inerentes, propiciadoras da sua destruição pelos agentes do crime, a que se junta a existência de regimes legais que estabelecem prazos máximos para a conservação de determinados dados por parte de fornecedores de serviços.

Tudo isto implica que o titular do inquérito deva, logo no início da investigação, apurar a eventual existência de prova digital que deva ser obtida, quais as entidades que terão disponibilidade e controlo sobre a mesma e quais os prazos máximos de conservação (se aplicáveis ao caso). Quando conclua por essa existência, deverá imediatamente ordenar a apresentação ou concessão de acesso aos dados informáticos em causa ou ordenar a realização de pesquisa e apreensão de dados informáticos. Quando seja duvidosa a existência de prova digital ou os canais formais possam implicar a ultrapassagem de prazos máximos de conservação de dados, mandará a cautela que se ordene, quando seja caso disso, a preservação temporária de dados informáticos, o que permitirá abrir uma maior janela temporal de oportunidade para aceder aos mesmos[39].

Uma vez obtida a prova digital em sede de inquérito, haverá que proceder ao exame da mesma e, quando tal se imponha, à realização de perícia. Em ambos os casos, será necessário atribuir a realização dessas diligências a entidades dotadas de conhecimentos técnicos que permitam, não apenas extrair significado e conteúdo da prova digital já recolhida, mas também garantir que a mesma permaneça no estado original em que foi recolhida. Neste âmbito, entendemos pertinente começar a dar uso mais alargado aos protocolos existentes com instituições de Ensino Superior, de modo a descongestionar o Laboratório de Polícia Científica da PJ e a lograr obter períodos mais curtos de efectivação dessas diligências e, consequentemente, de encerramento do inquérito.

[39] Quando esteja em causa a obtenção de dados informáticos junto de operadores sedeados no estrangeiro, relativamente aos quais não existam protocolos ou acordos informais, o ponto de contacto 24/7 da Polícia Judiciária poderá constituir uma boa alternativa para assegurar uma preservação expedita.

O resultado destas diligências será sempre vertido em relatório, o qual deverá ser objecto de análise aprofundada por parte do titular do inquérito, que não se deverá limitar a aceitar acriticamente as asserções aí plasmadas. Tendo dúvidas quanto a determinados segmentos ou indicações constantes dos relatórios periciais ou de exames, o titular do inquérito deverá contactar directamente com o autor dos mesmos e solicitar todos os esclarecimentos pertinentes.

Impõe-se ainda ao titular do inquérito, um certo esforço de autodidactismo, assumindo uma postura proactiva de procura de conhecimentos técnicos que o habilitem, pelo menos, a uma compreensão rudimentar das matérias objecto de exame ou perícia. Passar um "cheque em branco" à entidade que assume a realização do exame ou da perícia corresponde a uma demissão do papel de direcção do inquérito que incumbe ao Ministério Público, abrindo a possibilidade da ocorrência de erros evitáveis em sede de investigação, que poderão pagar-se caro em julgamento.

Aquando da prolação do despacho de encerramento de inquérito, caberá ao titular do mesmo transformar a linguagem técnica desses relatórios, tantas vezes hermética ou de difícil compreensão pelo leigo, em linguagem escorreita e facilmente compreensível pelos destinatários. A tanto obrigam, não só os direitos de defesa do arguido, que deve perceber o que lhe é imputado, como também as probabilidades de sucesso de futuro julgamento e o exercício de escrutínio público da actividade investigatória pela comunidade. Um documento rico em conceitos técnicos não explicados perderá em compreensibilidade e abrirá caminho a interpretações ambíguas, favoráveis a estratégias de defesa enviesadas.

A eventual indicação como testemunha de quem realizou o exame ou a indicação do perito para prestação de esclarecimentos orais em audiência de julgamento, é uma faculdade que deverá ser ponderada nas situações em que os dados informáticos analisados sejam numerosos ou quando se coloquem questões técnicas de complexidade incomum. Nas demais, será talvez uma diligência desnecessária, sendo certo que o défice de meios humanos para realização dos exames e perícias informáticas obriga também a alguma parcimónia na sua indicação para serem ouvidos em julgamento.

No respeitante à fase de julgamento propriamente dita, as dificuldades que se colocam são, antes de mais, de natureza infra-estrutural. O défice e arcaísmo dos meios informáticos afectos aos tribunais é um obstáculo de vulto à cabal e ideal apresentação de prova digital, forçando a que os agentes judiciários se atenham frequentemente aos relatórios periciais ou de exame em suporte papel ou a uma utilização meramente superficial dos meios informáticos. A ultrapassagem deste problema depende, por um lado, de intervenção estadual e, por outro, do eventual uso de utilitários ou programas informáticos gratuitos, sempre no contexto do esforço de autodidactismo dos actores judiciários.

No demais atinente à fase de julgamento diremos que incumbirá ao Magistrado estar atento a eventuais dúvidas que sejam suscitadas sobre a fidedignidade da prova digital carreada para os autos, caso em que, dando uso à prerrogativa prevista no art. 340.º do CPP, deverá requerer a comparência em julgamento de quem obteve e manuseou a prova digital em causa. Na ulterior

realização de inquirição desses indivíduos, deverá procurar reconstituir-se a metodologia de obtenção da prova digital e todo o percurso subsequente de conservação e análise da mesma, tendo a preocupação de solicitar todas as explicações técnicas que se afigurem pertinentes a uma integral compreensão por parte do leigo.

4.2. Medidas anti-forenses e ferramentas forenses de uso livre

Falámos no subcapítulo antecedente de proactividade e autodidactismo como posturas a adoptar pelo titular de inquérito ou do Magistrado que assegure o julgamento, tendo em vista a obtenção de resultados positivos nessas fases. Isto serve-nos para introduzir algumas breves considerações sobre realidades que cremos deverem ser, ainda que em termos básicos, conhecidas dos Magistrados: as medidas anti-forenses e as ferramentas forenses de uso livre.
No que respeita ao que a doutrina norte-americana convencionou chamar de medidas anti-forenses, trata-se de um conceito abrangente, que inclui todos os métodos utilizados por agentes do crime para impedir ou obstaculizar a eventual investigação criminal dos ilícitos praticados pelos mesmos, aquando da prática do crime ou posteriormente, inutilizando a prova digital existente ou inviabilizando a sua análise por parte das autoridades estaduais. Dada a multiplicidade destes instrumentos e a economia do presente trabalho, faremos apenas breves referências a instrumentos que actuam ao nível da anonimização dos agentes do crime e da inutilização de prova digital[40].

A utilização de meios informáticos deixa sempre um rasto digital, a maior parte das vezes imperceptível para o utilizador, mas susceptível de recuperação e análise por especialistas forenses. A dificuldade de apagamento desse rasto é ampliada quando o utilizador se encontra em ambiente de rede, caso em que, além do rasto digital que quedará na máquina de que o mesmo se serve, existirá ainda um outro rasto, preservado pelos fornecedores de serviços de Internet. Daí que, na prática de ilícitos através de meios informáticos através da rede, tenha desde cedo existido a procura e desenvolvimento de meios de tornar anónima a actuação do utilizador, prevenindo a geração de rasto digital.

Entre os meios mais rudimentares de anonimização da actuação do agente do crime poderemos contar comportamentos tão simples como a criação de endereços de correio electrónico com dados diferentes dos pertencentes ao agente do crime, a utilização de pseudónimos ou a efectivação de acesso à Internet através de redes *Wi-fi* abertas ao público ou de equipamentos disponibilizados em instituições públicas, como é o caso de bibliotecas universitárias. A rudimentaridade destes métodos naturalmente não augura grandes probabilidades de sucesso aos agentes do crime.

Quanto aos meios mais complexos de anonimização, poderemos incluir os programas informáticos que permitem ocultar ou dissimular o endereço IP utilizado para aceder à Internet, os navegadores de Internet que permitem uma navegação inteiramente anónima (como o caso do conhecido navegador Tor) ou as moedas digitais que circulam sem a

[40] Na exposição subsequente, seguiremos de perto DAVID SILVA RAMALHO, *Métodos Ocultos de Investigação Criminal em Ambiente Digital*, pp. 147-175, onde a matéria se encontra analisada com maior detalhe.

existência de uma autoridade central e que são de uso corrente no branqueamento de capitais[41] (como a Bitcoin[42]). A sofisticação de alguns destes instrumentos tem constituído um óbice praticamente inultrapassável às investigações criminais, mesmo em países dotados de meios mais avançados e de maior dotação orçamental para o combate ao crime.

Quando não seja possível ao agente do crime prevenir o rasto digital, ou quando o mesmo necessite de manter em permanência dados informáticos para o desenvolvimento da sua actividade delituosa, existem vários programas informáticos de fácil obtenção, que permitem assegurar a obliteração definitiva desses dados (inviabilizando o uso de ferramentas forenses para a sua recuperação), a encriptação irreversível dos dados (impossibilitando o acesso aos mesmos por quem não tenha a chave correspondente), a dissimulação dos dados (tornando-os imperceptíveis aos olhos dos investigadores) ou a adulteração dos dados (alterando a configuração original dos mesmos e tornando-os inúteis para efeitos investigatórios).

Dada a constante mutação destes e de outros instrumentos, impõe-se uma especial atenção às entidades incumbidas da prevenção e repressão do fenómeno criminoso, sendo certo que existe amplíssima informação disponível *online*, com explicitações adequadas à compreensão do leigo.

Como espelho e contraposição a estas medidas anti-forenses, existem igualmente inúmeras ferramentas e programas informáticos com interesse e utilidade forense, muitos dos quais disponíveis gratuitamente ou *online*, e cujo manuseamento não exige mais do que conhecimentos informáticos rudimentares, podendo assim ser usadas por Magistrados, desde que o seu uso fique documentado nos autos.

Ainda quando não seja dado uso às mesmas, é importante que o Magistrado conheça, pelo menos, a existência de algumas destas ferramentas[43], como sejam as atinentes:

(i) À obtenção de dados relativos a endereços IP (como os websites http://dnstools.com/ e https://www.whatismyip.com/);

(ii) À obtenção de cabeçalhos de mensagens de correio electrónico[44];

(iii) À recuperação de ficheiros apagados (v.g. *Recuva*);

(iv) À captura forense de páginas *web* (v.g. *FAW – Forensics Acquisition of Websites*);

[41] Para uma melhor compreensão do que são estas moedas digitais e qual a sua repercussão ao nível das investigações criminais, dada a facilidade de uso das mesmas para efectivação de branqueamento de capitais veja-se *Virtual Currencies – The basic guide for financial investigators*, guia elaborado pela Europol e disponível no SIMP.
[42] O texto-base sobre a Bitcoin, explicando os termos básicos do seu funcionamento continua a ser *Bitcoin: a Peer-to-Peer Electronic Cash System*, de Satoshi Nakamoto (cuja verdadeira identidade permanece desconhecida), disponível em https://bitcoin.org/bitcoin.pdf.
[43] Uma listagem mais exaustiva de software forense gratuito poderá ser encontrada em https://forensiccontrol.com/resources/free-software/, de onde se retirou a maioria das ferramentas mencionadas.
[44] Para melhor compreensão do modo de extracção destes cabeçalhos e da sua leitura, vejam-se o *Manual de Recolha de Cabeçalhos Técnicos de Mensagens de Correio Electrónico*, elaborado pelo Núcleo de Polícia Técnica Forense da PSP, e o *Guia de recolha de cabeçalhos técnicos de mensagens de correio electrónico*, elaborado pela Polícia Judiciária, ambos disponíveis em SIMP.

(v) À cópia forense de ficheiros (v.g. *Nuix Evidence Mover*);

(vi) À identificação de formatos de ficheiros através da análise da sua assinatura (v.g. *Hexbrowser*);

(vii) À procura de ficheiros encriptados ou protegidos por *password* e à análise das possibilidades de desencriptação dos mesmos (v.g. *Encryption Analyzer*);

(viii) À análise forense de fotografias ou imagens digitais (v.g. *Forensic Image Viewer*);

(ix) À análise forense da estrutura interna de dispositivos móveis de comunicações (v.g. *Iphone Analyzer, ivMeta* ou *SAFT*);

(x) À extracção e visualização do histórico de *browser* e de *passwords* guardadas (v.g. *Browser History Capturer, Browser History Viewer* e *PasswordFox*);

(xi) À extracção de informação pública relativa ao Facebook, WhatsApp, Dropbox e Skype (v.g. *Facebook Profile Saver, WhatsApp Forensics, Dropbox Decryptor* e *SkypeLogView*); e

(xii) À extracção de informação quanto aos dispositivos USB que se ligaram a determinado computador (v.g. *USDeview*).

5. Conclusões

Todos os actores judiciários que se movam no palco do processo penal são hoje inevitavelmente confrontados com as realidades digitais, quer seja pela crescente expressão da cibercriminalidade, quer seja pela ubiquidade dos dados informáticos enquanto material com interesse probatório.

A eficaz prevenção e repressão de fenómenos delituosos depende de um conhecimento mínimo do modo como os mesmos se desenrolam: o combate à actividade de tráfico de estupefacientes depende de um conhecimento das origens dos produtos, da infra-estrutura necessária à sua transformação e da logística que permite fazer chegar o produto acabado aos consumidores. Do mesmo modo, o combate à cibercriminalidade depende de um conhecimento das potencialidades da máquina para a sua efectivação, dos nódulos problemáticos para a investigação, como sejam os instrumentos de anonimização ou encriptação, e das enormes potencialidades probatórias que um insuspeito disco rígido poderá conter.

Tornou-se já um lugar-comum dizer-se que as leis que temos em matéria de cibercriminalidade e prova digital são insuficientes e plenas de deficiências, uma crítica que é decerto justa, mas que não ajuda a resolver os problemas imediatos, os quais não podem aguardar pela morosidade de um processo de revisão legislativa, que de resto tarda em surgir.

No aqui e agora impõe-se procurar maximizar as potencialidades das referidas leis, as quais cremos propiciarem um leque relativamente alargado de instrumentos probatórios, e sem nunca esquecer que a atipicidade de dado meio probatório não comporta necessariamente a sua impossibilidade de utilização em processo penal.

A fragilidade dos dados informáticos impõe uma actuação célere e assertiva dos titulares dos inquéritos, antevendo onde possam encontrar-se dados informáticos com relevo probatório e fazendo uso das medidas cautelares e meios de obtenção de prova disponíveis para efectivação da sua recolha e apreensão. E impõe igualmente uma actuação cuidada sobre os mesmos, em sede de pesquisa, exame e perícia, de modo a obstar que a actividade investigatória venha a contaminar esses dados, tornando-os probatoriamente inidóneos.

O aparente hermetismo da linguagem técnica utilizada, profusa em vocábulos anglófonos de uso pouco corrente, e a própria dificuldade de apreensão de alguns conceitos, que se apresentam como contra-intuitivos ou sem qualquer familiaridade, são obstáculos de vulto. A sua ultrapassagem apenas poderá ser efectivada através de um esforço de aprendizagem por parte dos actores judiciários, fazendo uso das muitas fontes abertas que existem na Internet (sendo conveniente o domínio da língua inglesa) e interpelando directamente os examinadores ou peritos informáticos, colocando as questões que se imponham – quem investiga e apresenta uma causa em Tribunal deverá ser capaz de a compreender e a explicar de forma perceptível para os leigos.

Pretendemos, contudo, encerrar o presente trabalho com uma nota de optimismo, salientando diversos sinais positivos e no caminho certo, como seja o trabalho desenvolvido pelo Gabinete Cibercrime, avultando já na correspondente secção do SIMP um manancial considerável e variado de materiais de estudo, a crescente profusão de ferramentas forenses gratuitas e o surgimento de algumas iniciativas e projectos de informatização judiciária, de que destacamos o SIIP – Sistema Integrado de Informação Processual[45].

[45] Sobre esta ferramenta informática, desenvolvida conjuntamente por um Magistrado Judicial e dois elementos de OPC, e pensada sobretudo para os processos de maior dimensão, veja-se http://visao.sapo.pt/actualidade/portugal/2017-08-19-Estes-homens-estao-a-acelerar-a-Justica--e-chovem-elogios- e http://www.justicacoma.com/public/scaffold_edicoes/7edi%C3%A7%C3%A3o.pdf.

6. Referências bibliográficas

- CALLEJA, Álvaro Manuel Monge, "A Investigação criminal face à Globalização e o Cibercrime", Investigação Criminal, n.º 11, ASFICPJ, Fevereiro de 2017, pp. 170-187.

- CASEY, Eoghan, *Handbook of Digital Forensics and Investigation*, Elsevier Academic Press, 2009.

- CONDE CORREIA, João, "Prova digital: as leis que temos e a lei que devíamos ter", *Revista do Ministério Público*, n.º 139, Ano 35, Sindicato dos Magistrados do Ministério Público, pp. 29-59.

- CONSELHO DA EUROPA, *Electronic Evidence Guide*, de 3 de Fevereiro de 2013. [Retirado de https://www.coe.int/en/web/cybercrime/home].

- MARQUES DA SILVA, Germano, *Curso de Processo Penal, Volume II*, Editorial Verbo, 2002.

- MESQUITA, Paulo Dá, "Prolegómeno Sobre Prova Electrónica e Intercepção de Telecomunicações no Direito Processual Penal Português – O Código e a Lei do Cibercrime", *Processo Penal, Prova e Sistema Judiciário*, Coimbra Editora, 2010, pp. 83-129.

- RAMALHO, David Silva, "A Investigação Criminal na Dark Web", *Revista de Concorrência & Regulação*, Ano 4, n.º 16, Outubro-Dezembro de 2013, Almedina, pp. 195-243.

- ------, "O Uso de Malware como Meio de Obtenção de Prova em Processo Penal, *Revista de Concorrência & Regulação*, Ano 4, n.º 14/15, Abril/Setembro de 2013, Almedina, pp. 385-431.

- ------, "A Recolha de Prova Penal em Sistemas de Computação em Nuvem, *Revista de Direito Intelectual*, n.º 2, Almedina, 2014.

- ------, *Métodos Ocultos de Investigação Criminal em Ambiente Digital*, Almedina, 2017.

- SAMMONS, John, *The Basics of Digital Forensics – The Primer for Getting Started in Digital Forensics*, Syngress, 2012.

- VERDELHO, Pedro, "Cibercrime", *Direito da Sociedade da Informação – Volume IV*, Coimbra Editora, 2004, pp. 347-383.

- ------, "Cibercrime e Segurança Informática", *Polícia e Justiça – Revista do Instituto Superior de Polícia Judiciária e Ciências Criminais*, III Série, n.º 6, Julho-Dezembro 2005, pp. 159-175.

- ------, "A Convenção sobre Cibercrime do Conselho da Europa – Repercussões na Lei Portuguesa", *Direito da Sociedade da Informação – Volume VI*, Coimbra Editora 2006, pp. 257-276.

– ------, "Técnica no novo C.P.P.: Exames, Perícias e Prova Digital", *Revista do CEJ*, 1.º Semestre 2008, Número 9 (Especial), Jornadas sobre a revisão do CPP, pp. 145-171.
–
– ------, "A nova Lei do Cibercrime", *Scientia Ivridica*, Tomo LVIII, n.º 320 – Outubro/Dezembro de 2009, Universidade do Minho.

CENTRO
DE ESTUDOS
JUDICIÁRIOS

6.

Medidas cautelares e de polícia. Enquadramento jurídico, prática e gestão processual

Sílvia Catarina Pais Silva

CENTRO
DE ESTUDOS
JUDICIÁRIOS

6. MEDIDAS CAUTELARES E DE POLÍCIA. ENQUADRAMENTO JURÍDICO, PRÁTICA E GESTÃO PROCESSUAL

Sílvia Catarina Pais Silva*

I. Introdução

O presente trabalho reporta-se às situações em que os órgãos de polícia criminal têm necessidade de agir, em termos processuais penais, antes da intervenção das autoridades judiciárias, ou mesmo após a intervenção destas sempre que esteja em causa assegurar novos meios de prova.

São estas situações que o Código de Processo Penal vem regular através das denominadas "medidas cautelares e de polícia".

*Agradecimentos
Pelos contributos dados para o desenvolvimento da presente obra, um especial agradecimento ao Dr. Luís Carlos Pereira Lopes, Procurador-Adjunto, a exercer funções na seção distrital do Departamento de Investigação e Ação Penal de Évora.

Trata-se de garantir uma competência que possibilita aos órgãos de polícia criminal uma intervenção de caráter garantístico e por isso excecional, porquanto, em princípio, atuariam por encargo de autoridade judiciária.

As medidas cautelares e de polícia devem ser comunicadas à autoridade judiciária competente, no mais curto espaço de tempo possível e sempre em conformidade com os limites temporais estabelecidos na lei, daí resultando a sua provisoriedade.

As medidas cautelares distinguem-se das medidas de polícia, estas são os atos da competência própria das polícias, expressamente previstos na lei, que revestem caráter preventivo, na medida em que visam atuar sobre um perigo para prevenir a lesão de um bem jurídico, permitem restringir, na medida do estritamente necessário, direitos fundamentais do cidadão para garantir a defesa de outros direitos de igual valor.

II. Objetivos

O presente guia tem como destinatários aqueles que pretendam compreender o regime jurídico das medidas cautelares, previsto no Código de Processo Penal e em legislação extravagante.

Quanto às medidas de polícia propomo-nos efetuar uma breve referência às mesmas, definindo o seu objeto e procedendo à sua identificação.

O objetivo principal deste estudo foi analisar os diversos tipos de medidas cautelares, previstos no Código de Processo Penal e em alguma legislação avulsa, e refletir sobre as principais questões jurídicas que se levantam relativamente a cada uma delas, sob uma perspetiva prática e, nesta medida, referenciando jurisprudência à medida que forem sendo abordados os diversos conteúdos.

Num segundo momento visa-se consciencializar para as boas práticas de gestão processual, espelhada na forma de articulação entre os órgãos de polícia criminal e as autoridades judiciárias, sublinhando o papel de direção do inquérito que cabe ao Ministério Público, a necessidade de permanente circulação de informação entre Ministério Público e órgãos de polícia criminal e de cumprimento dos prazos estabelecidos na lei.

III. Resumo

Efetuaremos a análise de cada uma das medidas cautelares previstas no Código de Processo Penal, abordando ainda situações contempladas em legislação extravagante, procurando referir as principais questões jurídicas que se têm verificado na prática para cada medida cautelar e a forma como os nossos tribunais superiores as têm resolvido, a fim de conferir uma dinâmica prática ao presente documento.

No final faremos uma referência sobre as questões que se colocam a nível de gestão e prática processual e formas de abordagem desta problemática.

1. Medidas Cautelares e de Polícia – Enquadramento jurídico

1.1. Medidas de polícia

As medidas de polícia são os atos da competência própria das polícias, de caráter preventivo, que visam atuar sobre um perigo para prevenir a lesão de um bem jurídico e que permitem restringir, na medida do estritamente necessário, direitos fundamentais do cidadão para garantir a defesa de outros direitos de igual valor.

Marcelo Caetano define as medidas de polícia como "providências limitativas da liberdade de certa pessoa ou de direito de propriedade de determinada entidade, aplicadas pelas autoridades administrativas independentemente da verificação e julgamento de transgressão ou de contravenção ou da produção que outro ato concretamente delituoso com o fim de evitar a produção de danos sociais, cuja prevenção caiba no âmbito das atribuições da polícia".[1]

O n.º 2 do artigo 272.º da Constituição da República Portuguesa, sob a epígrafe "Polícia", estabelece que: "(…) 2. As medidas de polícia são as previstas na lei, não devendo ser utilizadas para além do estritamente necessário."

Do exposto assinalamos uma diferença entre as medidas de polícia e as medidas cautelares, uma vez que as primeiras são taxativas (apenas são permitidas as previstas na lei), e as segundas são admissíveis desde que não sejam proibidas por lei (em conformidade com princípio da legalidade da prova previsto no artigo 125.º do Código de Processo Penal), sendo este o sentido do advérbio "nomeadamente", incluso no n.º 2 do artigo 249.º do Código de Processo Penal.

A Lei de Segurança Interna (LSI) – Lei n.º 53/2008, de 29 de Agosto, que tem por objeto a atividade desenvolvida pelo Estado para garantir a ordem, a segurança e a tranquilidade públicas, proteger pessoas e bens, prevenir e reprimir a criminalidade e contribuir para assegurar o normal funcionamento das instituições democráticas, o regular exercício dos direitos, liberdades e garantias fundamentais dos cidadãos e o respeito pela legalidade democrática (cfr. artigo 1.º do referido diploma legal), estabelece nos artigos 28.º e 29.º as medidas de polícia[2].

[1] Caetano, Marcelo, Manual de Direito Administrativo, 3.ª reimpressão da 10.ª edição, Almedina, Coimbra, volume 2, p. 1170.

[2] Artigo 28.º (Medidas de polícia)
1 - São medidas de polícia:
a) A identificação de pessoas suspeitas que se encontrem ou circulem em lugar público, aberto ao público ou sujeito a vigilância policial;
b) A interdição temporária de acesso e circulação de pessoas e meios de transporte a local, via terrestre, fluvial, marítima ou aérea;
c) A evacuação ou abandono temporários de locais ou meios de transporte.

Os artigos 30.º a 34.º da LSI[3] estabelecem os princípios orientadores da aplicação das medidas previstas nos artigos 28.º e 29.º e os procedimentos a que a aplicação das mesmas se encontra sujeita.

---

2 - Considera-se também medida de polícia a remoção de objectos, veículos ou outros obstáculos colocados em locais públicos sem autorização que impeçam ou condicionem a passagem para garantir a liberdade de circulação em condições de segurança.
Artigo 29.º (São medidas especiais de polícia):
a) A realização, em viatura, lugar público, aberto ao público ou sujeito a vigilância policial, de buscas e revistas para detectar a presença de armas, substâncias ou engenhos explosivos ou pirotécnicos, objectos proibidos ou susceptíveis de possibilitar actos de violência e pessoas procuradas ou em situação irregular no território nacional ou privadas da sua liberdade;
b) A apreensão temporária de armas, munições, explosivos e substâncias ou objectos proibidos, perigosos ou sujeitos a licenciamento administrativo prévio;
c) A realização de acções de fiscalização em estabelecimentos e outros locais públicos ou abertos ao público;
d) As acções de vistoria ou instalação de equipamentos de segurança;
e) O encerramento temporário de paióis, depósitos ou fábricas de armamento ou explosivos e respectivos componentes;
f) A revogação ou suspensão de autorizações aos titulares dos estabelecimentos referidos na alínea anterior;
g) O encerramento temporário de estabelecimentos destinados à venda de armas ou explosivos;
h) A cessação da actividade de empresas, grupos, organizações ou associações que se dediquem ao terrorismo ou à criminalidade violenta ou altamente organizada;
i) A inibição da difusão a partir de sistemas de radiocomunicações, públicos ou privados, e o isolamento electromagnético ou o barramento do serviço telefónico em determinados espaços.
[3] Artigo 30.º (Princípio da necessidade)
Com excepção do caso previsto no n.º 2 do artigo 28.º, as medidas de polícia só são aplicáveis nos termos e condições previstos na Constituição e na lei, sempre que tal se revele necessário, pelo período de tempo estritamente indispensável para garantir a segurança e a protecção de pessoas e bens e desde que haja indícios fundados de preparação de actividade criminosa ou de perturbação séria ou violenta da ordem pública.
Artigo 31.º (Dever de identificação)
Os agentes e funcionários de polícia não uniformizados que, nos termos da lei, aplicarem medida de polícia ou emitirem qualquer ordem ou mandado legítimo devem previamente exibir prova da sua qualidade.
Artigo 32.º (Competência para determinar a aplicação)
1 - No desenvolvimento da sua actividade de segurança interna, as autoridades de polícia podem determinar a aplicação de medidas de polícia, no âmbito das respectivas competências.
2 - Em casos de urgência e de perigo na demora, a aplicação das medidas de polícia previstas no artigo 28.º e nas alíneas a) e b) do artigo 29.º pode ser determinada por agentes das forças e dos serviços de segurança, devendo nesse caso ser imediatamente comunicada à autoridade de polícia competente em ordem à sua confirmação.
3 - Salvo em casos de urgência e de perigo na demora, a aplicação das medidas de polícia previstas nas alíneas e) a h) do artigo 29.º é previamente autorizada pelo juiz de instrução do local onde a medida de polícia virá a ser aplicada.
Artigo 33.º (Comunicação ao tribunal)
1 - A aplicação das medidas previstas no artigo 29.º é, sob pena de nulidade, comunicada ao tribunal competente no mais curto prazo, que não pode exceder quarenta e oito horas, e apreciada pelo juiz em ordem à sua validação no prazo máximo de oito dias.
2 - Não é aplicável o disposto no número anterior no caso de a aplicação da medida de polícia ter sido previamente autorizada nos termos do n.º 3 do artigo anterior.
3 - Para efeitos do disposto no n.º 1 é competente o juiz de instrução do local onde a medida de polícia tiver sido aplicada.
4 - Não podem ser utilizadas em processo penal as provas recolhidas no âmbito de medidas especiais de polícia que não tiverem sido objecto de autorização prévia ou validação.
Artigo 34.º (Meios coercivos)
1 - Os agentes das forças e dos serviços de segurança só podem utilizar meios coercivos nos seguintes casos:
a) Para repelir uma agressão actual e ilícita de interesses juridicamente protegidos, em defesa própria ou de terceiros;
b) Para vencer resistência à execução de um serviço no exercício das suas funções, depois de ter feito aos resistentes intimação formal de obediência e esgotados os outros meios para o conseguir.
2 - O recurso à utilização de armas de fogo e explosivos pelas forças e pelos serviços de segurança é regulado em diploma próprio.

Além das medidas de polícia enumeradas na LSI, existem outras que se encontram contempladas em legislação avulsa, sendo exemplo disso:

– A Lei n.º 39/2009, de 30 de julho – regime jurídico do combate à violência, ao racismo, à xenofobia e à intolerância nos espetáculos desportivos -, prevê no artigo 25.º, a possibilidade de as forças de segurança, bem assim como os assistentes de recinto desportivo, poderem proceder, sempre que tal se mostre necessário, a revistas aos espetadores, por forma a evitar a existência no recinto de objetos ou substâncias proibidos ou suscetíveis de possibilitar atos de violência.

– A Lei n.º 5/2006, de 23 de fevereiro – Lei das Armas - no artigo 109.º prevê-se a possibilidade de, no âmbito de operações especiais de prevenção criminal, se poderem realizar, em função da necessidade, a identificação das pessoas que se encontrem na área geográfica onde têm lugar, bem como a revista de pessoas, e a busca de viaturas ou de equipamentos e, quando haja indícios da prática dos crimes previstos no n.º 1, risco de resistência ou de desobediência à autoridade pública ou ainda a necessidade de condução ao posto policial, por não ser possível a identificação suficiente, a realização de buscas no local onde se encontrem.

1.2. Medidas Cautelares e de Polícia (previstas no Código de Processo Penal e em legislação avulsa)

1.2.1. A notícia do crime

O capítulo do Código de Processo Penal destinado às medidas cautelares (capítulo II, do título I do livro VI), inicia-se com a notícia do crime, consagrada no artigo 248.º do referido diploma legal, que não é, em si mesma, uma medida cautelar porquanto, reporta-se ao modo como o Ministério Público tem conhecimento da prática de determinado ilícito criminal. Este conhecimento pode advir por modo próprio, por intermédio dos órgãos de polícia criminal ou mediante denúncia – cfr. artigo 241.º do Código de Processo Penal, dando origem à abertura de inquérito (artigo 262.º, n.º 2 do Código de Processo Penal), ressalvando os casos em que o Código de Processo Penal exige para essa abertura a manifestação da vontade de alguém (artigos 48.º e 49.º do mesmo diploma).

A notícia do crime dá lugar ao levantamento do auto de notícia (artigo 243.º do Código de Processo Penal) e importa ainda considerar a notícia do crime quanto a outras matérias como na detenção do suspeito (artigo 254.º e seguintes do Código de Processo Penal); na forma de processo aplicável; na necessidade de obtenção de queixa do ofendido (artigo 49.º, n.º 1, do Código de Processo Penal e 113.º, n.º 1, do Código Penal) para manutenção da detenção (artigo 255.º, n.º 3, do Código de Processo Penal) e confere, ainda, aos órgãos de polícia criminal a possibilidade de, após a notícia de todos os factos juridicamente relevantes, procederem a todo o conjunto de atos tendentes à obtenção e conservação dos meios de prova – cfr. artigo 249.º e seguintes do Código de Processo Penal.

a) Atuação por iniciativa própria do órgão de polícia criminal

A iniciativa própria dos órgãos de polícia criminal surge na sequência da notícia do crime (cfr. artigo 55.º, n.º 2, do Código de Processo Penal), isto é, a partir do momento em que o órgão de polícia criminal tenha conhecimento da ocorrência deve, ainda antes de comunicar à autoridade judiciária competente, realizar as diligências necessárias, proceder à aplicação de medidas cautelares e de polícia, atendendo sempre aos pressupostos de necessidade e urgência.

Nesta medida, deve ser respeitado o princípio da proporcionalidade, de modo a que não sejam causados aos cidadãos danos mais graves do que os estritamente necessários e indispensáveis para a prossecução dos fins da aplicação dessas medidas.

Segundo Paulo Dá Mesquita, a iniciativa própria dos OPC deve conformar-se com dois vetores principais: "por um lado, devem os actos cautelares e de polícia integrar as finalidades do processo penal, existindo uma substituição precária da autoridade judiciária por parte dos OPC e, por outro lado, os mesmos estão sujeitos aos pressupostos de necessidade e urgência, justificando-se assim a sua actuação sem prévio encargo por parte da autoridade judiciária, o que justificadamente só deverá ocorrer mediante "rigorosos pressupostos legais."

"Assim, todos os actos de investigação por iniciativa própria dos OPC que não se enquadrem no âmbito das medidas cautelares e de polícia que forem praticados antes de comunicada a notícia do crime ao MP ou, depois, mas que extravasem ou não se coadunem com o despacho de delegação de competências do MP, são ilegais, sendo inadmissível a posterior validação dos mesmos por parte do MP." [4]

b) A comunicação da notícia do crime

Colhida a notícia do crime, seja por conhecimento próprio ou mediante denúncia, ainda que infundada, sobrevém a obrigatoriedade legal, por parte dos órgão de polícia criminal de a transmitir ao Ministério Público no mais curto prazo possível, que não pode exceder 10 dias – cfr. artigo 248.º, n.º 1, do Código de Processo Penal.

A transmissão pode ser efetuada por qualquer meio para o efeito disponível e a comunicação oral deve ser seguida de comunicação escrita – artigos 242.º e 248.º, n.º 3, do Código de Processo Penal.

Sempre que uma autoridade judiciária, um órgão de polícia criminal ou outra entidade policial presenciarem um crime de denúncia obrigatória, devem lavrar auto de notícia circunstanciado – artigo 243.º, n.º 1, do Código de Processo Penal.

A comunicação da notícia de um crime no prazo legalmente previsto, deve conter, na medida do possível, todos os elementos que permitam a sua tipificação legal, a qual é fundamental

[4] Mesquita, Paulo Dá, *Repressão Criminal e Iniciativa Própria dos Órgãos de Polícia Criminal, in* Revista do Ministério Público, Lisboa, A.25 (98), Abr-Jun., 2004, p. 11.

para determinar o órgão de polícia criminal com competência legal e material para a sua investigação, de acordo com os critérios fixados na Lei n.º 49/2008, de 27 de agosto - Lei de Organização da Investigação Criminal (LOIC).[5]

Acresce que, nos termos do disposto no artigo 2.º, n.º 3, da LOIC, e da Diretiva n.º 1/2002, de 4 de abril[6], que contém os despachos de delegação genérica nos órgãos de polícia criminal, a que se refere o artigo 270.º, n.º 4, do Código de Processo Penal, os órgãos de polícia criminal devem iniciar de imediato a investigação e, em todos os casos, praticar os actos cautelares necessários e urgentes para assegurar os meios de prova.[7]
Paulo Pinto de Albuquerque entende que o prazo de 10 dias para comunicação da notícia do crime ao Ministério Público "não é consentâneo com a CRP nem com outros prazos estabelecidos pelo próprio CPP", e que nesse período de tempo os órgãos de polícia criminal atuam numa "intolerável (…) zona de semi-clandestinidade".[8]

Ainda quanto à comunicação da notícia do crime no prazo de 10 dias ao Ministério Público e da legitimidade do órgão de polícia criminal para realização de diligências de inquérito, nesse prazo, pronunciou-se o acórdão do Tribunal da Relação de Évora de 16.02.2016, relator João Gomes de Sousa, disponível *in* www.dgsi.pt.

Nesse acórdão esteve em discussão, nomeadamente, uma situação em que a Polícia Judiciária (PJ) entre o dia 11 de julho, data em que teve conhecimento através das entidades policiais inglesa e espanhola da chegada, ao aeroporto de Faro de um indivíduo referenciado com a

[5] Note-se as dificuldades que surgem inicialmente, por vezes, em qualificar um evento como, por exemplo: um crime de homicídio doloso ou negligente, sendo que esta qualificação é importante para efeitos de determinação do órgão de polícia criminal competente para realização da investigação, nos termos do artigo 7.º, n.º 2, alínea a) do LOIC.
[6] Circular n.º 6/2002 da Procuradoria-Geral da República (PGR), de 11 de março.
[7] A este propósito já se pronunciou o Conselho Consultivo da PGR, cujo Parecer n.º 45/2012, disponível *in* http://www.dgsi.pt, determina o seguinte:
1.ª O Ministério Público é a entidade competente para a direção do inquérito e para a seleção dos atos dirigidos aos respetivos fins: investigar a existência de um crime, determinar os seus agentes e a responsabilidade deles, e descobrir e recolher as provas em ordem à decisão sobre o exercício da ação penal.
2.ª Os órgãos de polícia criminal podem realizar atividades dirigidas aos fins do processo penal: a) Ao abrigo direto da lei, no caso de medidas cautelares e de polícia (sempre dependentes dos pressupostos urgência e perigo na demora); ou b) Por encargo do Ministério Público (caso em que é necessária a cobertura de um despacho de delegação de competência).
3.ª Os órgãos de polícia criminal apenas podem praticar atos de investigação criminal ao abrigo de despacho de delegação de competência depois da comunicação da notícia do crime ao Ministério Público, de acordo com os termos estabelecidos no despacho e no respeito das competências reservadas do juiz e do Ministério Público.
4.ª Na impossibilidade de comunicação com o Ministério Público competente, o órgão de polícia criminal pode contactar qualquer magistrado ou agente do Ministério Público e este pode determinar os atos urgentes de aquisição e conservação de meios de prova que considerar pertinentes ao abrigo do disposto no artigo 264.º, n.º 4, do CPP.
5.ª A prática de atos relativos aos fins do inquérito por iniciativa própria do órgão de polícia criminal depende sempre da verificação dos pressupostos de necessidade e urgência.
6.ª As autoridades e os órgãos de polícia criminal da PSP e da GNR, por iniciativa própria que vise a prossecução de fins do processo penal, podem:
a) Quanto a matérias que não integrem a reserva judiciária legal, praticar todos os atos cautelares necessários e urgentes para assegurar os meios de prova que não atinjam direitos protegidos por lei (artigo 249.º, n.º 1, do CPP);
b) Relativamente a matérias previstas nas reservas de competência das autoridades judiciárias, realizar os atos permitidos por previsão legal especial dentro dos estritos pressupostos jurídico-normativos estabelecidos pela lei.
[8] Albuquerque, Paulo Pinto de, *in* Código de Processo Penal anotado, 2010, Universidade Católica Editora, p. 671, pontos 2. e 5..

prática de um crime de tráfico de estupefacientes, e o dia 15 de julho, data em que comunicou ao Ministério Público a notícia do crime, realizou diversas diligências (designadamente vigilâncias), o que os recorrentes entenderam como atos de investigação e não medidas cautelares e que a informação recebida no dia 11 de julho pela PJ tratou-se de uma denúncia de um crime, e, nessa medida, deveria ter sido comunicada de imediato ao MP.

O Tribunal da Relação de Évora entendeu que a informação policial recebida pela polícia portuguesa não é uma "denúncia", mas uma informação policial que necessita de ser confirmada e que o artigo 248.º, n.º 1, do Código de Processo Penal permite – no prazo ali indicado (10 dias) e sem abuso policial - a recolha de informação que vise assegurar a prática de atos cautelares previstos nos artigos 249.º a 252.º do diploma, que foi o que a Polícia Judiciária fez.

Relativamente à natureza do prazo de 10 dias, entendemos que tem natureza meramente ordenadora ou indicativa. Assim, ainda que a notícia do crime ocorra após a verificação deste prazo, nem por isso perde a sua validade, não obstante a responsabilidade disciplinar de quem não respeitou o prazo e, eventual responsabilidade civil por danos decorrentes do exercício da função administrativa.

As medidas de polícia, quando comunicadas ao Ministério Público e quando não derem lugar à abertura de inquérito devem ser registadas, de acordo com a Ordem de Serviço n.º 4/2015 da Procuradoria-Geral da República (PGR), nas espécies processuais respetivas (Medidas de Polícia - Apreensão de correspondência; Medidas de Polícia - Identificação de suspeito; Medidas de polícia – Lei das Armas (Lei n.º 5/2006, de 23/2); Medidas de polícia – Metais não preciosos (Lei n.º 54/2012 de 6/9); Medidas de Polícia - Localização celular; Medidas de polícia – Outras Medidas de Polícia - Revista a pessoas).

1.2.2. A conservação e o exame de vestígios

a) O Exame

O exame, como medida cautelar, encontra-se previsto no artigo 249.º, n.º 2, alínea a), do Código de Processo Penal[9] e revela-se no plano da inspeção ao local do crime.

Nesta sede, e quanto aos primeiros intervenientes policiais chamados ao local – *first responders* – é particularmente importante que, através do cumprimento de um conjunto de regras e de boas práticas, desenvolvidas num contexto de atuação coordenada, contribuam ativamente para a proteção do local do crime e para a preservação dos elementos de prova nele existentes.

[9] Que prevê que os órgãos de polícia criminal têm competência, mesmo antes de receberem ordem da autoridade judiciária competente, para procederem "a exames dos vestígios do crime em especial às diligências previstas no n.º 1, do artigo 171.º, e artigo 173.º, assegurando a manutenção do estado das coisas e dos lugares."

Como acontece a todas as medidas cautelares e de polícia, o exame, para ser realizado nos termos previstos, tem de obedecer a critérios de urgência e *periculum in mora*.

Seguindo Germano Marques da Silva, "a finalidade do exame é fixar documentalmente ou permitir a observação direta pelo tribunal de factos relevantes em matéria probatória", sem que haja necessidade do elemento que o realiza possuir conhecimentos especiais, uma vez que os vestígios do crime "ou são depois objeto de perícia ou valorados direta e livremente pela autoridade judiciária".[10]

Depois de encontrados e fixados os vestígios, compete proceder à sua interpretação. O exame é apreciado segundo as regras dispostas no artigo 127.º do Código de Processo Penal.

Tendo em conta o artigo 171.º, n.º 1, do Código de Processo Penal, os exames consistem numa inspeção/observação que visa detectar a presença ou localização de vestígios e/ou indícios, sem qualquer análise técnica, científica ou artística, reservada à perícia (artigos 151.º e seguintes do Código de Processo Penal). Visa-se, com os exames "*fixar documentalmente ou permitir a observação direta pelo tribunal de factos relevantes em matéria probatória*".[11]

b) A Perícia

Existem vestígios que podem ser interpretados por qualquer um dos intervenientes na investigação (investigador, juiz) – exames - e outros que, por serem complexos, somente poderão ser interpretados por um especialista, com recurso a métodos técnicos, científicos ou artísticos, esta última situação constitui a prova pericial – artigos 151.º e 157.º do Código de Processo Penal.

Quanto à perícia, esta tem como finalidade quer a compreensão dos factos quer a sua valoração, "*o perito pode descobrir meios de prova, recorrendo a métodos científicos únicos a permitirem a sua apreensão ou pode exigir-se ao perito não a descoberta dos factos probatórios, mas apenas a sua apreciação*".[12]
A perícia apenas pode ser ordenada "*oficiosamente ou a requerimento, por despacho da autoridade judiciária*" competente (artigo 154.º do Código de Processo Penal)[13], os exames podem ser realizados no âmbito das medidas cautelares e de polícia (artigo 249.º, n.º 1 e 2, alínea a) do Código de Processo Penal), não obstante os casos dependentes de ordem ou autorização da autoridade judiciária competente, artigos 179.º, n.º 2, 269.º, n.º 1, alínea b) e 270.º, n.º 2, alínea c) e n.º 3, do Código de Processo Penal).[14] [15]

[10] Silva, Germano Marques da, Curso de Processo Penal – II volume, 4ª edição revista e atualizada, Lisboa, Editorial Verbo, 2008, p. 234.
[11] Silva, Germano Marques da, ob. cit, pág. 190.
[12] Cfr. Silva, Germano Marques da, ob. cit., pág. 210.
[13] Esta competência da autoridade judiciária obriga a um conhecimento mínimo, prévio, sobre a perícia a realizar, da sua adequação e relevância para a descoberta da verdade material, bem como para uma posterior interpretação dos resultados obtidos contidos no relatório pericial. Os conhecimentos deverão ser necessariamente maiores nos casos vertidos artigo 163.º do Código de Processo Penal, de modo a que o julgador possa fundamentar, de forma rigorosa e no mesmo plano científico, uma eventual divergência entre a sua convicção e o juízo contido no parecer dos peritos.
[14] A perícia é uma matéria que se situa fora das competências dos órgãos de polícia criminal, ficando excluída dos atos que lhe podem ser delegados pelo Ministério Público, artigo 270.º, n.º 2, alínea b), do Código de Processo

Há casos de perícias, enquanto medidas cautelares, previstas em legislação avulsa:

Na Lei do Combate à Droga, Decreto-Lei n.º 15/93, de 22 de janeiro, havendo indícios de alguém ocultar ou transportar, no interior do seu corpo (ex: estômago; ânus) estupefacientes, pode ser, com consentimento do visado, realizada perícia, prévia à comunicação ao Ministério Público e sem necessidade de intervenção das autoridades judiciárias – cfr. artigo 53.º do referido Decreto-Lei.

No âmbito da Lei n.º 45/2004, de 19 de agosto - regime jurídico das perícias médico-legais e forenses- o artigo 13.º prevê os procedimentos a adotar no caso de perícias médico-legais urgentes, cuja realização se verifica independentemente da intervenção da autoridade judiciária e poderá ser prévia à instauração de inquérito.

O n.º 1 deste artigo define o conceito de perícias médico-legais urgentes, como "aquelas em que se imponha assegurar com brevidade a observação de vítimas de violência, tendo designadamente em vista a colheita de vestígios ou amostras susceptíveis de se perderem ou alterarem rapidamente, bem como o exame do local em situações de vítimas mortais de crime doloso ou em que exista suspeita de tal. "

E os restantes números deste artigo dispõem sobre o modo de realização das referidas perícias urgentes.[16]

Penal (exceção da PJ, artigo 12.º da Lei n.º 37/2008, de 06 de agosto, Lei Orgânica da PJ). Não obstante esta exclusão, vemos uma extensão das medidas cautelares, quando, em casos de urgência ou de perigo na demora, a lei (n.º 3 do mesmo artigo 270.º) prevê a possibilidade de o Ministério Público delegar nas autoridades de polícia criminal - cujo conceito se encontra definido pelo artigo 1.º, alínea d), do Código de Processo Penal - "a faculdade de ordenar a efetivação de perícias relativamente a determinados tipos de crime, ex: poderá uma autoridade de polícia criminal ordenar a realização de perícia lofoscópica, após prévia recolha de impressões digitais (através de exame) a objeto encontrado no local do crime, de modo a interpretar os vestígios encontrados.

[15] Soares, Paulo, *in* Meios de obtenção de prova no âmbito de medidas cautelares e de Polícia, 2017, 2ª edição, pg.135, enuncia situações que não têm valor pericial: O relatório social – artigo 1.º, g) do Código do Processo Penal – cfr. acórdão do STJ de 20 de janeiro de 1998; O exame macroscópico direto efetuado à vista desarmada por médica veterinária, onde esta afirma que: "*não sendo visíveis as marcas sanitárias oficiais de inspeção sanitária, presumo tratar-se de abate clandestino*" (crime previsto e punido pelo artigo 22.º, n.º 1, alíneas a) e b), do Decreto-Lei n.º 28/84, de 20 de janeiro) – Acórdão do TRE, de 12 de abril de 2005, proc. 194/05-1, Relator Fernando Ribeiro Cardoso; O reconhecimento por parte de militar da GNR de que determinado jogo é de fortuna ou de azar – Acórdão do TRP, de 24 de janeiro de 2007, proc. 0644669, relator António Gama; O auto de exame e avaliação de objetos feito por funcionário ligado à investigação – Acórdão do TRP, de 14 de junho de 2006, proc. 0612322, relator Guerra Banha. "*A opinião emitida por um médico que seja testemunha no processo que incida sobre matéria médica, não obstante qualificada pelo seu conhecimento profissional, será sempre uma opinião não qualificada, face à opinião pericial*" – Acórdão do TRE, de 05 de fevereiro de 2013, proc. 529/08.2TAPTG-E1, relator João Sousa.

[16] N.º 2 a 7 do artigo 13.º, da lei n.º 45/2004, de 19 de agosto: "2 - Para a realização das perícias médico-legais urgentes a que se refere o número anterior haverá, diariamente, em cada delegação e gabinete médico-legal, um perito em serviço de escala, sendo da responsabilidade do director da delegação ou do coordenador do gabinete médico-legal indicar, para cada mês, os médicos escalados.
3 - Para assegurar a realização de perícias médico-legais urgentes fora do horário normal de funcionamento dos serviços, as delegações do Instituto e os gabinetes médico-legais elaboram e remetem às autoridades judiciárias e aos órgãos de polícia criminal da respectiva área de actuação a lista dos peritos em serviço de escala no mês seguinte, indicando os seguintes elementos:
a) Nome dos peritos;
b) Período de tempo assegurado por cada perito;
c) Contacto de cada perito durante o respectivo período de prevenção.

1.2.3. Revistas e Buscas

As noções de revista e busca encontram-se previstas no artigo 174.º do Código de Processo Penal.

De facto, de acordo com o n.º 1 do referido artigo "Quando houver indícios de que alguém oculta na sua pessoa quaisquer objectos relacionados com um crime ou que possam servir de prova, é ordenada revista."

Por sua vez, o n.º 2 prescreve que "quando houver indícios de que os objectos referidos no número anterior, ou o arguido ou outra pessoa que deva ser detida, se encontram em lugar reservado ou não livremente acessível ao público, é ordenada busca".

Em regra as revistas e buscas são autorizadas ou ordenadas pela autoridade judiciária competente, contudo a lei prevê situações em que os órgãos de polícia criminal podem proceder a estas diligências, sem necessidade de autorização da autoridade judiciária.

De facto, prevê o n.º 5 do artigo 174.º do Código de Processo Penal que as revistas e buscas efetuadas pelos órgãos de polícia criminal podem ser realizadas nos casos de:

a) De terrorismo, criminalidade violenta ou altamente organizada, quando haja fundados indícios da prática iminente de crime que ponha em grave risco a vida ou a integridade de qualquer pessoa;

b) Em que os visados consintam, desde que o consentimento prestado fique, por qualquer forma, documentado; ou

c) Aquando de detenção em flagrante por crime a que corresponda pena de prisão, podem ser realizadas sem autorização da autoridade judiciária.

Prevê ainda o artigo 177.º, do Código de Processo Penal, relativamente às buscas domiciliárias, que:

"**1** – A busca em casa habitada ou numa sua dependência fechada só pode ser ordenada ou autorizada pelo juiz e efectuada entre as 7 e as 21 horas, sob pena de nulidade.

4 - O disposto nos n.ºs 2 e 3 só se aplica aos gabinetes médico-legais em funcionamento que disponham de peritos do quadro do Instituto em número suficiente para assegurar o período de prevenção.
5 - As perícias médico-legais urgentes relativas a vítimas de agressão realizadas fora das horas normais de funcionamento dos serviços médico-legais poderão ter lugar em serviços de urgência de hospitais públicos ou outros estabelecimentos oficiais de saúde, dependendo, neste último caso, da prévia celebração de protocolos de cooperação entre estes e o Instituto.
6 - Nas situações previstas no n.º 4, excepcionalmente, sempre que se verificar o impedimento do perito médico de escala ou nas comarcas não compreendidas na área de actuação das delegações ou dos gabinetes médico-legais em funcionamento, pode a autoridade judiciária nomear médico contratado para o exercício de funções periciais ou médico de reconhecida competência para a realização de perícias médico-legais urgentes.
7- O Instituto ou os médicos referidos no número anterior podem cobrar, por cada perícia médico-legal urgente efectuada, os preços previstos em tabela aprovada por portaria do Ministro da Justiça, valendo as quantias arbitradas como custas do processo."

2 – Entre as 21 e as 7 horas, a busca domiciliária só pode ser realizada nos casos de:

a) Terrorismo ou criminalidade especialmente violenta ou altamente organizada;

b) Consentimento do visado, documentado por qualquer forma;

c) Flagrante delito pela prática de crime punível com pena de prisão superior, no seu máximo, a 3 anos.

3 – As buscas domiciliárias podem também ser ordenadas pelo Ministério Público ou ser efectuadas por órgão de polícia criminal:

a) Nos casos referidos no n.º 5 do artigo 174.º, entre as 7 e as 21 horas;

b) Nos casos referidos nas alíneas b) e c) do número anterior, entre as 21 e as 7 horas.
(...)"

Resulta deste artigo, a possibilidade de um órgão de polícia criminal, na sequência da detenção em flagrante pela prática de crime punível com pena de prisão superior, no seu máximo, a 3 anos, e mesmo antes de comunicar a notícia do crime, proceder à realização de busca domiciliária, inclusivamente sem qualquer limitação de horário.

Prevê também o artigo 251.º do Código de Processo Penal que:

"**1** – Para além dos casos previstos no n.º 5 do artigo 174.º, os órgãos de polícia criminal podem proceder, sem prévia autorização da autoridade judiciária:

a) À revista de suspeitos em caso de fuga iminente ou de detenção e a buscas no lugar em que se encontrarem, salvo tratando-se de busca domiciliária, sempre que tiverem fundada razão para crer que neles se ocultam objectos relacionados com o crime, susceptíveis de servirem a prova e que de outra forma poderiam perder-se;

b) À revista de pessoas que tenham de participar ou pretendam assistir a qualquer acto processual ou que, na qualidade de suspeitos, devam ser conduzidos a posto policial, sempre que houver razões para crer que ocultam armas ou outros objectos com os quais possam praticar actos de violência.

2 – É correspondentemente aplicável o disposto no n.º 6 do artigo 174.º"

As revistas e buscas previstas nas alíneas a) e c) do n.º 5 do artigo 174.º e no artigo 251.º, bem assim como as buscas domiciliárias na sequência de flagrante delito, são portanto medidas urgentes, que importa adotar em face das circunstâncias do caso, com vista a evitar, nomeadamente, a perda das provas presumidamente albergadas pelo objeto da revista/busca. E cuja execução eficaz é incompatível com qualquer dilação, nomeadamente a condição de imposição de prévia autorização judicial.

Analisando estes artigos verifica-se que:

a) As revistas e buscas realizadas na sequência de flagrante delito deverão ser realizadas ao abrigo dos artigos 174.º, n.º 5, alínea c), podendo realizar-se busca domiciliária, nos termos do disposto no artigo 177.º, n.º 2, alínea c) e 3, alínea b), do Código de Processo Penal.

b) As revistas a detidos fora de flagrante delito e buscas no lugar onde se encontrem, deverão ser realizadas ao abrigo do artigo 251.º, n.º 1, alínea a), do Código de Processo Penal, sempre que existir fundada razão para crer que neles se ocultam objetos relacionados com o crime que possam servir a prova;

c) As revistas de suspeitos, em caso de fuga iminente, serão realizadas ao abrigo do artigo 251.º, n.º 1, alínea a), do Código de Processo Penal, sempre que existir fundada razão para crer que neles se ocultam objetos relacionados com o crime que possam servir a prova;

d) As revistas de pessoas que tenham de participar ou pretendam assistir a qualquer ato processual, sempre que houver razões para crer que ocultam armas ou outros objetos com os quais possam praticar atos de violência, deverão ser realizadas ao abrigo do disposto no artigo 251.º, n.º 1, alínea b), do Código Processo Penal.

e) As revistas a suspeitos que devam ser conduzidos a posto policial, designadamente para efeitos de identificação, sempre que houver razões para crer que ocultam armas ou outros objetos com os quais possam praticar atos de violência, deverão ser realizadas ao abrigo do disposto no artigo 251.º, n.º 1, alínea b), do Código Processo Penal.

f) As revistas e buscas, mesmo domiciliárias, enquanto medidas cautelares poderão ser sempre realizadas no caso de consentimento do visado, o qual deverá ficar documentado nos autos, nos termos dos artigos 174.º, n.º 5, alínea b) e artigo 177.º n.º 2, alínea b) e n.º 3, alíneas a) e b), ambos do Código de Processo Penal.

De facto, ainda que os órgãos de polícia criminal possam, cautelarmente e nas condições *supra* descritas, realizar revistas e buscas independentemente de consentimento do visado, nada obsta que, para reforço da validade de tais atos, se obtenha do respetivo visado o respetivo consentimento, o qual deverá ser documentado nos autos.

Na prática judiciária é comum verificar-se que, não raras vezes, os órgãos de polícia criminal se limitam a elaborar autos de notícia e autos de apreensão, descurando a realização um auto de revista.

A boa prática, e bem assim a lei processual penal, impõem que se elabore igualmente o auto de revista, no qual se deve consignar, além da identificação do visado, da data, hora e local onde a mesma decorreu, também os motivos que a fundamentou (por ex. a detenção, as concretas suspeitas de que no visado se ocultam objetos relacionados com o crime que possam servir a prova, o consentimento do visado, etc), bem como os objetos apreendidos e o local onde foram encontrados.

À semelhança das perícias, também a legislação avulsa prevê a possibilidade de serem realizadas revistas e buscas.

Em matéria de repressão do crime de tráfico de estupefacientes, prevê o artigo 53.º do Decreto-Lei n.º 15/93, de 22 de janeiro:

"1 – Quando houver indícios de que alguém oculta ou transporta no seu corpo estupefacientes ou substâncias psicotrópicas, é ordenada revista e, se necessário, procede-se a perícia".

2 – O visado pode ser conduzido a unidade hospitalar ou a outro estabelecimento adequado e aí permanecer pelo tempo estritamente necessário à realização da perícia.

3 – Na falta de consentimento do visado, mas sem prejuízo do que se refere no n.º 1 do artigo anterior, a realização da revista ou perícia depende de prévia autorização da autoridade judiciária competente, devendo esta, sempre que possível, presidir à diligência.

4 – Quem, depois de devidamente advertido das consequências penais do seu acto, se recusar a ser submetido a revista ou a perícia autorizada nos termos do número anterior é punido com pena de prisão até 2 anos ou com pena de multa até 240 dias."

O regime estabelecido neste artigo em nada difere do regime regra estabelecido no Código de Processo Penal, na medida em que, se a revista não for consentida, tem de ser determinada por autoridade judiciária.

Note-se porém, que o artigo 4.º, n.º 1, da Lei n.º 30/2000, de 29 de novembro, que aprovou o Regime Jurídico do Consumo de Estupefacientes, estabelece um regime diverso, neste âmbito, permite-se que as autoridades policiais possam proceder à revista do consumidor de estupefacientes e à apreensão das plantas, substâncias ou preparações referidas no artigo 1.º encontradas na posse daquele.

1.2.4. Identificação de suspeito e pedido de informações

a) Identificação do suspeito

Trata-se de uma medida cautelar prevista no artigo 250.º do Código de Processo Penal e que este diploma legal expressamente exclui do âmbito das medidas de coação e de garantia patrimonial, nos termos do artigo 191.º, n.º 2. Na verdade, o artigo 250.º regula um mero procedimento policial, que ainda que possa restringir a liberdade de movimentos da pessoa, não o faz de forma significativa a poder ser considerado como uma medida de coação.

Através desta medida cautelar é atribuído ao órgão de polícia criminal um poder relevante que, como tal, deve ser exercido nos precisos termos descritos na norma.

O primeiro pressuposto inserto no artigo 250.º do Código de Processo Penal é que seja localizado um suspeito no lugar público. Segundo, que seja suspeito da prática de crimes; de pendência de processo de extradição ou expulsão; de permanência irregular em território nacional ou que haja contra si mandado de detenção.

Como refere Paulo Pinto de Albuquerque[17] o artigo 250.º estabelece um procedimento legal de identificação de suspeito que se divide em 4 fases:

a) Prova de qualidade de órgão de polícia criminal ao suspeito;[18]

b) Comunicação ao suspeito pelo órgão de polícia criminal das circunstâncias que fundamentam a obrigação de identificação e indicação dos meios de prova por que este se pode identificar.

c) Identificação do suspeito (pelos documentos do artigo 250.º, n.ºs 3 e 4 e pelos meios alternativos do n.º 5).[19]

d) Condução do suspeito ao posto policial mais próximo para identificação onde pode estar detido até 6 horas (n.º 6 do artigo 250.º), através de provas dactiloscópicas, fotográficas ou de natureza análoga (não incluindo a colheita e obtenção de perfil de ADN, segundo Helena Moniz, 2009: 147, nota 6).

Segundo José Brás[20], é discutível que o conceito de provas "de natureza análoga" possa abranger, no âmbito de medidas cautelares, exames e perícias que incidam sobre caraterísticas físicas por força do disposto nos artigos 154.º, n.º 2 e 269.º, n.º 1, alínea b), do Código de Processo Penal.

Sobre a problemática da identificação de suspeito veja-se a Lei n.º 67/2017, de 9 de agosto, que regula a identificação judiciária lofoscópica e fotográfica para efeitos de prevenção criminal, cujo artigo 3.º, quanto ao âmbito de aplicação da referida lei, prevê na alínea d) que são sujeitos a identificação judiciária os suspeitos nos termos do n.º 1 do artigo 250.º do Código de Processo Penal, que não sejam portadores de documento de identificação, não possam identificar-se por qualquer dos meios previstos nos n.ºs 3, 4 e 5 daquele artigo, ou recusem identificar-se perante autoridades ou órgãos de polícia criminal, nos termos aí prescritos.

Este diploma legal fixa as diligências que o órgão de polícia criminal deve realizar para efeitos de identificação de um suspeito (*vide* artigos 4.º a 6.º da Lei n.º 67/2017, de 9 de agosto que

[17] *In* ob. cit., ponto 3, p. 690.
[18] Quanto à necessidade do órgão de polícia criminal provar a sua qualidade antes de proceder à identificação, prevista no n.º 2 do artigo 250.º do Código de Processo Penal, entende-se que a lei adjetiva penal não comina qualquer sanção para a inobservância do disposto no artigo 250.º, n.º 2, do Código de Processo Penal, pelo que a falta de comunicação prévia da razão de ser da identificação por parte de qualquer entidade policial constituirá, quando muito, uma mera irregularidade – n.º 2 do artigo 118.º do Código de Processo Penal.
[19] Quanto ao reconhecimento da identidade por pessoa identificada nos termos do n.º 3 ou 4, parece-nos que padece de valor jurídico, porquanto a pessoa pode mentir, sem que qualquer sanção recaia sobre a mesma.
[20] *In* Investigação Criminal, a organização, o método e a prova, os desafios da nova criminalidade, 2009, Almedina, p. 231.

referem, como meios de identificação: a recolha de amostras-referência; amostras-problema e fotografia técnico-policial de identificação).

Relativamente ao período de detenção até 6 horas em posto policial, para efeitos de identificação (referido no artigo 250.º, n.º 6, do Código de Processo Penal) tem cobertura constitucional – cfr. artigo 27.º, n.º 3, alínea g), da Constituição da República Portuguesa.

A condução ao posto policial tem de ser reduzida a auto que deve detalhar a hora e o local de abordagem do suspeito no "lugar público", a hora de entrada do suspeito no posto policial e a hora de saída.

Este documento nunca pode ser destruído sem autorização prévia do Ministério Público, sob pena de violação do poder de direção do inquérito pelo Ministério Público.

Refira-se ainda a Lei n.º 53/2008, de 29 de agosto (Lei de Segurança Interna) que nos seus artigos 28.º, n.º 1, alínea a), e 31.º, estabelece como medida de polícia, a identificação de cidadãos, nos exatos termos previstos no artigo 250.º do Código de Processo Penal.

b) As consequências da recusa de identificação

O artigo 250.º, n.º 6, do Código de Processo Penal, relativo à condução a posto policial para efeitos de identificação, reflete a questão da impossibilidade de identificação nos termos dos números anteriores.

A questão que se coloca é saber se o conceito de "impossibilidade" referido no mencionado n.º 6 do artigo 250.º é um conceito amplo que compreenderá a "recusa" em se identificar, ou antes pelo contrário, se tratam de situações jurídicas diversas e, consequentemente, sujeitas a diferente tratamento jurídico.

Caso se entenda que estão em causa situações jurídicas merecedoras de tratamento diferenciado, a "impossibilidade" de o identificando se identificar despoletaria o procedimento previsto no artigo 250.º, n.º 6, do Código de Processo Penal (condução a posto policial para efeitos de identificação) e a "recusa" em se identificar originaria a prática do crime de desobediência, previsto e punido pelo artigo 348.º do Código Penal, devendo o identificando ser detido em flagrante delito, nos termos dos artigos 27.º, n.º 3, alínea a), da Constituição da República Portuguesa, 255.º e 256.º do Código de Processo Penal.[21]
Acompanhamos a posição assumida por Jean Christophe dos Santos Carvalho[22], entendemos que o conceito de "impossibilidade" em se identificar, inclui a "recusa", assim esta figura não fica obrigatoriamente relacionada com o crime de desobediência para atingir a sua eficácia prática, uma vez que as consequências dos mecanismos de identificação dos suspeitos,

[21] Neste sentido Afonso, João José Rodrigues, *in* O regime legal da identificação – reflexões sobre o instituto da detenção para efeitos de identificação, Coimbra: Almedina, 2008, p. 384-385, defendendo a posição doutrinal que, perante a recusa de identificação por parte de suspeitos da prática de crime, esta consubstancia um crime de desobediência.
[22] *In* Dissertação de mestrado integrado em ciências policiais, "Da identificação de suspeitos e consequências jurídicas da recusa", 2014, p. 57.

obedecendo ao princípio da escalada de meios patentes no artigo 250.º do Código de Processo Penal, são idóneas na obtenção da sua finalidade – a identificação do suspeito.

É a existência de um dever efetivo de identificação, consagrado no artigo 250.º do Código de Processo Penal e na LSI, que se concretiza o procedimento de condução coativa de um suspeito a um posto policial, ao abrigo do n.º 6 do artigo 250.º do Código de Processo Penal, já esgotados os outros procedimentos previstos no referido preceito.[23]

Caso se verifique a recusa do identificando em acompanhar o órgão de polícia criminal ao posto policial, ou aí se encontrando, se recuse a realizar provas dactiloscópicas ou de outra natureza, entendemos que deve o órgão de polícia criminal constranger (utilizando a força estritamente necessária) o identificando a cumprir o legalmente estatuído.[24]

No mesmo sentido vão as mais recentes alterações legislativas consagradas na Lei n.º 67/2017, de 9 de agosto, cujo artigo 4.º, quanto à recolha de amostras-referência, prevê no n.º 3 que "Em caso de recusa, a autoridade judiciária competente pode ordenar a sujeição à diligência, nos termos do disposto no Código de Processo Penal quanto à sujeição a exame."

c) "Conversas informais"

O n.º 8 do artigo 250.º do Código de Processo Penal, relativamente ao fornecimento pelo suspeito de informações criminais úteis, sem a prévia constituição como arguido, está condicionado a que tais informações não sejam autoincriminatórias. Fora desse caso, deve a pessoa sobre quem recaem suspeitas da prática do crime ser constituída arguida, nos termos do disposto no artigo 59.º do Código de Processo Penal.

A propósito desta matéria coloca-se a pertinente questão das "conversas informais" mantidas entre os órgãos de polícia criminal e eventuais suspeitos da prática de um crime, existindo abundante jurisprudência sobre este assunto no sentido da legalidade desta conversas desde que verificados determinados pressupostos legais.[25] [26]

[23] A este propósito ver Parecer do Conselho Consultivo da PGR n.º 28/2008, disponível in www.dgsi.pt/, em especial o voto de vencido de António Leones Dantas quanto à cominação como crime de desobediência a recusa do identificado em se identificar "seria uma forma simples de coagir um cidadão à identificação, mas violadora de princípios fundamentais, nomeadamente do princípio da subsidiariedade da intervenção penal."

[24] Em sentido discordante o Parecer do Conselho Consultivo da PGR n.º 13/96, disponível *in* simp.pgr.pt (relator: Souto de Moura).

[25] Veja-se a título de exemplo o acórdão do TRL de 22.06.2017, disponível in www.dgsi.pt, relatora Filipa Costa Lourenço "I- Não existem conversas informais quando as forças policiais se limitam a cumprir os preceitos legais, quer pela necessidade de "documentar" a prática do ilícito e suas sequelas, designadamente providenciar os actos cautelares que se imponham (v. g. artigos 243.º, 248 a 250.º do C.P.P.), quer quando actuam por imposição legal ao detectarem a prática de um ilícito e o suspeito decide, por sua iniciativa, de forma voluntária e sem actuação criticável das forças policiais, fazer afirmações não sugeridas, provocadas ou imaginadas por aqueles OPC, estando estes a cumprir preceitos legais que lhes impõem uma actuação; II- As forças policiais não estão proibidas de falar com os cidadãos que podem vir a ser constituídos arguidos ou com os suspeitos, ou com quem se encontra numa "cena de crime", desde que não houver culpa sua no atrasar da formalização daquela constituição. E, como mera decorrência do n.º 5 do artigo 58.º do Código de Processo Penal, a omissão ou violação das formalidades previstas nos números anteriores implica que qualquer declaração daquele que já deveria ter sido constituído como arguido não pode ser utilizada como prova. III-Face ao ordenamento português, o simples cidadão ou cidadão suspeito não goza do direito ao silêncio e, como tal, a prova produzida pelas suas declarações, melhor, depoimento, é válido. Se ainda não havia obrigação de constituição como arguido e as entidades policiais agiam dentro dos poderes

1.2.5. Apreensão de correspondência

A apreensão de correspondência encontra-se prevista no artigo 252.º do Código de Processo Penal e tem tutela constitucional, prevista no artigo 34.º da Constituição da República Portuguesa.[27]

O Código de Processo Penal prevê duas situações de apreensão de correspondência: a título cautelar, prevista neste artigo 252.º, e a do regime geral, prevista no artigo 179.º.

Em qualquer dos casos encontra-se sujeita ao crivo judicial, veja-se que o artigo 252.º, n.º 1, prevê que caso o órgão de polícia criminal apreenda correspondência, transmite-a intacta ao juiz.

O Código de Processo Penal distingue, no n.º 2 deste artigo 252.º, o caso da apreensão de encomendas ou valores fechados sempre que se tiver razões para crer que podem conter informações úteis à investigação de um crime. Nesta situação o órgão de polícia criminal informa o juiz, pelo meio mais rápido, o qual pode ordenar a abertura imediata.

O n.º 3 do artigo 252.º prevê ainda a possibilidade do órgão de polícia criminal poder ordenar a suspensão da correspondência pelo prazo de 48 horas, durante as quais tem de obter a autorização do juiz para a sua apreensão.

Entendemos que apenas este número 3 corresponde a uma medida cautelar, porquanto, nas situações dos n.ºs 1 e 2 do artigo 252.º, o juiz já autorizou ou ordenou a diligência.

---

concedidos pelas normas reguladoras da aquisição e notícia do crime (artigos 241.º e 242.º) e de medidas cautelares e de policia (artigos 248.º e seguintes, designadamente o artigo 250.º do C.P.P.) e, sem má fé ou atraso propositado na constituição de arguido, ouvem do cidadão ou suspeito a informação da prática de um crime, isso não constitui violação de lei ou fraude à lei, nem obtenção de prova proibida. IV-Por isso a proibição de "conversas informais" só deve abranger afirmações posteriores à constituição de arguido e nunca antes da sua constituição pois ai nem existem propriamente "conversas informais", mas sim afirmações de um cidadão, que pode ser suspeito ou nem isso. E este é, no ordenamento processual penal português, uma testemunha. V - Assim, a questão centra-se, no caso de situações de fronteira, na distinção a fazer entre as figuras de "suspeito" e "arguido". Este goza de direitos, aquele é testemunha. O arguido goza do direito ao silêncio, o suspeito não. VI - Logo a constituição formal de arguido constitui a "linha de fronteira" da admissibilidade da reprodução em audiência de julgamento das ditas "conversas informais", sendo que a partir daquele momento as declarações só têm valor de prova quando prestadas em actos mencionados na lei, considerando-se sem carácter probatório todas as demais provas que foram recolhidas informalmente, em conversas ou em actos sem previsão ou legitimação legal. VII- As afirmações produzidas nesta fase preliminar por qualquer pessoa abordada no decurso de operação policial, seja ela, suspeito ou potencial testemunha do crime, não traduzem "declarações" *strictu sensu* para efeitos processuais, já que não existe, ainda, verdadeiramente um processo penal a correr os seus termos. São diligências de aquisição e conservação de prova, lícitas, dada a sua conformidade com o comando legal prescrito no art. 249.º do CPP, não sendo, por isso, proibido o seu relato em audiência (em sede de audiência vale como prova testemunhal)."

[26] No mesmo sentido, vejam-se ainda o Acórdão do TRE de 04.06.2013, relator João Gomes de Sousa; o Acórdão do TRE de 16.02.2016, relator João Gomes de Sousa e o Acórdão do TRP, de 17.06.2015, relator Artur Oliveira, todos disponíveis in www.dgsi.pt.

[27] O artigo 34.º da Constituição da República Portuguesa estabelece que "*1. O domicílio e o sigilo da correspondência e dos outros meios de comunicação privada são invioláveis.*
(...)
4. É proibida toda a ingerência das autoridades públicas na correspondência, nas telecomunicações e nos demais meios de comunicação, salvos os casos previstos na lei em matéria de processo criminal".

Em matéria de correspondência, a questão que se tem colocado na prática é saber se um órgão de polícia criminal, designadamente no exercício de acções fiscalizadoras em matéria fiscal ou alfandegária[28] pode proceder à abertura de correspondência / encomendas e verificando que as mesmas contêm no seu interior objetos suscetíveis de integrar um ilícito criminal, se deve proceder à apreensão cautelar dos mesmos.

Quanto a este assunto pronunciou-se o Conselho Consultivo da PGR através do Parecer n.º 15/95[29], no seguinte sentido:

" (…) 2 – O sigilo da correspondência estatuído nos n.ºs 1 e 4 do artigo 34.º da Constituição da República não abrange os pacotes e encomendas postais, contendo mercadorias, que devem ser apresentados a fiscalização alfandegária;

3 – Consequentemente, a fiscalização, pelas autoridades aduaneiras, dos "objetos de correspondência postal e das encomendas postais" conduzidos à alfândega, para assegurar o cumprimento da legislação aduaneira e demais disposições aplicáveis às mercadorias sob fiscalização aduaneira, nos termos previstos nos Regulamentos (CEE) n 2913/92, de 12 de outubro, do Conselho das Comunidades Europeias, diretamente aplicáveis na ordem interna, é compatível com o sigilo da correspondência previsto nos n.ºs 1 e 4 do artigo 34.º da Constituição da República;

4 – A fiscalização referida na conclusão insere-se numa competência própria das autoridades aduaneiras, como órgãos de polícia fiscal, não carecendo, como tal, de intervenção das autoridades judiciárias."

Em sentido diverso encontra-se o acórdão do STJ, de 18.05.2006, relator Santos Carvalho, disponível *in* www.dgsi.pt, quanto à atuação das autoridades aduaneiras:

"Dos arts. 26.º, n.º 1, 18.º, n.º 2, 32.º, n.º 8, e 34.º da CRP, bem como 126.º, n.º 3, e 179.º, n.ºs 1 e 3, do CPP, resulta que a proteção do direito à reserva da vida privada é especialmente salvaguardada quando está em jogo correspondência, sendo que se precisa de que por tal se consideram não só as cartas, como ainda encomendas, valores, telegramas ou qualquer outra forma similar de comunicação entre pessoas.
II – A violação da correspondência só pode ser feita por ordem do juiz e este é a primeira pessoa que toma conhecimento do conteúdo da mesma.
III – Pode admitir-se que numa situação em que haja urgência ou perigo na demora, os órgãos de polícia criminal possam efetuar apreensões de correspondência, mas tal ato fica sujeito a validação no prazo máximo de 72h pela "autoridade judiciária" (art. 178.º, n.ºs 4 e 5), isto é, pelo juiz e não o MP, já que há reserva de competência daquele (art. 179.°).
IV – Fora dessas situações, estamos perante a nulidade de um meio de prova.
V – Não deve confundir-se a nulidade dos actos processuais, prevista nos art.ºs 118.º a 123.º do CPP, com a nulidade dos meios de prova, pois o próprio art.º 118.º, n.º 3, estabelece que as

[28] No caso da propriedade industrial o órgão de polícia criminal competente é a Unidade de Acção Fiscal da GNR; caso se trate a fiscalização alfandegária, a competência encontra-se atribuída às autoridades alfandegárias.
[29] Disponível nas bases de dados do simp.pgr.pt/basesmj.

58 disposições do presente título (nulidades) não prejudicam as normas desse Código relativas a proibições de prova.
VI – E, assim, enquanto que a nulidade de um ato pode ser sanável ou insanável, a nulidade do meio de prova dá lugar à proibição de ser usado para esse fim (de prova).
VII – As autoridades aduaneiras podem exercer fiscalização sobre toda a correspondência que envolve o transporte de mercadoria, mas tal fiscalização não passa pela apreensão nem pela abertura não autorizada das embalagens, mas pela faculdade de só emitir o despacho alfandegário quando houver a certeza de que a declaração da mercadoria corresponde ao real conteúdo da correspondência, o que pode ser concretizado pelo pedido de documentação adicional ou pelo pedido de desembalagem ao interessado – é o que resulta, por exemplo, dos arts. 37.º e 46.º do Código Aduaneiro Comunitário, Regulamento (CEE) n.º 2913/92 do Conselho.
VIII – Essa faculdade de retenção da mercadoria até ao seu despacho alfandegário não pode confundir-se com a apreensão e muito menos com a violação de correspondência, pois aquela, ao contrário destas, não confere a faculdade de quebrar o direito ao sigilo da vida privada e, portanto, não interfere com as normas constitucionais ou de processo penal indicadas.
IX – O mesmo se passa com o visionamento de correspondência através de técnicas que não envolvem a abertura da correspondência e que só permitem uma conferência sumária do interior da mesma, pois tais técnicas afiguram-se proporcionais e adequadas aos fins visados (conferir a mercadoria com a declaração alfandegária) e não dão azo a uma violação do referido direito constitucional."[30]

De acordo com o entendimento do STJ, o não cumprimento destes procedimentos processuais gera uma nulidade insanável, por utilização de métodos proibidos de produção de prova, nos termos do artigo 126.º, n.º 3 do Código de Processo Penal, solução com a qual se concorda.

1.2.6. Localização celular

Esta medida encontra-se prevista no artigo 252.º - A do Código de Processo Penal.

Refere Pedro Verdelho[31] que "A localização celular revela, por via da observação da sua ligação à rede telefónica móvel, a localização de um detentor de determinado aparelho telefónico. Obter a localização celular tem, portanto, o mesmo intuito probatório de uma vigilância tradicional efetuada por agentes policiais sobre um determinado indivíduo".
Trata-se de um sistema de localização geográfica global com elevado rigor científico, que se socorre da tecnologia GSM (Global System for Mobile Comunication), e permite realizar a trajetória geográfica de um determinado aparelho de telemóvel.

Nas palavras de Fernando Gama Lobo[32] "admitindo-se que o sinal rádio navega à velocidade da luz, é medido o tempo entre a transmissão pelo telemóvel e a receção do sinal pela BTS

[30] No mesmo sentido veja-se ainda o acórdão do TRC, de 07.06.2017, relator Maria Pilar de Oliveira, disponível *in* www.dgsi.pt.
[31] *In* Ver. CEJ, n.º 9, 1.º semestre de 2008.
[32] *In* Código de Processo Penal Anotado, Almedina, 2015, p. 343.

(torre onde estão as antenas voltadas para um azimute de acordo com a região que se deseja irradiar pelo sinal) e então é estimada a distância do telefone celular a essa torre. Cruzando estes dados com outras BTS vizinhas, através de um procedimento de triangulação, é possível chegar a uma localização muito aproximada do telemóvel, em média não superior a 250 metros para locais urbanos ou 800 metros para áreas rurais."

Quanto mais BTS existirem maior é a capacidade de triangulação e, consequentemente maior rigor de localização geográfica.

O Código de Processo Penal apenas admite o recurso a esta medida para proteção de bens de natureza pessoal (perigo para a vida ou ofensas à integridade física grave).

Não é admitido o recurso a esta medida cautelar para acautelar bens de natureza patrimonial.

O artigo 189.º, n.º 2, do Código de Processo Penal (quanto ao meio de obtenção de prova das escutas telefónicas) também alude à localização celular, impondo para este efeito que "A obtenção e junção aos autos de dados sobre a localização celular ou de registos da realização de conversações ou comunicações só podem ser ordenadas ou autorizadas, em qualquer fase do processo, por despacho do juiz, quanto a crimes previstos no n.º 1 do artigo 187.º e em relação às pessoas referidas no n.º 4 do mesmo artigo."[33]

1.2.7. Localização através do sistema GPS (*Global Positioning System*)

É diverso da localização celular porquanto visa a localização direta e com alto grau de precisão de pessoas ou bens (normalmente viaturas, através de aparelhos vulgarmente denominados "balizas"), através do fornecimento pelo sistema de satélites das suas coordenadas geográficas.[34]

Importa considerar duas questões fundamentais quanto a este assunto:

1. É necessário autorização judicial para fazer uso desta medida em sede de inquérito?

[33] Não obstante a norma transcrita não impor, de forma expressa, a aplicação das formalidades previstas no artigo 188.º do Código de Processo Penal, tem sido entendido por alguma doutrina e jurisprudência que o Juiz de Instrução deve exercer uma função de controlo no que diz respeito à junção dos dados aos autos, designadamente no que diz respeito ao cumprimento dos pressupostos legais bem como à relevância da informação recolhida para a investigação. Neste sentido o acórdão do Tribunal da Relação de Lisboa, de 15-09-2011, relator Carlos Benido, segundo o qual "*embora tenha sido ordenado pelo Mmo. JIC o acesso à facturação detalhada e localização celular, não existindo despacho do juiz a ordenar a junção aos autos do material colhido, a ponderar se esse material tem todo ele ou só parte relevância, ordenando a junção do material com interesse e a destruição do restante, aquela prova é nula*". Somos da opinião que o entendimento expresso no acórdão referido peca por excessivamente "colado" à letra do preceito do artigo 189.º, n.º 2, do Código de Processo Penal, porventura descurando outros critérios de interpretação de uma norma jurídica, como o sistemático, histórico, axiológico, sociológico e teleológico, os quais, em nosso entender levariam a considerar uma solução diversa da sustentada.

[34] Acórdão do TRE de 07.10.2008, relator Martinho Cardoso, disponível *in* www.dgsi.pt, sobre a localização por GPS "*é activada por um aparelho sintonizado com pelo menos dois satélites, dos quais recebe a informação das coordenadas da longitude e da latitude a que o aparelho se encontra, fornecendo-lhe assim a localização do sítio exato por reporte ao mapa das estradas dessa região, informação que é transmitida e reproduzida num recetor na posse, neste caso da autoridade policial*".

A regulamentação desta questão está omissa na lei, pelo que deve entender-se que segue o regime previsto no artigo 125.º do Código de Processo Penal, ou deve enquadrar-se no disposto no artigo 126.º, n.º 3, do mesmo diploma legal, e considerar que se trata de uma intromissão na vida privada?

O acórdão do TRE de 07.10.2008, disponível *in* www.dgsi.pt, relator Martinho Cardoso refere que "Mas ter a autoridade policial no decurso de um inquérito criminal acesso à informação de onde está a cada momento um determinado veículo automóvel, não pode ser visto como uma intromissão na vida privada de quem vai nesse veículo, pois o GPS é um aparelho surdo e cego no sentido de que não escuta as conversas dos ocupantes do carro, nem identifica quem lá vai e o que estão a fazer, apenas informa aonde está o veículo, circunstância que é visível a olho nu para quem olhe para o carro e lhe vê a matrícula. Situação bem diferente seria – como está bom de ver – a de utilizar localizadores de GPS em pessoas individuais ou grupo de pessoas individuais."

De acordo com esta interpretação a localização GPS seria uma forma até menos gravosa de realizar uma vigilância / seguimento de um suspeito.[35]

Diferente entendimento se encontra expresso no acórdão do Supremo Tribunal de Justiça, de 08.01.2014, relator Armindo Monteiro, disponível em www.dgsi.pt:

"*A localização celular é uma inovação introduzida pela Lei 48/2007, de 29-08, que, enquanto meio de obtenção de prova, se mostra prevista nos arts. 188.º e 252.º-A do CPP, com um sentido e alcance bem distintos. A obtenção de dados através da localização celular, muito em uso no meio militar e até civil, para controle da localização de pessoas, pela adaptação de um dispositivo (GPS ou GSM) ao telemóvel, diz respeito à utilização de dados, revela o percurso físico que o titular do telemóvel fez ou a está a fazer, a sua mobilidade ou permanência; por via da sua ligação à rede telefónica revela a localização do aparelho telefónico, obedecendo ao mesmo propósito que uma vigilância policial sobre um dado indivíduo potenciada pelos meios electrónicos disponíveis pelas forças policiais, não permitindo aperceber ou revelar quaisquer comunicações nem o seu conteúdo (cf., neste sentido, Pedro Verdelho, RMP, Ano 27, 115/116, e Revista do CEJ, 1.º semestre, 2008, pág. 169). São aí incluídos «a latitude, longitude e altitude, a direcção de deslocação, o nível de precisão da informação de localização, a identificação da célula da rede em que o equipamento terminal está localizado em dado momento e hora de registo de informação da localização», complementa o Parecer da PGR de 02-10-2009, VII - A obtenção de dados de localização celular, nos termos do art. 189.°, n.º 2, do CPP, está submetida à autorização, por despacho do Juiz quanto a crimes previstos no art. 187.°, n.º 1, do CPP, e em relação às pessoas mencionadas no seu n.º 4, ou seja, a crimes de catálogo, portadores, pois, de uma certa gravidade referentes a pessoas que preencham um estatuto aí especificado.*"

[35] Dizemos menos gravosa porque uma vigilância pessoal permite determinar outros elementos alheios à utilização de GPS, ex: quem segue com o suspeito; o que fez o suspeito durante o trajeto, etc…

Dúvidas não restam quanto à possibilidade de utilização do sistema GPS ser restrita a viaturas e excluir a sua aplicação a pessoas, sob qualquer que seja o pretexto.

2. É admitido o recurso a esta forma de localização como medida cautelar, com base no pressuposto que as medidas cautelares e de polícia estão elencadas na lei de forma não taxativa, como decorre do artigo 249.º, n.º 2 do Código de Processo Penal?

Entendemos que desde que se verifiquem os requisitos exigidos por lei para qualificar um determinado ato como medida cautelar de polícia: a urgência e perigo na demora e impossibilidade de recorrer em tempo útil às autoridades judiciárias competentes, e desde que estejam em causa situações previstas no artigo 252.º-A do Código de Processo Penal, deve ser seguido, por analogia, este regime.

1.2.8. A Videovigilância

A videovigilância surge regulamentada em diversos diplomas legais.[36]

As vídeo-gravações em espaços públicos, para proteção e segurança da comunidade naqueles locais, não são ilícitas, sobretudo quando previamente autorizadas pela comissão nacional de proteção de dados, nos termos da Lei n.º 67/98, de 26 de outubro, Lei da Proteção de Dados Pessoais.[37]
Contudo, existe diversa jurisprudência que admite a valoração de imagens de videovigilância como prova ainda que os sistemas de videovigilância não tenham sido autorizados pela CNPD ou caso se desconheça se o foram[38].

Sendo patente que os sistemas de videovigilância estão direcionados para o desempenho de finalidades relativas à «protecção de pessoas e bens», apresentando-se como medida preventiva e de dissuasão em relação à prática de infrações penais e podendo, ao mesmo tempo, servir de prova nos termos da lei processual penal, é imprescindível que – de acordo com o princípio da necessidade – o acesso às imagens seja restrito às entidades que delas

[36] Lei n.º 34/ 2013 – utilização de sistemas de videovigilância pelos serviços de segurança privada e de autoproteção; Portaria 273/ 2013 – Regula a Lei n.º 34/2013; Lei 1/ 2005 – regula a videovigilância pelas forças de segurança em locais públicos de utilização comum (alterada e republicada); Decreto-Lei n.º 207/ 2005 – Regula os meios de vigilância eletrónica rodoviária utilizados pelas forças de segurança; Lei n.º 51/ 2006 – regula a utilização de sistemas de vigilância rodoviária pela EP e pelas concessionárias rodoviárias; Lei n.º 33/ 2007 – regula a instalação e utilização de sistemas de videovigilância em táxis; Portaria 1164-A/ 2007 – aprova o modelo de aviso de videovigilância em táxis; Lei n.º 67/98, de 26 de outubro e Código do Trabalho – artigo 20.º.
[37] Quanto a esta matéria veja-se Paulo Pinto de Albuquerque, *in* Comentário do Código de Processo Penal, 2011, pg. 463, ponto c. "As imagens e os sons obtidos por sistema mecânico de videovigilância colocado dentro do imóvel do ofendido ou à entrada do mesmo (acórdão do TRL, de 28.05.2009, proc. 10210/2008-9, e acórdão do TRG, de 26.04.2010, *in* CJ XXXV, 2, 289) ou em postos de abastecimento de combustíveis, caixas de multibanco, escolas ou outros lugares públicos ou ainda em espaços divisórios entre duas propriedades, desde que devidamente autorizado, uma vez que ele se dirige à generalidade do público e não a qualquer pessoa ou grupo de pessoas em especial, não sendo por isso aplicável o disposto no artigo 6.º, n.º 1, da Lei n.º 5/2002, de 11.01 (acórdão do STJ de 20.06.2001, *in* CJ, Acs. do STJ, IX, 2, 221, acórdão do TRG, de 30.09.2002, *in* CJ, XXVII, 4, 285).
[38] Vejam-se nesse sentido o acórdão do TRP de 26.03.2008, *in* CJ, XXXIII, 2, 223, admitindo mesmo as imagens obtidas por sistemas de videovigilância não autorizados, e acórdão do TRL, de 04.03.2010, *in* CJ, XXV, 2 134, admitindo as imagens obtidas por sistemas em relação aos quais se desconheça se foram comunicados à CNPD.

precisam para alcançar as finalidades delineadas. Uma vez detetada a prática de infração penal, a entidade responsável pelo tratamento deve – com a respetiva participação – enviar ao órgão de polícia criminal ou à autoridade judiciária competente as imagens recolhidas.

O que está em causa na utilização destes meios é assegurar a dissuasão, sempre com o conhecimento das pessoas e com proteção dos seus direitos fundamentais bem como registar e documentar a eventual prática de infrações. Como se salienta no Parecer da Procuradoria-Geral da República n.º 95/2003, de 6 de novembro[39] – sobre Direito à imagem – Direito a informar – Recolha de imagem – Intimidade da vida privada – Direitos, liberdades e garantias – Conflito de direitos – Fotografia ilícita – Medida de polícia, em relação à prevenção criminal levada a cabo pela polícia – com referência ao acórdão do Tribunal Constitucional n.º 456/93 – os «atos de polícia de natureza preventiva» podem decorrer da vigilância ou ser independentes dela: «umas vezes configuram-se como atos genéricos, dirigindo-se a uma pluralidade de pessoas; outras vezes como atos individuais. A vigilância genérica poderá ser essencialmente preventiva; por seu lado, a vigilância individualmente dirigida apresentar-se-á, na normalidade dos casos, mais como ato de averiguação ou, então, de prevenção direta determinada pela prévia existência de elementos de suspeita relativamente a algum comportamento individual».

Estes conceitos e princípios são aplicáveis à realidade da videovigilância levada a efeito pelas entidades responsáveis que decidem avançar com o tratamento vocacionado para a «protecção de pessoas e bens». A recolha de som e imagem não está direcionada, em geral, para atos individuais mas abrange o universo das pessoas – não se sabe quais – que frequentam o estabelecimento e sem que haja, à partida, a mínima suspeição sobre a sua conduta. As imagens só têm relevância e só são «pertinentes» (cf. artigo 5.º, n.º 1, al. c), da Lei n.º 67/98) quando ocorrer algum facto com relevância em sede de investigação criminal. Neste caso serão as imagens encaminhadas para a autoridade competente.[40]

Do exposto resulta que, o órgão de polícia criminal competente pode, logo no momento da notícia do crime, e sem dispor ainda de qualquer delegação de competências ou autorização por parte da autoridade judiciária competente, solicitar a preservação de imagens ou o acesso às mesmas, caso exista algum sistema de videovigilância que permita a recolha de elementos probatórios para os autos.

1.2.9. Via Verde

A via verde dispõe de informação relativa aos registos de passagens nas portagens efetuados por veículos automóveis.

É fácil compreender a relevância desta informação para efeitos de investigação criminal e, a necessidade, desde que preenchidos os requisitos legalmente estabelecidos, de socorrer destes registos mesmo ao nível das medidas cautelares.

[39] Disponível *in* http://www.dgsi.pt.
[40] Deliberação n.º 61/ 2004 da CNPD, princípios sobre o tratamento de dados por videovigilância.

Porém, a via verde tem exigido, para prestação desta informação aos órgãos de polícia criminal, uma ordem proveniente de autoridade judiciária.

Entendemos que face ao previsto no artigo 417.º (art.º 519.º CPC 1961) do Código de Processo Civil, *ex vi* artigo 4.º do Código de Processo Penal existe o dever de cooperação para a descoberta da verdade:
"1 - Todas as pessoas, sejam ou não partes na causa, têm o dever de prestar a sua colaboração para a descoberta da verdade, respondendo ao que lhes for perguntado, submetendo-se às inspeções necessárias, facultando o que for requisitado e praticando os atos que forem determinados.
2 - Aqueles que recusem a colaboração devida são condenados em multa, sem prejuízo dos meios coercitivos que forem possíveis; se o recusante for parte, o tribunal aprecia livremente o valor da recusa para efeitos probatórios, sem prejuízo da inversão do ónus da prova decorrente do preceituado no n.º 2 do artigo 344.º do Código Civil."

Somos ainda da opinião que se aplica a Lei n.º 51/2006, de 29 de agosto sobre sistemas de vigilância eletrónica rodoviária (regula a instalação e utilização de sistemas de vigilância electrónica rodoviária e a criação e utilização de sistemas de informação de acidentes e incidentes pela EP - Estradas de Portugal, E.P.E., e pelas concessionárias rodoviárias), porquanto trata-se de informação relacionada com a proteção e segurança das pessoas e bens, públicos ou privados, no que respeita à circulação rodoviária ou o controlo e monitorização do tráfego rodoviário, nos termos previstos no seu artigo 2.º.

Esta lei no artigo 16.º sobre Comunicação de dados dispõe que: "1 - Os dados pessoais obtidos através dos sistemas de vigilância electrónica rodoviária e dos sistemas de informação de acidentes e incidentes devem ser comunicados, sempre que solicitado, às seguintes entidades:
a) Forças de segurança, nos termos e para os efeitos da legislação em vigor;
b) Autoridades judiciárias, para efeitos de instauração ou condução dos processos a seu cargo;"

Assim, parece que a recusa de fornecimento de registos de circulação por parte da via verde aos órgãos de polícia criminal, no âmbito de uma medida cautelar e desde que verificados os pressupostos exigidos por lei (urgência e perigo na demora), carece de fundamentação legal.
Não se vislumbra que a obtenção de registos da via verde deva obedecer a um espartilho mais apertado do que a localização celular ou a obtenção de imagens de videovigilância.

1.2.10. Medidas cautelares na Lei do Cibercrime

a) Preservação expedita de dados

Nos termos dos n.ºs 1 do artigo 12.º da Lei n.º 109/2009, de 15 de setembro – Lei do Cibercrime -, se no decurso do processo for necessário à produção de prova, tendo em vista a descoberta da verdade, obter dados informáticos específicos armazenados num sistema informático, incluindo dados de tráfego, em relação aos quais haja receio de que possam

perder-se, alterar-se ou deixar de estar disponíveis, a autoridade judiciária competente ordena a quem tenha disponibilidade ou controlo desses dados, designadamente a fornecedor de serviço, que preserve os dados em causa.

Essa ordem de preservação, nos termos do n.º 2 do mesmo artigo, pode ser dada pelo órgão de polícia criminal mediante autorização da autoridade judiciária competente ou quando haja urgência ou perigo na demora, devendo aquele, neste último caso, dar notícia imediata do facto à autoridade judiciária e transmitir-lhe o relatório previsto no artigo 253.º do Código de Processo Penal.

b) Pesquisa de dados informáticos

Dispõe o n.º 1 do artigo 15.º da Lei n.º 109/2009, de 15 de setembro[41], quanto à pesquisa de dados informáticos, que quando no decurso do processo se tornar necessário à produção de prova, tendo em vista a descoberta da verdade, obter dados informáticos específicos e determinados, armazenados num determinado sistema informático, a autoridade judiciária competente autoriza ou ordena por despacho que se proceda a uma pesquisa nesse sistema informático, devendo, sempre que possível, presidir à diligência.

Porém, o órgão de polícia criminal pode, nos termos do n.º 3 do mesmo artigo, proceder à pesquisa, sem prévia autorização da autoridade judiciária, quando:

a) A mesma for voluntariamente consentida por quem tiver a disponibilidade ou controlo desses dados, desde que o consentimento prestado fique, por qualquer forma, documentado;

b) Nos casos de terrorismo, criminalidade violenta ou altamente organizada, quando haja fundados indícios da prática iminente de crime que ponha em grave risco a vida ou a integridade de qualquer pessoa.

No caso referido na alínea b) a realização da diligência é, sob pena de nulidade, imediatamente comunicada à autoridade judiciária competente e por esta apreciada em ordem à sua validação (n.º 4 do artigo 15.º). Deve ser sempre elaborado e remetido à autoridade judiciária competente o relatório previsto no artigo 253.º do Código de Processo Penal.

c) Apreensão de dados informáticos

Dispõe o n.º 1 do artigo 16.º da Lei n.º 109/2009, de 15 de setembro, que quando, no decurso de uma pesquisa informática ou de outro acesso legítimo a um sistema informático, forem

[41] O conceito de dados informáticos encontra-se previsto no artigo 2.º, alínea b) da Lei n.º 109/2009, de 15 de setembro, trata-se de qualquer representação de factos, informações ou conceitos sob uma forma suscetível de processamento num sistema informático, incluindo programas aptos a fazerem um sistema informático executar uma função. Pode ser um documento eletrónico nos termos do Decreto-Lei n.º 290D/99, de 02 de agosto; um programa de computador protegido ou não nos termos do Decreto-Lei n.º 252/94 de 20 de outubro; dados pessoais nos termos da Lei n.º 67/98, de 26 de outubro ou dados de tráfego ou de localização celular nos termos da Lei n.º 41/2004, de 18 de agosto.

encontrados dados ou documentos informáticos necessários à produção de prova, tendo em vista a descoberta da verdade, a autoridade judiciária competente autoriza ou ordena por despacho a apreensão dos mesmos.

Tal como referido anteriormente, também neste caso, o órgão de polícia criminal pode efetuar apreensões, sem prévia autorização da autoridade judiciária, no decurso de pesquisa informática legitimamente ordenada e executada nos termos do artigo anterior, bem como quando haja urgência ou perigo na demora (n.º 2).

As apreensões efetuadas por órgão de polícia criminal são sempre sujeitas a validação pela autoridade judiciária (quer as devidamente autorizadas quer as realizadas como medida cautelar, sujeitas ao crivo da urgência ou perigo na demora), no prazo máximo de 72 horas (n.º 4).

2. Gestão e prática processual

Os modelos de organização judiciária num Estado de Direito Democrático privilegiam a separação de poderes do Estado; a independência do poder judicial e a ideia de investigação como atividade auxiliar da justiça, que atua na sua dependência.[42]

Em Portugal, nos termos do artigo 219.º da Constituição da República Portuguesa e do artigo 3.º, n.º 1, alínea c), da Lei n.º 47/86, de 15 de outubro (Estatuto do Ministério Público), o titular da ação penal é o Ministério Público.

Compete ao Ministério Público, nos termos do artigo 2.º da Lei n.º 49/2008, de 27 de agosto (Lei de Organização da Investigação Criminal – LOIC), dirigir a investigação criminal, na fase do inquérito, determinando e/ou promovendo o conjunto de ações necessárias e adequadas a comprovar a existência de crime, a determinar os seus agentes e a sua responsabilidade, a descobrir e recolher as provas em ordem à decisão sobre o exercício daquela ação penal.[43]
Aos órgãos de polícia criminal cabe-lhes coadjuvar as autoridades judiciárias em tudo quanto diga respeito às suas tarefas processuais penais. O princípio geral, dentro do inquérito, é o da atuação subordinada dos órgãos de polícia criminal ao Ministério Público, "criando-se entre eles uma relação de supremacia sem hierarquia (…) não se criando, porém, qualquer relação de serviço (…) A supremacia consiste no reconhecimento de um poder de directa orientação do Ministério Público sobre os órgãos de polícia criminal. O poder de orientação traduz-se num poder contínuo e permanente do Ministério Público emitir directivas que orientem e dirijam a atividade dos órgãos de polícia criminal quanto a todos os aspetos de que tenham sido encarregados. Ao poder de orientação são conaturais certos poderes de informação e controlo. Ao estabelecer a directa orientação, o CPP possibilita ao Ministério Público o concreto contacto com agentes (órgãos de polícia criminal)".[44]

[42] Brás, José, *in* Ciência, Tecnologia e Investigação Criminal, Almedina, 2016, p. 122.
[43] O artigo 3.º e seguintes da LOIC definem a natureza e as competências dos órgãos de polícia criminal.
[44] Cunha, Damião da *in* "O Ministério Público e os órgãos de polícia criminal", p. 147.

Seguindo o pensamento de Damião da Cunha[45], com o qual somos concordantes, o Código de Processo Penal "pretendeu estabelecer um processo interno circular de constante informação que garanta a responsabilidade "política" do Ministério Público durante o inquérito, baseado nos juízos de caráter técnico dos órgãos de polícia criminal".

Assim, os órgãos de polícia criminal, nos termos do Código de Processo Penal, só podem praticar atos de investigação ou atividades dirigidas aos fins do processual penal:

– Após despacho de delegação de competência do Ministério Público, que deve respeitar o estabelecido na LOIC, sem prejuízo de uma atuação imediata nos termos do despacho de natureza genérica previsto no n.º 4 do artigo 270.º do Código de Processo Penal e constante da Directiva n.º 1/2002, da PGR;

– Ao abrigo direto da lei, e antes de qualquer despacho de delegação de competência, sempre que, nos termos do artigo 249.º do Código de Processo Penal, haja necessidade de iniciar de imediato a investigação e praticar todos os atos cautelares necessários e urgentes para assegurar os meios de prova.[46]

Em sede de medidas cautelares, assume particular importância o artigo 253.º do Código de Processo Penal, o qual estabelece a necessidade dos órgãos de polícia criminal elaborarem um relatório onde mencionem, de forma resumida (mas minuciosa acrescentamos nós), as investigações levadas a cabo, os resultados das mesmas, a descrição dos factos apurados e as provas recolhidas, o que corresponde a uma forma de controlo do exercício da legalidade democrática pelas polícias, por parte do Ministério Público ou do Juiz de Instrução, trata-se de um referencial analítico para suportar as decisões a tomar pelas autoridades judiciárias.
Ainda que a medida cautelar levada a cabo pelo órgão de polícia criminal seja reduzida a auto (conforme estatuído no artigo 275.º do Código de Processo Penal), tal não se confunde com a obrigatoriedade de realização do referido relatório, que deve ser enviado juntamente com o(s) auto(s).[47]

O Código de Processo Penal e a demais legislação extravagante estabelecem prazos de comunicação das medidas cautelares adotadas pelos órgãos de polícia criminal, por forma a garantir o controlo da prática destes atos, através do circular constante de informação.

Quanto aos prazos de comunicação das medidas cautelares adoptadas, realçam-se os seguintes:

[45] *In* ob. cit., p. 148.
[46] Entende a doutrina que a prática de atos relativos aos fins do inquérito por iniciativa própria do órgão de polícia criminal depende, sempre, da verificação dos pressupostos de necessidade e urgência e, ainda assim, apenas em relação a matérias que não integram a reserva judiciária legal, ou cuja concretização não atinja direitos protegidos por lei (v. Parecer n.º 45/2012 do Conselho Consultivo do PGR).
[47] É ainda obrigatória a elaboração de relatório no caso de uso de arma de fogo por órgão de polícia criminal, que deve ser remetido para o Ministério Público, nos termos previstos no artigo 7.º do Decreto-Lei n.º 457/99, de 05 de novembro.

i) Imediatamente, no caso de realização de revistas e buscas como medida cautelar, nos termos do disposto nos artigos 174.º, n.º 6 e 251.º, n.º 2, do Código de Processo Penal;

ii) Imediatamente, quanto à preservação de dados informáticos, nos termos do disposto no n.º 2 do artigo 12.º da Lei n.º 109/2009, de 15 de setembro e quanto à pesquisa de dados informáticos, nos termos do artigo 15.º do mesmo diploma;

iii) o prazo de 48 horas, para comunicação ao Juiz de Instrução, da obtenção de dados de localização celular, nos termos do disposto no artigo 252.º-A, n.º 2, do Código de Processo Penal;

iv) O prazo de 48 horas, para convalidação judicial da suspensão de remessa de correspondência previsto no artigo 252.º, n.º 3, do Código de Processo Penal;

v) O prazo de 72 horas para efeitos de validação das apreensões efetuadas, previsto no artigo 178.º, n.º 5, do Código de Processo Penal;

vi) O prazo de 72 horas, para validação pela autoridade judiciária da apreensão de dados ou informáticos, nos termos do artigo 16.º da Lei n.º 109/2009, de 15 de setembro;

A lei ao estabelecer prazos precisos para efeitos de comunicação das medidas cautelares visa assegurar um controlo da legalidade dos atos praticados pelos órgãos de polícia criminal.
No que diz respeito à temática da gestão processual entendemos que constitui uma boa prática do Ministério Público, providenciar, aos órgãos de polícia criminal, as orientações necessárias em matéria de medidas cautelares e estar permanentemente disponível para resolver situações concretas.

Nessa medida, deverão ser estabelecidos "canais" diretos de comunicação entre o Ministério Público e os órgãos de polícia criminal.

IV. Hiperligações e referências bibliográficas

Hiperligações

Acórdão do Tribunal Constitucional n.º 456/93
Acórdão do Supremo Tribunal de Justiça, de 20.01.1998
Acórdão do Supremo Tribunal de Justiça, de 18.05.2006
Acórdão do Supremo Tribunal de Justiça, de 08.01.2014
Acórdão do Tribunal da Relação de Évora, de 12.04.2005
Acórdão do Tribunal da Relação de Évora, de 07.10.2008
Acórdão do Tribunal da Relação de Évora, de 05.02.2013
Acórdão do Tribunal da Relação de Évora, de 04.06.2013
Acórdão do Tribunal da Relação de Évora, de 16.02.2016
Acórdão do Tribunal da Relação de Lisboa, de 15.09.2011
Acórdão do Tribunal da Relação de Lisboa, de 22.06.2017

Acórdão do Tribunal da Relação do Porto, de 14.06.2006
Acórdão do Tribunal da Relação do Porto, de 24.01.2007
Acórdão do Tribunal da Relação do Porto, de 17.06.2015
Acórdão do Tribunal da Relação de Coimbra, de 07.06.2017
Parecer do Conselho Consultivo da PGR n.º 15/95
Parecer do Conselho Consultivo da PGR n.º 13/96
Parecer do Conselho Consultivo da PGR n.º 95/2003
Parecer do Conselho Consultivo da PGR n.º 28/2008
Parecer do Conselho Consultivo da PGR n.º 45/2012
Deliberação da Comissão Nacional de Proteção de Dados, n.º 61/2004

Referências bibliográficas

– Caetano, Marcelo, Manuel de Direito Administrativo, 3.ª reimpressão da 10.ª edição, Almedina, Coimbra, volume 2, p. 1170.

– Mesquita, Paulo Dá, *Repressão Criminal e Iniciativa Própria dos Órgãos de Polícia Criminal, in* Revista do Ministério Público, Lisboa, A.25 (98), Abr-Jun., 2004, p. 11.

– Albuquerque, Paulo Pinto de, *in* Código de Processo Penal anotado, 2010, Universidade Católica Editora, pp. 463, 671 e 690.

– Silva, Germano Marques da, curso de processo penal – II volume, 4.ª edição revista e atualizada, Lisboa, Editorial Verbo, 2008, pp. 190, 210 e 240.

– Soares, Paulo, *in* Meios de obtenção de prova no âmbito de medidas cautelares e de Polícia, 2017, 2.ª edição, p.135.
–
– *Brás, José, In* Investigação Criminal, a organização, o método e a prova, os desafios da nova criminalidade, 2009, Almedina, p. 231.

– Afonso, João José Rodrigues, *in* O regime legal da identificação – reflexões sobre o instituto da detenção para efeitos de identificação, Coimbra: Almedina, 2008, pp. 384-385.

– Carvalho, Jean Christophe dos Santos, dissertação de mestrado integrado em ciências policiais, "Da identificação de suspeitos e consequências jurídicas da recusa", 2014, pp. 57.

– Verdelho, Pedro, *in* CEJ, n.º 9, 1.º semestre de 2008.

– Lobo, Fernando Gama, *in* Código de Processo Penal Anotado, Almedina, 2015, p. 343.

– Brás, José, *in* Ciência, Tecnologia e Investigação Criminal, Almedina, 2016, pp. 122.

- Cunha, Damião da in "O Ministério Público e os órgãos de polícia criminal", pp. 147 e 148.

7.

Medidas cautelares e de polícia. Enquadramento jurídico, prática e gestão processual

Telmo Oliveira

CENTRO
DE ESTUDOS
JUDICIÁRIOS

7. MEDIDAS CAUTELARES E DE POLÍCIA. ENQUADRAMENTO JURÍDICO, PRÁTICA E GESTÃO PROCESSUAL

Telmo Oliveira

I. Introdução

Portugal é um Estado de direito democrático assente no respeito pela dignidade da pessoa humana, princípio que norteia (ou deve nortear) a atuação dos operadores judiciários – Órgãos de Polícia Criminal (OPC) e Autoridades Judiciárias (AJ). A Polícia, órgão da Administração Pública, e o Tribunal, órgão do poder judicial, encontram-se subordinados à Constituição e à lei.

À luz do Código de Processo Penal, o Ministério Público é o detentor da ação penal, sendo sua incumbência a direção da fase de inquérito. Para tanto, dispõe do auxílio dos OPC, sendo estes órgãos auxiliares da Administração da Justiça.

O legislador processual penal optou, assim, pelo modelo de dependência funcional para regular as relações entre o Ministério Público e os OPC, pois, embora detentores de autonomia organizacional, ao atuarem no âmbito do processo penal, fazem-no na dependência funcional da autoridade judiciária.

No entanto, sucede que, muitas vezes, os OPC têm de agir ainda antes da intervenção do Ministério Público, de modo a acautelarem os meios de prova existentes, fazendo-o, processualmente, ao abrigo das medidas cautelares e de polícia, que são, assim, um espaço de iniciativa própria dos OPC, ainda que sujeito a posterior convalidação.

Assim, as medidas cautelares e de polícia são instrumentos de grande importância, no âmbito da atuação dos OPC, e são poderes materiais que detêm para atuarem *motu* próprio, e o seu fundamento reside na necessidade de, imediatamente, após receberem a notícia do crime, e mesmo antes da intervenção do Ministério Público, de assegurarem os meios de prova, sob pena de, não o fazendo, os mesmos se perderem irremediavelmente.

A atividade dos OPC, no âmbito da coadjuvação com o Ministério Público, tem uma grande influência na posterior definição do objeto do processo. Por isso mesmo, não obstante atuarem sob dependência funcional e direção do MP, mediante a delegação de competências, podem fazer uso, perante a constatação dos requisitos de necessidade e urgência, das medidas cautelares e de polícia, sob pena de ser colocada em causa a descoberta da verdade material.

II. Objetivos

A elaboração do presente guia, subordinado às medidas cautelares e de polícia visou, em síntese e no essencial, criar uma ferramenta de trabalho, concisa e de fácil leitura, que forneça uma visão panorâmica acerca desta temática.

Dada a dimensão do presente guia, bem como a divergência doutrinária e jurisprudencial existente na tramitação das diversas medidas, não temos a ilusão de querer ser exaustivos ou esgotar todas as possíveis análises desta matéria. Pretendemos, apenas e tão-somente, fornecer o *esqueleto arquitetónico* destas ferramentas de uso policial.

Neste guia, apenas serão abordadas as medidas cautelares e de polícia previstas na lei processual penal, não sendo alvo de estudo todas as demais medidas na legislação avulsa, designadamente na Lei do Cibercrime, Lei de Segurança Interna ou na Lei das Armas.

III. Resumo

O presente Guia divide-se em duas partes fundamentais: uma referente ao enquadramento jurídico das medidas cautelares e de polícia, onde se analisa cada uma das medidas cautelares e de polícia, e a segunda referente à prática e gestão processual.

1. Enquadramento jurídico

1.1. Aproximação ao tema

As medidas cautelares e de polícia podem ser encaradas como um direito de primeira intervenção, uma vez que permitem a atuação dos OPC logo após terem obtido conhecimento da notícia do crime, mas à *priori* da intervenção das autoridades judiciárias.

Refere Maia Gonçalves: "*As medidas cautelares e de polícia…destinam-se a acautelar a obtenção de meios de prova, que sem elas poderiam perder-se, mediante uma tomada imediata de providências pelos órgão de polícia criminal, mesmo sem prévia autorização da autoridade judiciária competente, e isto pelo carácter urgente das diligências a praticar ou pela natureza perecível dos meios de prova a recolher*."[1]

As medidas cautelares e de polícia são, assim, atos de natureza pré-processual por serem levadas a cabo antes de iniciado o processo, podendo vir a ser integradas no processo após apreciação e validação da autoridade judiciária competente. Porém, a sua aplicação está sujeita a rigorosos requisitos previstos na lei processual penal, uma vez que não são levadas a cabo por encargo do Ministério Público, mas sim pela discricionariedade (não arbitrariedade) dos OPC, visando a eficácia da ação policial e através desta, a realização da justiça.

Segundo GERMANO MARQUES DA SILVA[2] "*Os actos regulados nos artigos 248.º a 253.º (...) não são ainda actos processuais, são actos de polícia (...). Trata-se de uma realidade extraprocessual conexa com a processual.*" No mesmo sentido, MAIA GONÇALVES: «Os actos cautelares necessários e urgentes para assegurar os meios de prova não são actos processuais, só vindo a ser integrados no processo se forem aceites e confirmados pela autoridade judiciária competente.»[3]

O legislador ao optar por introduzir as medidas cautelares e de polícia no Código de Processo Penal assumiu, clara e indubitavelmente, a opção de que a realização de uma investigação criminal, para ser eficaz, necessita de ter ao seu dispor meios de atuação rápidos, eficazes e eficientes para a aquisição da prova.

Quanto à concordância prática entre medidas cautelares e de polícia e compressão de direitos, responde Anabela Rodrigues: «*Sendo particularmente chocante qualquer solução que absolutizasse ou a finalidade de realização da justiça e descoberta da verdade material, ou a protecção dos direitos fundamentais das pessoas, a solução encontrada representa, sem*

[1] Maia Gonçalves, Código de Processo Penal Anotado, 12.ª edição, Almedina, pág. 512.
[2] Germano Marques da Silva: Curso de Processo Penal I, II, III, Editorial Verbo.
[3] Maia Gonçalves, Código de Processo Penal Anotado, 12.ª edição, Almedina, pág. 513.

dúvida, na situação concreta, a salvaguarda do máximo de conteúdo de cada uma das finalidades».[4]

1.2. Enquadramento constitucional

O art. 272.º da CRP, sob a epígrafe "Polícia", consagra a atividade policial, fazendo-o de forma generalista, isto é, abrangendo todas as modalidades de polícia: a polícia administrativa em sentido restrito, a polícia de segurança e a polícia judiciária[5]. Aqui, interessa-nos a polícia judiciária.

A principal razão de ser da Polícia é a manutenção da ordem e a preservação da segurança e da tranquilidade pública, onde se enquadra, por exigências de segurança geral, a prevenção criminal e a luta contra a criminalidade. Daí que se lhe permita, como órgão auxiliar da Justiça, a prática de atos processuais penais de competência própria, e atos processuais penais por determinação da autoridade judiciária competente em cada fase do processo em curso, ou seja, o Ministério Público, na fase do inquérito, o Juiz de Instrução Criminal, na fase da instrução, e o Juiz, na fase do julgamento.

As medidas cautelares e de polícia encontram respaldo constitucional no art. 272.º da CRP, especificamente no n.º 2 que estabelece: "*As medidas de polícia são as previstas na lei, não devendo ser utilizadas para além do estritamente necessário*."; acrescenta o n.º 3: "*A prevenção de crimes…só pode fazer-se com observância das regras gerais sobre polícia e com respeito pelos direitos liberdades e garantias…*".

De onde resulta que a Lei Fundamental as reveste de dois princípios estruturais: o princípio da tipicidade legal, estritamente conexo com o princípio da legalidade – na medida em que a lei penal deve ser prévia, estrita, certa e escrita – e o princípio da proibição de excesso.

Pegando nas palavras do acórdão do Tribunal Constitucional[6]: "*Os fins dos poderes funcionais assim atribuídos à polícia terão de ser actuados através de medidas previstas na lei (princípio da tipicidade legal), sendo que, por força da regra de correlação existente entre os meios e os fins, as medidas de polícia não devem ser utilizadas para além do estritamente necessário (princípio da proibição do excesso)*."

Estabeleceu assim o legislador constitucional a exigência da tipificação e do respeito pelos princípios da proporcionalidade, necessidade e adequação.

O princípio da tipicidade legal diz-nos que todas as medidas de polícia têm de ter assento legal, e devem traduzir-se em procedimentos individualizados, e com conteúdo suficientemente definido na lei, seja qual for a sua natureza, e só podem ser utilizadas pela polícia as que taxativamente obtiverem consagração legal. Assim, o OPC deve escolher as medidas que,

[4] Anabela Rodrigues, in Jornadas de Direito Processual Penal, pág. 71.
[5] Dada a tradicional distinção entre "*polícia administrativa*" e "*polícia judiciária*".
[6] Acórdão n.º 479/94, Rel. Conselheiro Diniz.

atendendo à situação em causa, estejam previstas no catálogo, pelo que lhe é vedada toda e qualquer modificação das medidas previstas na lei.

O princípio da proibição de excesso significa que a aplicação destas medidas apenas deve ser feita quando essas medidas sejam necessárias, devendo ser aplicadas proporcionalmente ao caso concreto, tendo em consideração a exigibilidade requerida.

Assim, tendo em conta de que estamos perante atuações policiais que são suscetíveis de causar lesões a direitos fundamentais exige-se, por isso, que seja justificada face à situação em concreto, que se faça um juízo de proporcionalidade entre o prejuízo que se pode provocar e os bens jurídicos que se visam tutelar, e que sejam as medidas idóneas a responder à situação em causa.

1.3. Enquadramento no âmbito do sistema processual

O tema das medidas cautelares e de polícia vem consagrado no Livro VI – Das fases preliminares, Título I – Disposições Gerais, Capítulo II, do Código de Processo Penal, sob a epígrafe: "Das medidas cautelares e de polícia". Atendendo à lógica do Código e à sua inserção no Livro respeitante às fases preliminares, podemos extrair que estamos perante atos de natureza pré-processual, isto é, que são levados a cabo ainda antes de iniciado o processo.

Assim, as medidas cautelares e de polícia, estão previstas no articulado dos preceitos 248.º a 253.º[7], sendo consequentemente estes e não outros, aqueles que consagram as medidas cautelares e de polícia, ainda que existam outras medidas de polícia na legislação avulsa.

1.3.1. Pressupostos de aplicação

A aplicação destas medidas tem como pressupostos os critérios de necessidade e urgência.

Segundo PAULO DÁ MESQUITA[8] estes critérios dizem respeito a "*um circunstancialismo que exige uma intervenção pronta do órgão de polícia criminal, sendo globalmente norteados por um princípio de eficácia que justifica que os órgãos de polícia criminal atuem sem prévia autorização do Ministério Público, o que apenas pode ocorrer dentro de rigorosos pressupostos legais*."

Por urgência deve entender-se uma situação que é séria e grave e que, portanto, necessita de resposta imediata dos OPC, sob pena de, não agindo neste tipo de situações, se colocar em causa a descoberta da verdade material.

[7] Art. 248.º - Comunicação da notícia do crime; art. 249.º - Providências cautelares quanto aos meios de prova; art. 250.º - Identificação de suspeito e pedido de informações; art. 251.º - Revistas e buscas; art. 252.º - Apreensão de correspondência; art. 252.º-A - Localização celular; art. 253.º - Relatório.
[8] Cf. Paulo Dá Mesquita, *Repressão Criminal e Iniciativa Própria dos Órgãos de Polícia Criminal,* p. 11.

Quanto ao pressuposto da necessidade significa que tal ação deve ser imprescindível e inevitável.

1.4. Os Órgãos de Polícia Criminal

O art. 1.º, al. c), do Código de Processo Penal define "*órgãos de polícia criminal*" como "*todas as entidades e agentes policiais a quem caiba levar a cabo quaisquer atos ordenados por uma autoridade judiciária ou determinados por este Código*."; São "autoridades de polícia criminal" os "*diretores, oficiais inspetores, e subinspectores de polícia e todos os funcionários policiais a quem as leis respetivas reconhecerem essa qualidade*", cfr. al. d), n.º 1, do Código de Processo Penal.

O legislador empregou aqui uma técnica de "duplo reenvio", pois remete-nos sempre, internamente, para a definição formal constante daquelas alíneas do n.º 1 e destas, externamente, para as leis orgânicas e estatutárias das diversas polícias.

Daquelas alíneas decorre igualmente que o Código de Processo Penal não atribui competências processuais especificamente a uma qualquer polícia, resultando antes que o estatuto de órgão e de autoridade de polícia criminal, e as respetivas competências, decorrem da lei, nomeadamente da Lei de Organização da Investigação Criminal (doravante LOIC)[9], e das leis próprias daqueles órgãos e autoridades.

1.4.1. Competência no âmbito do Processo Penal

As medidas cautelares e de polícia devem obedecer ao princípio da tipicidade (ou *numerus clausus*), *i.e.* só podem ser levadas a cabo as medidas cautelares e de polícia, no campo de atuação por iniciativa própria dos OPC, que se encontrem previstas na lei processual penal.

As medidas cautelares servem para assegurar os meios de prova, sendo que esta competência, precisamente por ter um carácter de garantia, é excecional pois, por regra, os OPC atuam por encargo da Autoridade Judiciária.

Esta competência própria (que se encontra expressa no art.º 55.º, n.º 2, do CPP) tem acuidade e pertinência, pois, "*o conhecimento de factos criminais (ou a sua suspeita) é, em grande parte, uma tarefa policial, dada, em especial, a grande mobilidade das forças policiais, a sua proximidade espacial e, ainda, e sobretudo, porque a forma de intervir quer na descoberta, quer logo após a descoberta do crime, pressupõe um conhecimento e um domínio de técnicas policiais (de criminalística) que só a polícia (órgãos de polícia criminal) possui.*"[10]

Nesta medida, os OPC têm um papel preponderante na investigação criminal, recaindo sobre os mesmos a função de salvaguarda dos meios de prova, procurando desta forma a

[9] Lei n.º 49/2008, de 27 de agosto.
[10] Cf. José Damião da Cunha, *O Ministério Público e os Órgãos de Polícia Criminal,* p. 137.

investigação criminal recolher, conservar, examinar e interpretar os indícios de forma a descobrir os seus autores, tal como localizar e apresentar provas pessoais que conduzam ao esclarecimento da verdade material dos factos.

A investigação criminal tem pois que estar alicerçada na eficácia da descoberta da verdade, na recolha de indícios e interpretação dos mesmos em tempo útil, visto que, de outra forma, os mesmos perder-se-iam irremediavelmente.

O art. 55.º, do Código de Processo Penal, sob a epígrafe "*Competência dos órgãos de polícia criminal*" determina nos números 1 e 2 que lhes compete, em 1.ª linha, coadjuvar as autoridades judiciárias com vista à realização das finalidades do processo e que lhes compete em especial e mesmo por iniciativa própria:

– Colher notícia dos crimes (1);
– Impedir quando possível as suas consequências (2);
– Descobrir os seus agentes (3);
– Levar a cabo os atos necessários e urgentes destinados a assegurar os meios de prova, daqui decorrendo as medidas cautelares e de polícia.

A autonomia técnica dos OPC assenta na utilização de um conjunto de conhecimentos e de métodos adequados de agir, enquanto a autonomia táctica consiste na possibilidade de opção pela melhor via e momento de cumprir as suas atribuições legais.

A subordinação funcional dos OPC perante o Ministério Público não invalida, todavia, que aqueles detenham o poder-dever de, em casos pontuais, praticar atos processuais no uso de uma competência própria e não meramente delegada, designadamente no que diz respeito às medidas cautelares e de polícia e de detenção, nos termos previstos nos artigos 248.º a 261.º do Código de Processo Penal, contudo trata-se de uma competência para a prática de determinados atos singulares, necessariamente precários e carentes de apreciação e validação judicial.

Isto significa que não existe qualquer ligação ao nível orgânico, preservando assim a autonomia técnica e táctica das polícias, conforme o disposto no art.º 2.º, n.º 5, da LOIC[11]. É, também, no n.º 6 do referido artigo que vem consagrada a distinção entre autonomia técnica – que "*assenta na utilização de um conjunto de conhecimentos e métodos de agir adequados*" e autonomia táctica – que "*consiste na escolha do tempo, lugar e modo adequados à prática dos atos correspondentes ao exercício das atribuições legais dos órgãos de polícia criminal*."

Cabe, assim, à autoridade judiciária dirigir, enquanto a polícia executa materialmente as tarefas de investigação, que, não obstante surgirem por via de delegação de competência genérica, específica ou presumida, aquela detém sempre os poderes de avocação, direção e devolução. Tanto assim é que o n.º 7 do art.º 2.º, da LOIC nos diz: "*os órgãos de polícia*

[11] Onde se diz: "As investigações e os actos delegados pelas autoridades judiciárias são realizados pelos funcionários designados pelas autoridades de polícia criminal para o efeito competentes, no âmbito da autonomia técnica e táctica necessária ao eficaz exercício dessas atribuições."

criminal impulsionam e desenvolvem, por si, as diligências legalmente admissíveis, sem prejuízo de a autoridade judiciária poder, a todo o tempo, avocar o processo, fiscalizar o seu andamento e legalidade e dar instruções específicas sobre a realização de quaisquer actos."

Assim, todos os atos de investigação por iniciativa própria dos OPC, que não se enquadrem no âmbito das medidas cautelares e de polícia que forem praticados antes de comunicada a notícia do crime ao Ministério Público ou, depois, mas que extravasem ou não se coadunem com o despacho de delegação de competências do Ministério Público, são ilegais, sendo inadmissível a posterior validação dos mesmos por parte do Ministério Público[12].

Daqui resulta que a prática de atos que não tenham natureza cautelar e urgente não podem ser convalidados pela AJ, quer tenham tido lugar antes da comunicação da notícia do crime, quer tenham extravasado os termos da delegação feita pelo MP, sendo consequentemente nulos.

Por isso, toda a atividade cautelar do órgão de polícia criminal (tenha ela lugar numa fase "pré-processual" ou durante o inquérito) deve ser sindicada pelo Ministério Público após a comunicação do relatório do órgão de polícia criminal.

DÁ MESQUITA[13] sintetiza da seguinte forma:

«*As autoridades e os órgãos de polícia criminal podem, por iniciativa própria que vise a prossecução de fins do processo penal, praticar:*

1- *Todos os atos cautelares necessários e urgentes para assegurar os meios de prova quanto a matérias que não integrem a reserva judiciária legal;*

2- *Os atos permitidos por previsão legal especial e dentro dos estritos pressupostos jurídico-normativos relativamente a matérias previstas nas reservas de competência das autoridades Judiciárias (v.g. artigos 174.º, n.º 5, 177.º, n.º 3, 178.º, n.º 4, 249.º, n.º 2, alínea c), 251.º, n.º 1, alínea a), do CPP).*»

Pegando nas palavras de DÁ MESQUITA[14]: "Em consequência, afigura-se incompatível com as competências de coadjuvação dos órgãos de polícia criminal atos de investigação por iniciativa própria insuscetíveis de ser enquadrados nas medidas cautelares e de polícia que:

(1) Sejam praticados em momento anterior à comunicação da notícia do crime, ou
(2) Realizados posteriormente àquela comunicação não respeitem os precisos termos (temporais e substanciais) da delegação de competência."

1.4.1.1. Atuação por iniciativa própria

[12] Neste sentido, Paulo Dá Mesquita, *Repressão Criminal e Iniciativa própria dos Órgãos*..., p. 21.
[13] Cf. Paulo Dá Mesquita no Parecer do Conselho Consultivo da PGR n.º 000452012.
[14] Idem.

A diferença estrutural entre os atos por iniciativa própria e os atos por encargo, reside na legitimação *ope legis* dos primeiros, fundada no perigo na demora, sendo os atos por iniciativa própria dos OPC conformados pelos princípios da necessidade e urgência da intervenção policial, e vinculados ao dever de ser transmitida imediata notícia à autoridade judiciária.

Dito de outro modo, ao OPC está vedada a prática cautelar e urgente dos atos que pertencem à reserva de competência exclusiva do juiz da instrução e do Ministério Público (artigos 268.º, 269.º, 270.º, n.º 2, e 290.º, n.º 2), cabendo todos os demais atos no âmbito da cláusula geral de competência cautelar fixada no art. 249.º, n.º 1, do Código de Processo Penal.

A prática de atos que não tenham natureza cautelar, não pode ser convalidada pela autoridade judiciária, quando eles tenham tido lugar antes da comunicação da notícia do crime ou, tendo ocorrido depois dela, tenham extravasado os termos da delegação feita pelo Ministério Público, padecendo de nulidade insanável (art. 119.º, al. a), b) e e), do CPP).

A iniciativa própria dos OPC surge na sequência da notícia do crime, isto é, a partir do momento em que tenham conhecimento da ocorrência de um crime devem, ainda antes de comunicarem à autoridade judiciária competente, executar as medidas cautelares e de polícia que se impuserem, fundando-se assim no *periculum in mora*.

Segundo PAULO DÁ MESQUITA[15], a iniciativa própria dos OPC deve conformar-se com dois vectores principais: por um lado, devem os atos cautelares e de polícia integrar as finalidades do processo penal, existindo uma substituição precária da autoridade judiciária por parte dos OPC e, por outro lado, os mesmos estão sujeitos aos pressupostos de necessidade e urgência, justificando-se assim a sua atuação sem prévio encargo por parte da autoridade judiciária, o que justificadamente só deverá ocorrer mediante "*rigorosos pressupostos legais*."

A relevância processual penal da iniciativa própria dos OPC compreende, assim, o surgimento da notícia do crime em sentido material e a realização de atos fundados numa pressuposta notícia do crime ou relacionados com uma notícia do crime.

A iniciativa própria dos órgãos de polícia criminal obedece a três vetores principais:

1 – Os atos cautelares e de polícia integram-se nas finalidades do processo penal, agindo as entidades policiais em substituição precária da autoridade judiciária;
2 – Os atos cautelares e de polícia dependem dos pressupostos de necessidade e de urgência, isto é, de um circunstancialismo que exige uma intervenção pronta da entidade policial, sendo globalmente norteados por um princípio de eficácia que justifica que atuem sem prévia solicitação da autoridade judiciária, o que apenas pode ocorrer dentro de rigorosos pressupostos legais.

[15] Paulo Dá Mesquita, *Repressão Criminal e Iniciativa Própria dos Órgãos*..., pág. 11.

3 – Deve ser respeitado o princípio da proporcionalidade, *i.e.*, atendendo ao caso concreto, de modo a que não sejam causados aos cidadãos danos mais graves do que os estritamente necessários e indispensáveis para a prossecução dos fins da aplicação dessas medidas.

1.4.1.2. Atuação por encargo da autoridade judiciária

A atuação por encargo de uma autoridade judiciária traduz-se na realização de atos por parte dos OPC que visam as finalidades do processo penal e que lhes foram imputados por encargo de uma autoridade judiciária, mediante um despacho de delegação de competência[16].

Em regra, os atos de investigação criminal praticados pelos OPC só podem ser levados a cabo depois da comunicação da notícia do crime ao MP, o que deve ocorrer no mais curto espaço de tempo, conforme decorre do art.º 248.º, do Código de Processo Penal.

É assim, sob a orientação do Ministério Público, que os OPC atuam na fase de inquérito, uma vez que este é o titular do mesmo[17].

Segundo JOSÉ DE FARIA COSTA, esta orientação corresponde á garantia da titularidade do inquérito por parte do MP e, ao contrário do que acontece com outras autoridades judiciárias, detém "*um poder de direta orientação sobre os órgãos de polícia criminal*" que implica, por um lado, contato direto com os agentes responsáveis pela investigação criminal e, por outro, a possibilidade permanente e contínua de emitir diretivas, orientando assim a investigação[18].

1.5. As medidas cautelares e de polícia

Após estas notas introdutórias, comecemos a viagem pelas medidas cautelares e de polícia, observando cada uma delas.

1.5.1. Comunicação da notícia do crime

Nos termos do art.º 248.º, n.ºs 1 e 2, do Código de Processo Penal:

Os OPC que tiverem notícia de um crime, por conhecimento próprio ou mediante denúncia, ainda que manifestamente infundada:

- Transmitem-na ao Ministério Público no mais curto prazo;
- Que não pode exceder 10 dias.

[16] *Vide* art. º 270.º do CPP.
[17] Conforme decorre do art.º 263º do CPP que nos diz no n.º 1 que "A direcção do inquérito cabe ao Ministério Público, assistido pelos órgãos de polícia criminal."
[18] José de Faria e Costa, *As relações entre o Ministério Público e a Polícia,* p. 234.

Em caso de urgência, a transmissão a que se refere o número anterior pode ser feita por qualquer meio de comunicação para o efeito disponível. A comunicação oral deve, porém, ser seguida de comunicação escrita (art. 248.º, n.º 3, do Código de Processo Penal).

Em contraponto à sobredita obrigação, resulta que não têm enquadramento legal quaisquer pré-inquéritos na sequência da aquisição da notícia do crime[19], pois a notícia do crime determina – sempre - o dever de comunicação ao Ministério Público e, para este órgão, a obrigatoriedade de abertura do processo penal[20].

A comunicação da notícia do crime tem lugar mesmo no caso de denúncia de crime manifestamente infundada, pois só ao Ministério Público compete avaliar, como *dominus* do inquérito, se a notícia do crime é ou não fundada.

Visa-se assim transmitir, no mais curto espaço de tempo possível a notícia do crime, para os efeitos do art. 48.º, do Código de Processo Penal e seguintes, a fim de o Ministério Público assumir imediatamente o conhecimento e a condução do inquérito.

Com a fixação de prazo para a comunicação, é manifesta a preocupação do legislador em garantir a inexistência de uma atividade investigatória pré-processual desenvolvida a "coberto" de medidas cautelares, assegurando assim uma rápida intervenção do Ministério Público e subsequente abertura de inquérito, onde formal e materialmente decorrerá a investigação na sua dependência funcional.

1.5.2. Das providências cautelares quanto aos meios de prova

Sem prejuízo do dever de comunicação "*no mais curto prazo*", o OPC pode proceder a atos cautelares necessários e urgentes "para assegurar os meios de prova". Trata-se, portanto, de uma competência cautelar que pode ser exercida mesmo antes de instaurado o inquérito.

Nos termos do art. 249.º, n.ºs 1 e 2, do Código de Processo Penal, compete aos OPC, mesmo antes de receberem ordem da autoridade judiciária competente para procederem a investigações, praticar os atos cautelares necessários e urgentes para assegurar os meios de prova, nomeadamente:

- Proceder a exame de vestígios, providenciando para evitar, quando possível, que os seus vestígios se apaguem ou alterem antes de serem examinados, proibindo, se necessário, a entrada ou o trânsito de pessoas estranhas no local do crime ou quaisquer outros atos que possam prejudicar a descoberta da verdade, [cfr art. 171.º, n.º 2, do Código de Processo Penal];
- Determinar que alguma ou algumas pessoas se não afastem do local do exame e obrigar,

[19] Não se confunda estes pré-inquéritos com as ações de prevenção previstas na Lei n.º 36/94, de 29/09, pois recolhidos elementos que confirmem a suspeita de crime, é obrigatória a comunicação e denúncia ao Ministério Público.
[20] Cfr. art. 262.º, n.º 2, do Código de Processo Penal: "Ressalvadas as exceções previstas neste Código, a notícia de um crime dá sempre lugar à abertura de inquérito."

com o auxílio da força pública, se necessário, as que pretenderem afastar-se a que nele se conservem enquanto o exame não terminar e a sua presença for indispensável, [cfr. art. 173.º, n.º 1, do Código de Processo Penal];
- Colher informações das pessoas que facilitem a descoberta dos agentes do crime e a sua reconstituição;
- Proceder a apreensões no decurso de revistas ou buscas ou em caso de urgência ou perigo na demora, bem como adotar as medidas cautelares necessárias à conservação ou manutenção dos objetos apreendidos.

Não obstante serem maioritariamente atividade pré-processual, no sentido em que são, em regra, atos praticados pelas polícias antes do inquérito ter início, as medidas cautelares e de polícia também podem ser desenvolvidas concomitantemente com as fases processuais iniciais (inquérito e instrução), sem prejuízo de deverem dar deles notícia imediata àquela autoridade. [cfr. art. 249.º, n.º 3, do Código de Processo Penal]

1.5.2.1. O exame

Refere o art. 171.º, n.º 1, do Código de Processo Penal que é por intermédio de exames, de pessoas**,** dos lugares e das coisas, que se inspecionam os vestígios que possa ter deixado o crime e todos os indícios relativos ao modo como e ao lugar onde foi praticado, às pessoas que o cometeram ou sobre as quais foi cometido.

Nos termos do n.º 2, "*Logo que houver notícia da prática de crime, providencia-se para evitar, quando possível, que os seus vestígios se apaguem ou alterem antes de serem examinados…*".

Exame é, pois, um meio de obtenção de prova, através do qual se inspecionam e registam documentalmente todos os vestígios que possa ter deixado o crime e todos os indícios relativos ao modo, como e ao lugar onde foi praticado, e às pessoas que o cometeram ou sobre as quais foi cometido. Este pode ser realizado em pessoas, lugares e em coisas (art. 171.º, n.º 1, do CPP), embora em sede de medidas cautelares e de polícia é concretizado essencialmente em lugares.

Os referidos exames consistem portanto numa inspeção, com recurso porventura a meios ou instrumentos técnicos ou científicos, que visa detetar a presença ou localização de vestígios e/ou indícios.

Ressalve-se que esta competência atribuída aos OPC, à semelhança das demais medidas cautelares e de polícia, não afasta a regra geral de direção do inquérito por parte do Ministério Público. Compreende-se, no entanto, que não estando essa autoridade judiciária presente, e em que a morosidade do seu contato poderia comprometer a investigação criminal, seja justificável a adoção das medidas convenientes à conservação e incolumidade da prova.

A realização de exame a quem não se quer a ele sujeitar, ou a coisa que não se quer facultar, está sempre dependente de decisão da autoridade judiciária competente.[21]

Neste caso, o exame segue o regime aplicável ao das perícias (art. 154.º, n.º 3 e 156.º, n.ºs 6 e 7, *ex vi* art. 172.º, n.º 2, do Código de Processo Penal), estando por isso sujeito a despacho do juiz, depois de ponderada a necessidade da sua realização, e tendo em conta a integridade pessoal do visado e a reserva da intimidade da sua vida privada.[22]

1.5.2.1.1. O exame ao local do crime

Este preceito consubstancia uma das mais importantes atividades que a investigação criminal comporta, posto que é um momento decisivo do processo de produção de prova, com reflexos a jusante no ulterior desenvolvimento da investigação criminal: a inspeção ao local do crime ou inspeção judiciária.

Como refere José Braz: «*…a inspeção judiciária concentra em si mesma desenvolvimento de um conjunto de medidas cautelares e de polícia, de meios de prova e meios de obtenção de prova, com particular destaque para os exames e, por isso, constitui uma das áreas nucleares da investigação criminal e um dos momentos decisivos do processo de produção de prova*.»[23]
É no estrito e adequado cumprimento das medidas cautelares e de polícia que se trata indelevelmente o sucesso de muitas investigações. Falhados estes procedimentos, comprometida fica muitas vezes a prova e, consequentemente o êxito da investigação, uma vez que se trata da aquisição da matéria criminal de forma imediata e em situações que não se repetem.

Como Heraclito diremos: "a água nunca passa duas vezes debaixo da mesma ponte". Ou seja, o que não for observado, analisado e recolhido naquela "cena de crime" não poderá voltar a sê-lo.

Saragoça da Matta refere a este propósito: «d*ada a extrema velocidade dos acontecimentos na nossa era" e a "volatilidade dos instrumentos e dos cenários" de crime, urge determinar as medidas cautelares e de polícia "efectivamente urgentes", de forma a garantir a resposta mais rápida possível em cenário de crime para permitir a efectivação da justiça*»[24].

[21] Art. 172.º, n.º 1, do Código de Processo Penal: "Se alguém pretender eximir-se ou obstar a qualquer exame devido ou a facultar coisa que deva ser examinada, pode ser compelido por decisão da autoridade judiciária competente. "
[22] A propósito dos exames realizados em pessoas, contra a sua vontade, veio o Tribunal Constitucional (Ac. TC n.º 155/2007, de 02/03/2007, proc. 695/06) esclarecer que, contendendo os exames coativos a pessoas (sem o seu consentimento), de forma relevante com os seus direitos fundamentais (arts. 25.º, 26.º e 32.º, n.º 4, da Constituição da República Portuguesa), necessitam, como tal, de prévia intervenção da autoridade judiciária competente, a saber, o juiz de instrução.
[23] Cf. José Braz, Investigação Criminal: a organização, o método e a prova, Os Desafios da Nova Criminalidade, Almedina, Outubro 2009, pág. 200.
[24] Saragoça da Matta, "Old ways and new needs? ou New ways and old needs?: uma perspectiva das reformas necessárias ao Processo Penal português", *in Revista do Ministério Público,* Ano 31, n.º 122 (Abril – Junho 2010), pp. 19-20.

Um significativo número de atos criminosos ocorre em lugar determinado. A ação e/ou omissão do agente criminoso, bem como o seu resultado, estabelecem com o local onde ocorrem e/ou com a vítima, uma relação de causa-efeito, suscetível, em muitos casos, de perdurar no tempo e de ser fisicamente identificável.

Já em 1932, o francês Edmond Locard[25], por muitos considerado o pai da moderna investigação criminal, enunciava no seu tratado de criminalística o conhecido princípio das trocas, segundo o qual, o autor do crime leva sempre consigo alguma coisa da vítima e/ou do local do crime onde agiu, dos instrumentos e objetos que utilizou, deixando nestes, algo de si mesmo.

Assim, a inspeção ao local do crime ou inspeção judiciária traduz, normalmente, o primeiro contato da investigação criminal com muitos dos eventos criminosos que constituem objeto da sua atividade, permitindo, desde logo, a obtenção, através de procedimentos típicos e sistemáticos, de valiosa informação, tendente à recriação da factualidade material que irá suportar e condicionar toda a atividade investigatória.

A grande importância deste exame é pois que o local do crime é precário, frágil e irrepetível, sendo que a sua integridade está permanentemente ameaçada, quer pela natureza precária dos próprios vestígios[26], quer por múltiplos outros factores exteriores, humanos e/ou naturais[27], voluntários ou involuntários que lhe são potencialmente hostis. Assim, torna-se fundamental a sua manutenção e preservação, bem como a adopção de condutas que assegurem a inviolabilidade dos elementos obtidos e que servirão como meio de prova.

1.5.2.2. Recolha de informações

Esta atividade policial justifica-se por razões de urgência na recolha de informações, que podem ser preponderantes para o apuramento da verdade material dos factos.
Essa colheita de informações pode ter como fonte, as pessoas que presenciaram os factos penalmente relevantes, ou que, por quaisquer outras razões, possam fornecer dados úteis, suscetíveis de esclarecer os factos, ou conduzir à identificação de suspeitos.

Tratando-se de mera "recolha de informações", não impende sobre essas pessoas qualquer imposição que as obrigue a prestar informações.

1.5.2.3. Apreensões cautelares

Nos termos do art. 249.º, n.º 2, al. c), do Código de Processo Penal é atribuída competência aos OPC para procederem "*a apreensões no decurso de revistas ou buscas ou em caso de urgência ou perigo na demora, bem como adoptar as medidas cautelares necessárias à conservação ou manutenção dos objectos apreendidos*."

[25] Princípio das trocas (Locard Exchange principle).
[26] Imagine-se vestígios lofoscópicos (vulgarmente referidos como impressões digitais) que mais não são do que suor facilmente evaporável.
[27] Por exemplo, pluviosidade que destrói muitos vestígios.

As apreensões vêm reguladas nos artigos 178.º e seguintes do Código de Processo Penal, referindo o n.º 1: "*São apreendidos os instrumentos, produtos ou vantagens relacionados com a prática de um facto ilícito típico, e bem assim todos os objetos que tiverem sido deixados pelo agente no local do crime ou quaisquer outros suscetíveis de servir a prova*."

Conforme resulta do n.º 3: as apreensões são autorizadas (quando solicitadas pelo OPC), ordenadas (quando é a própria autoridade judiciária que o determina) ou validadas (quando é o OPC que toma a iniciativa de apreensão) por despacho da autoridade judiciária, as quais, nos termos do n.º 6, são sujeitas a validação pela autoridade judiciária, no prazo máximo de setenta e duas horas.

1.5.3. Identificação de suspeito e recolha de informação

O art. 250.º do Código de Processo Penal consagra a possibilidade de identificar um suspeito e do poder de os OPC solicitarem informações, não apenas a todas as pessoas suscetíveis de fornecerem informações úteis, mas também ao suspeito.

1.5.3.1. A identificação do suspeito

A obrigação de um suspeito perante um determinado OPC, nos termos e para os efeitos do art. 250.º, do Código de Processo Penal, é uma medida cautelar e de polícia, estando a sua aplicação subordinada aos pressupostos e limites que condicionam toda a atividade policial, com especial relevância do princípio da proibição do excesso, devendo, por isso, obedecer aos requisitos da necessidade, exigibilidade e proporcionalidade.

Nos termos do n.º 1 do art. 250.º, os OPC podem proceder à identificação de qualquer pessoa:

- Encontrada em lugar público; aberto ao público ou, sujeito a vigilância policial.
- Sempre que sob ela recaiam fundadas suspeitas:
- Da prática de crimes,
- Da pendência de processo de extradição ou de expulsão,
- De que tenha penetrado ou permaneça irregularmente no território nacional ou,
- De haver contra si mandado de detenção.

Antes de procederem à identificação, devem [art. 250.º, n.º 2, Código de Processo Penal]:

- Fazer prova da sua qualidade,
- Comunicar ao suspeito os motivos que fundamentam a obrigação de identificação,
- Indicar quais os meios pelos quais este se pode identificar.

O suspeito pode identificar-se mediante a apresentação de um dos seguintes documentos [art. 250.º, n.º 3, alíneas a) e b), do Código de Processo Penal]:

1. Se o suspeito for cidadão português:
- Bilhete de identidade / Cartão do Cidadão, ou Passaporte.

2. Se for cidadão estrangeiro:
- Através do título de residência; Bilhete de identidade, Passaporte ou documento que o substitua.

Na impossibilidade de apresentação dos documentos referidos, o suspeito pode-se identificar apresentando documento original, ou cópia autenticada, que contenha o seu nome completo, a sua assinatura e a sua fotografia. [art. 250.º, n.º 4, Código de Processo Penal]

Se não for portador de nenhum documento de identificação, o suspeito pode identificar-se por um dos seguintes meios [art. 250.º, n.º 4, alíneas a), b) e c), do Código de Processo Penal]:

- Comunicação com uma pessoa que apresente os seus documentos;
- Deslocação, acompanhado pelos OPC, até ao local onde se encontram os seus documentos;
- Reconhecimento da sua identidade por uma pessoa que possa ser identificada pelos meios já referidos e que garanta a veracidade dos dados pessoais fornecidos pelo suspeito.

Por fim, esgotados os meios referidos até então, e não sendo possível a identificação do suspeito, podem os órgãos de polícia criminal [art. 250.º, n.º 6, do Código de Processo Penal]:

- Conduzir o mesmo até ao posto policial mais próximo e fazê-lo permanecer nesse local somente pelo tempo estritamente necessário, nunca superior a seis horas[28][29], para que seja efetuada a sua identificação e, se necessário, pode ser levado a realizar provas dactiloscópicas, fotográficas ou de natureza análoga e pode-lhe ser pedido que indique residência através da qual possa ser encontrado e receber comunicações.

Segundo Manuel Guedes Valente[30], este prazo de seis horas começa "*a contar desde o momento exacto em que a pessoa fica privada do seu ius ambulandi, ou seja, desde que o cidadão foi interceptado pelo OPC.*"

Tais atos de identificação são sempre reduzidos a auto e as provas de identificação dele constantes são destruídas na presença do identificando, a seu pedido, se a suspeita não se confirmar. [art. 250.º, n.º 7, do Código de Processo Penal]

Será sempre facultada ao identificando possibilidade de contatar com pessoa da sua confiança. [art. 250.º, n.º 9, do Código de Processo Penal]

[28] O período de detenção até seis horas tem cobertura constitucional - art. 27.º, n.º 3, alínea g), da CRP.
[29] No caso de menor entre os 12 e os 16 anos a permanência em posto policial não pode exceder as 3 horas - art. 50.º, alínea b), da Lei Tutelar Educativa (Lei n.º 166/99, de 14/09.
[30] Cfr. Manuel Guedes Valente, Teoria Geral do Direito Policial, pág. 250.

Havendo condução à esquadra deve ser elaborado auto de identificação, cfr. art. 250.º, n.º 7, do Código de Processo Penal. Nos restantes casos, basta um Relatório dando conhecimento da diligência efetuada, nos termos do art. 253.º do Código de Processo Penal, onde bastará referir que se procedeu à identificação das pessoas que se encontravam no local, não havendo necessidade de referir as respetivas identidades. Em ambos os casos, deve ser dado conhecimento do Ministério Público.

1.5.3.2. Informações relativas ao crime

Os OPC podem pedir [art. 250.º, n.º 8, do Código de Processo Penal]:

- Ao suspeito,
- A quaisquer pessoas susceptíveis de fornecerem informações úteis, e deles receber, sem prejuízo, quanto ao suspeito, do disposto no art. 59.º, informações relativas a um crime e, nomeadamente, à descoberta e à conservação de meios de prova que poderiam perder-se antes da intervenção da autoridade judiciária.

Se durante o pedido de informações ao suspeito se tornar fundada a suspeita da autoria de crime, a diligência deve ser imediatamente suspensa, e aquele constituído arguido. Se as diligências se dirigem à comprovação da imputação, tem aquele direito, a seu pedido, de ser constituído arguido. [art. 250.º, n.º 8, e 59.º, números 1 e 2, do Código de Processo Penal]

1.5.4. Revistas e buscas – art. 251.º do Código de Processo Penal

Revistas e buscas são meios de obtenção da prova.

Há lugar a revista quando existem indícios de que alguém oculta, na sua pessoa, quaisquer objetos relacionados com um crime ou que possam servir de prova – art. 174.º, n.º 1, do CPP.

Já se existirem indícios de que, quaisquer objetos relacionados com um crime ou que possam servir de prova, ou de que o arguido ou outra pessoa que deva ser detida, se encontram em lugar reservado ou não livremente acessível ao público, será ordenada busca – art. 174.º, n.º 2, do CPP.

Em regra, as revistas e as buscas são autorizadas ou ordenadas pela autoridade judiciária competente (art. 174.º, n.º 3, do Código de Processo Penal), contudo a lei permite que, em situações excecionais, também os OPC possam lançar mão desses meios de obtenção de prova.

As buscas e as revistas constituem medidas excecionais, porque restritivas de direitos fundamentais dos cidadãos, desde logo no que concerne ao domicílio e à reserva da intimidade da vida privada, donde têm que ser necessárias, adequadas e proporcionais à

gravidade dos crimes em investigação, nos termos dos arts. 18.º, n.º 2, 26.º, 32.º e 34.º, da CRP, e 191.º, 192.º e 378.º, do Código Penal.

Como medida cautelar, e sem prejuízo do disposto nos artigos 174.º, n.º 5[31] e 177.º, n.º 3[32] do Código de Processo Penal, os OPC podem, sem a prévia autorização da autoridade judiciária [art. 251.º, n.º 1, alíneas a) e b), do Código de Processo Penal]:

i. Proceder a revistas a suspeitos em caso de fuga iminente ou de detenção, e a buscas no lugar em que se encontrarem, salvo tratando-se de busca domiciliária ➔ Pressuposto: Sempre que tiverem fundada razão para crer que neles se ocultam objetos relacionados com o crime, suscetíveis de servirem a prova e que de outra forma poderiam perder-se;

ii. À revista de pessoas que tenham de participar ou pretendam assistir a qualquer ato processual; Que, na qualidade de suspeitos, devam ser conduzidos a posto policial, ➔ Pressuposto: Sempre que houver razões para crer que ocultam armas ou outros objectos com os quais possam praticar actos de violência.

Tais buscas e revistas são, sob pena de nulidade[33], imediatamente comunicadas ao juiz de instrução e por este apreciada em ordem à sua validação [artigos 251.º, n.º 2, e 174.º, n.º 6, do Código de Processo Penal], sem prejuízo de serem ainda referidas no Relatório referido no art. 253.º CPP.

Em anotação a este artigo, MAIA GONÇALVES refere: «No caso deste art. 251.º, trata-se de uma nítida medida cautelar, de uma actividade típica de polícia, visando evitar a perda de um meio de prova que poderá desaparecer se não forem tomadas cautelas imediatas, por parecer iminente a fuga de um suspeito ou por existir fundada razão de que o lugar onde ele se encontra oculta objectos relacionados com o crime, susceptíveis de servir a prova, e que de outra forma poderiam perder-se.»[34]

1.5.5. Apreensão de correspondência – art. 252.º do Código de Processo Penal

Nos casos em deva proceder-se à apreensão de correspondência, os OPC:

a) Transmitem-na intata ao juiz que tiver autorizado ou ordenado a diligência. [art. 252.º, n.º 1, Código de Processo Penal].

[31] Os OPC podem realizar revistas e buscas não domiciliárias sem autorização da autoridade judiciária nos casos de: a) de terrorismo, criminalidade violenta ou altamente organizada, quando haja fundados indícios da prática iminente de crime que ponha em grave risco a vida ou integridade física de qualquer pessoa; b) Quando os visados consintam na diligência, desde que o consentimento fique documentado; c) Quando da detenção em flagrante delito por crime a que corresponda pena de prisão.
[32] Nas buscas domiciliárias, em casos de terrorismo, criminalidade especialmente violenta ou altamente organizada, entre as 07h00 e as 21h00, quando haja consentimento do visado e aquando de detenção em flagrante delito, estas entre as 21h00 e as 07h00.
[33] Nos termos do art.º 120, n.ºs. 1 e 3, al. c), do Código de Processo Penal, dependente de arguição até ao encerramento do debate instrutório ou até cinco dias após a notificação do despacho que designa dia para julgamento.
[34] Maia Gonçalves, Código de Processo Penal Anotado, 12.ª edição, Almedina, pág. 518.

b)Tratando-se de encomendas ou valores fechados suscetíveis de serem apreendidos, sempre que tiverem fundadas razões para crer que eles podem conter informações úteis à investigação de um crime ou conduzir à sua descoberta, e que podem perder-se em caso de demora, os órgãos de polícia criminal informam do facto, pelo meio mais rápido, o juiz, o qual pode autorizar a sua abertura imediata. [artigos 252.º, n.º 2, Código de Processo Penal].

c) Sempre que tiverem fundadas razões para crer que podem conter informações úteis à investigação de um crime ou conduzir à sua descoberta, e que pode perder-se em caso de demora, podem ordenar a suspensão da remessa de qualquer correspondência nas estações de correios e de telecomunicações, devendo ser informado o Juiz de imediato para conhecimento e validação no prazo de 48 horas. [artigos 252.º, n.º 3, Código de Processo Penal].

Esta suspensão de correspondência pode ser levada a cabo pelos OPC, apenas nos casos previstos no n.º 1 do art.º 179.º do CPP, ou seja, nos casos em que seria legítimo ao Juiz que ordenasse a sua apreensão.

Se, no prazo de 48 horas, a ordem não for convalidada por despacho fundamentado do juiz, a correspondência é remetida ao destinatário.

1.5.6. Localização celular – art. 252.º-A, do Código de Processo Penal

A localização celular prevista no art. 252.º-A, do CPP, não se confunde com a interceção prevista no art. 189.º, n.ºs 1 e 2, do Código de Processo Penal. É assim configurada no processo penal numa perspetiva dual: por um lado, é um meio de obtenção de prova, previsto no art. 189.º, n.º 2; por outro, é uma medida cautelar e de polícia, prevista no art. 252.º-A, que não é verdadeira interceção telefónica, mas apenas uma medida cautelar e de polícia consistente apenas numa localização celular.

As autoridades judiciárias e as autoridades de polícia criminal podem [artigos 252.º-A, do Código de Processo Penal]:

- Obter dados sobre a localização celular quando:

a) Forem necessários para afastar perigo para a vida, ou
b) De ofensa à integridade física grave.

Se os dados sobre a localização celular previstos no número anterior:

- Se referirem a um processo em curso, a sua obtenção deve ser comunicada ao juiz no prazo máximo de 48 horas.
- Se não se referirem a nenhum processo em curso, a comunicação deve ser dirigida ao juiz da sede da entidade competente para a investigação criminal.

É nula a obtenção de dados sobre a localização celular com violação do disposto nos números anteriores. [artigos 252.º-A, n.º 4, do Código de Processo Penal]

A iniciativa compete às autoridades policiais ou ao Ministério Público (e também ao juiz, em fase de instrução). Os n.ºs 2 e 3 do normativo citado supõe sempre a intervenção do juiz de instrução, a quem a iniciativa deve ser comunicada a medida no prazo máximo de 48 horas sob pena de a mesma ser nula (n.º 4).

Assim, esquematicamente, pressupõe-se para a aplicação do art. 252.º-A:

- A existência de uma "vítima" no sentido da al. c) do n.º 4 do art. 187.º do Código de Processo Penal;
- A existência de um perigo (em sentido amplo, risco, ameaça, situação potenciadora de violação da vida e integridade física) para a vida e a integridade física grave de alguém;
- A possibilidade de a localização celular obviar à concretização desse perigo.

Tão somente. Não se exige a existência de um processo nem a definição de um suspeito dos supostos crimes.

O n.º 1 deste preceito prevê a obtenção de dados sobre localização celular quando *forem necessários para afastar perigo para a vida ou de ofensa à integridade física grave*. O termo "*para afastar perigo*" significa que a ação que coloca os bens jurídicos sob ameaça iminente ainda não se consumou, pelo menos na íntegra, e que os bens jurídicos sob ameaça poderão vir a ser irremediavelmente sacrificados.

Também o legislador, ao referir-se a "*quando eles forem necessários*", dá-nos a indicação de que sempre que os dados sobre localização celular forem essenciais para determinar a localização do agressor e da vítima (sempre que necessário para eliminar o perigo) se fará recurso a tal medida.

Segundo PAULO PINTO DE ALBUQUERQUE[35], este artigo tem duas partes distintas: uma conexionada com matéria de prevenção criminal e outra com matéria processual penal. Assim, o n.º 2 do art.º 252.º-A, do CPP está ligada ao âmbito processual penal, enquanto o n.º 3 diz respeito a matéria da "*pura prevenção criminal*."

1.5.7. Relatório

Como já foi referido, as medidas cautelares e de polícia são instrumentos colocados à disposição dos OPC de modo a preservar e a adquirir meios de prova, mesmo antes da intervenção da Autoridade Judiciária.

[35] Cf. Paulo Pinto de Albuquerque, *Comentário do Código de Processo Penal,* Universidade Católica Editora, 4.ª ed., 2011, pág. 670.

Esta necessidade decorre da urgência de agir, sob pena de se perder a prova, se as medidas não forem imediatamente executadas, por demora da Autoridade Judiciária. Assim, não é possível sujeitar estas medidas ao controlo judicial e à autorização prévia, requisitos para a aplicação dos meios de obtenção de prova.

No entanto, e dadas as circunstâncias descritas, os OPC devem elaborar um relatório, sempre que levarem a cabo a aplicação das medidas cautelares e de polícia, o qual funciona como instrumento de controlo da autoridade judiciária sobre as diligências cautelares desenvolvidas pelos OPC.

Os OPC que procederem a exames, apreensões, identificações, revistas, buscas, apreensões de correspondência, e à obtenção de dados sobre localização celular elaboram um relatório onde mencionam, de forma resumida [art. 253.º, n.º 1, do Código de Processo Penal]: as investigações levadas a cabo, os resultados das mesmas, a descrição dos factos apurados e as provas recolhidas.

O relatório é remetido ao Ministério Público ou ao juiz de instrução, conforme os casos. [art. 253.º, n.º 2, do Código de Processo Penal]

Esclarece-se que, quando a diligência só puder ser ordenada ou autorizada pelo Juiz, aquele relatório deve ser-lhe remetido, independentemente da fase processual. Igualmente no caso de as diligências dos OPC terem ocorrido na pendência do processo e dentro da fase da instrução, tal relatório deverá ser sempre remetido ao Juiz de Instrução. Não assim, se praticadas antes do início do processo ou durante o inquérito, caso em que o relatório é remetido ao MP, ressalvados os casos de competência exclusiva do Juiz.

2. Prática e gestão processual

2.1. Introdução

O legislador, ao autonomizar as medidas cautelares e de polícia, procurou alargar a competência dos OPC para além dos limites da coadjuvação, mas sem permitir que haja uma autonomização da atividade policial[36]. No entanto, estas medidas não deixam de gozar de um certa autonomia uma vez que fogem ao poder de orientação do Ministério Público.

Decorre do art. 262.º, do Código de Processo Penal, sob a epígrafe "Finalidade e âmbito do inquérito", que o inquérito: *"compreende o conjunto de diligências que visam investigar a existência de um crime, determinar os seus agentes e a responsabilidade deles e descobrir e recolher as provas, em ordem à decisão sobre a acusação."*

2.2. A notícia de crime

[36] Damião da Cunha. *O Ministério Público e os Órgãos de Polícia Criminal no novo Código de Processo Penal.* Porto, pág. 127.

Sendo comunicadas medidas cautelares e de polícia, que não dêem origem à abertura de processo-crime, as mesmas deverão ser registadas de acordo com o anexo I da Ordem de Serviço n.º 4/2015 e seguidamente arquivadas.

A aquisição da notícia por parte do Ministério Público, também resulta do art. 248.º, n.º 1, do Código de Processo Penal, uma vez que, os OPC que tiverem notícia de um crime, transmitem-na ao Ministério Público no mais curto prazo, que não pode exceder os 10 dias.

Recebida essa notícia de crime, em regra, a mesma dá sempre lugar à abertura de inquérito, conforme resulta do art. 262.º, n.º 2, do Código de Processo Penal. No entanto, a legitimidade do Ministério Público para promover a ação penal está limitada pelas regras previstas nos artigos 49.º e 50.º, do Código de Processo Penal.

A referência ao prazo de 10 dias foi imposta pela Lei 48/2007, de 29 de Agosto, de 29 de Agosto, pois até aí apenas era referido que essa comunicação deveria ocorrer no mais curto prazo.

Quanto a este prazo levantam-se três questões:

1.ª: sua natureza: assume uma natureza meramente ordenadora, pelo que o seu não cumprimento, «rectius» a não comunicação atempada por parte do OPC, constitui mera irregularidade, que ficará sanada com a intervenção direta do Ministério Público no processo.

2.ª: Antes da comunicação ao Ministério Público, os OPC apenas podem praticar atividades que caibam na previsão dos artigos 249.º a 252.º-A do Código de Processo Penal? A resposta é negativa, pois o referido preceito permite suficiente margem de manobra para que se entenda nele estar contida a possibilidade de recolha de informação no sentido de confirmar comunicação de prática de atos ilícitos e de comprovar identidade e localização dos seus agentes, assim como o local da prática daqueles atos.

3.ª: A expressão "no mais curto prazo" significa menos que o prazo de 10 dias ali previsto: a resposta também é negativa; os OPC podem praticar atos de recolha de informação que comprove e os elucide quanto ao teor e credibilidade das denúncias recebidas[37].
Em sentido contrário, Paulo Pinto de Albuquerque: «*Este prazo não é consentâneo com a Constituição da República Portuguesa nem com outros prazos estabelecidos pelo próprio Código de Processo Penal. A CRP é incompatível com acções de prevenção criminal por iniciativa própria do órgão de polícia criminal, com recolha de informação por tempo*

[37] Neste sentido, Acórdão TRE, Proc. 235/14.9JELSB, Rel. João Gomes de Sousa: "1 - A informação policial recebida pela polícia portuguesa não é uma "denúncia", sim isso mesmo, uma informação policial que necessita de ser confirmada.2 - O artigo 248.º n.º 1 do Código de Processo Penal permite – no prazo ali indicado e sem abuso policial - a recolha de informação que vise assegurar a prática de actos cautelares previstos nos artigos 249.º a 252.º do diploma.

indeterminado…por violação da reserva da vida privada dos visados pelas ditas acções e do princípio da proporcionalidade.»[38]

«*Resulta do exposto que quer a CRP quer o próprio CPP supõem um prazo de comunicação da notícia do crime mais apertado do que dez dias. É intolerável esta "zona de semi-clandestinidade", por atentar contra a competência constitucional do Ministério Público de exercício da acção penal e de domínio sobre o inquérito e as garantias da defesa*.»[39]

E conclui, referindo que «*Portanto, são inconstitucionais os artigos 243.º, n.º 3, 245.º, e 248.º, n.º 1, por violarem os artigos 26.º, n.º 1, 32.º. n.ºs 1 e 5, e 219.º, n.º 1, na medida em que permitem a dilação da comunicação da notícia do crime pelo órgão de polícia criminal ao Ministério Público por período até 10 dias contados desde o dia em que o órgão de polícia criminal teve a notícia do crime.*»[40]

Acresce que este prolongamento da comunicação da notícia do crime não tem qualquer justificação prática ou logística, uma vez que "atendendo à actual dotação de meios técnicos, o mais curto prazo implica que sendo iniciadas as diligências investigatórias pelo órgão de polícia criminal, no mínimo a denúncia deva ser de imediato transmitida por fax ao Ministério Público, pois todos os postos policiais e serviços do MP estão equipados com meios de telecópia."[41]

2.3. Das validações

Como vimos, as medidas cautelares e de polícia carecem de validação por parte da autoridade judiciária.

Vejamos:

- ✓ Se se tratar de uma validação de apreensão, deverá sê-lo pelo magistrado do Ministério Público, ao abrigo do art. 178.º, n.º 6, do Código de Processo Penal.
- ✓ Se essa atividade cautelar do órgão de polícia criminal tiver lugar durante a instrução, ela deve ser sindicada pelo juiz de instrução após a comunicação do relatório do órgão de polícia criminal (artigo 253.º, n.º 2).
- ✓ No caso de suspensão de remessa da correspondência (artigo 252.º, n.º 3), revistas e buscas em caso de terrorismo, criminalidade violenta ou altamente organizada (artigo 174.º, n.º 5), revista de suspeito em caso de fuga iminente ou de detenção e busca não domiciliária em lugar em que ele se encontrar (artigo 251.º, n.ºs 1, al. a), e 2, a sindicância pertence em exclusivo ao juiz de instrução, tenham estes atos cautelares lugar numa fase "pré-processual", durante o inquérito ou na fase de instrução.

[38] Paulo Pinto de Albuquerque, Comentário do Código de Processo Penal à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem, 2.ª edição, Universidade Católica Editora, 2008, pág. 644.
[39] Idem, pág. 645.
[40] Idem, pág. 645.
[41] DÁ MESQUITA, Direcção do inquérito penal e garantia judiciária, Coimbra Editora, 2003, pág. 150.

- ✓ No caso de revista cautelar de pessoa que tenha de participar ou pretenda participar em acto processual, a sindicância pertence à autoridade judiciária que presidir ao acto (artigo 251.º, n.º 1, al. b), 1.ª parte, e n.º 2.
- ✓ No caso da revista cautelar de suspeito que deva ser conduzido a posto policial, a sindicância pertence ao Ministério Público se o ato cautelar tiver lugar numa fase "pré-processual" ou durante o inquérito e pertence ao juiz de instrução se o ato cautelar tiver lugar na fase de instrução (art 251.º, n.º 1, al. b), 2.ª parte, e 2.

2.4. A competência para a investigação

Conforme resulta do texto constitucional, ao Ministério Público compete representar o Estado e defender os interesses que a lei determinar, bem como participar na execução da política criminal definida pelos órgãos de soberania, exercer a acção penal orientada pelo princípio da legalidade e defender a legalidade democrática[42], formulação que é replicada pelo Estatuto do Ministério Público.

Resulta do art. 263.º, do Código de Processo Penal que *"a direcção do inquérito cabe ao Ministério Público, assistido pelos órgãos de polícia criminal"*, os quais para esse efeito *"actuam sob a directa orientação do Ministério Público e na sua dependência funcional"*.

Resulta, por outro lado, do referido art. 270.º, n.º 1, do Código de Processo Penal, que *"o Ministério Público pode conferir a órgãos de polícia criminal o encargo de procederem a quaisquer diligências e investigações relativas ao inquérito".* Acrescentando o n.º 3 do mesmo artigo que *"(…) a delegação a que se refere o n.º 1 pode ser efectuada por despacho de natureza genérica que indique os tipos de crime ou os limites das penas aplicáveis aos crimes em investigação".*

Assim, recebidos os autos, o magistrado do Ministério Público deve ponderar se efetua ele próprio a investigação do crime em causa, ou se, alternativamente, delega a competência para a investigação em órgão de polícia criminal[43], nos termos do artigo 270.º, n.º 1, do Código de Processo Penal.

De qualquer forma, compete ao magistrado do Ministério Público estabelecer e concretizar a estratégia de investigação que se revele mais adequada ao caso em investigação, sendo certo que poderá contar, para esse desiderato, com a intervenção dos OPC que tenham intervenção directa no apuramento da verdade dos factos.

Seguindo de perto o que dispõe a Circular n.º 6/2002 da Procuradoria-Geral da República, em especial, o seu Ponto 1, os magistrados do Ministério Público deverão intervir diretamente nos inquéritos relativos a crimes puníveis com pena de prisão superior a 5 anos, analisando a notícia do crime e, em princípio, definindo as diligências de investigação a levar a cabo, ou

[42] Cfr. art. 219.º, n.º 1, da Constituição da República Portuguesa
[43] Atendendo à distribuição de competências organizada pela Lei de Organização da Investigação Criminal, aprovada pela Lei n.º 49/2008, de 27 de agosto.

participando directamente na sua realização, quando o julgarem oportuno, sem prejuízo da delegação genérica de competências para a investigação.

Importa ainda assegurar as prioridades e orientações de política criminal impostas pela Lei n.º 96/2017, de 23 de agosto, bem como as determinações impostas pela Diretiva n.º 1/2017, de 13-10-2017, que concretiza os objetivos, prioridades e orientações de política criminal definidas pela Lei n.º 96/2017,de 23 de agosto.

2.5. Do encerramento do inquérito

Realizadas as diligências necessárias e convenientes à descoberta da verdade, caberá ao Ministério Público apreciar a prova recolhida, em ordem a um eventual arquivamento ou acusação.

Determina o artigo 276.º do CPP que *" o Ministério Público encerra o inquérito, arquivando-o ou deduzindo acusação..."*.

IV. Hiperligações e referências bibliográficas

Hiperligações

http://www.dgsi.pt/jtre.nsf/-/5D41F3148BEB520D80257F68003BB14C
http://www.dgsi.pt/jtrc.nsf/-/9955A8B640A61B5D802573EE005D433F
http://www.dgsi.pt/jtrp.nsf/c3fb530030ea1c61802568d9005cd5bb/84e679a6fe9f67008025726d004ded31?OpenDocument
http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/b566bfcc9c0c99e480257da500551a4c?OpenDocument
http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/aeb1820d0cb667658025739100381ce8?OpenDocument
http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/3444e3f534cfddcb802573d3005c5dcc?OpenDocument
http://www.dgsi.pt/JTRP.NSF/c3fb530030ea1c61802568d9005cd5bb/28cb03199104d3d480257b1900560eea?OpenDocument
http://www.stj.pt/index.php/jurisprudencia-42213/basedados
http://www.stj.pt/index.php/jurisprudencia-42213/basedados
http://www.dgsi.pt/jtrc.nsf/0/5d3fa89f24b219348025759b00510fbc?OpenDocument
http://www.tribunalconstitucional.pt/tc/acordaos/19940479.html
http://www.dgsi.pt/pgrp.nsf/f1cdb56ced3fdd9f802568c0004061b6/6484b1fdad517dc080257419003e00ab?OpenDocument

Referências bibliográficas

- ALBUQUERQUE, Paulo Pinto de; Comentário do Código de Processo Penal à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem; Universidade Católica Editora, 4.ª edição actualizada, 2011.

- BARREIROS, José António: Processo Penal, vol. 1, Coimbra: Almedina, 1981.

- BRAZ, José: Investigação Criminal: a organização, o método e a prova, Os Desafios da Nova Criminalidade, Almedina, Outubro 2009.

- BRAZ, José: A Prova numa perspectiva integrada da formação técnico-profissional de polícia, INPCC, Barro, Loures, 1990.

- CASTRO, Rui da Fonseca: Processo Penal, *Quid Juris*, Lisboa 2011.

- CANOTILHO, Gomes, MOREIRA, Vital, Constituição da República Portuguesa Anotada, vol. I, 4.ª edição revista, Coimbra, Editora, 2007.

- COSTA, Faria, Noções Fundamentais de Direito Penal (Fragmenta Iuris Poenalis), 1999.

- COSTA, José de Faria, *in* As relações entre o Ministério Público e a Polícia: a experiencia portuguesa in Boletim da Faculdade de Direito da Universidade de Coimbra, vol. LXX, Coimbra Editora, 1994.

- CUNHA, José Manuel Damião da. O relacionamento entre as Autoridades Judiciárias e Polícias no Processo Penal, *in* I Congresso de Processo Penal, Coimbra: Almedina, 2005.

- DIAS, Figueiredo *in* Direito Processual Penal, Reimpressão, Coimbra Editora, 2004.

- GONÇALVES, Maia: Código de Processo Penal anotado, 12.ª edição, Almedina, Coimbra, 2001.

- GONÇALVES, Fernando e Manuel João Alves: A Prova do Crime, meios legais para a sua obtenção, Almedina, Setembro, 2009.

- JESUS, Francisco Marcolino, *in* Os Meios de Obtenção da Prova em Processo Penal, Almedina, 2015, 2.ª edição.

- MESQUITA, Paulo Dá. Repressão criminal e iniciativa própria dos órgãos de polícia criminal, in I Congresso de Processo Penal. Coimbra: Almedina, 2005.

- MONTEIRO, Fernando Conde: Que futuro para o processo penal? Simpósio em homenagem a Jorge de Figueiredo Dias, Coimbra Editora, 2009.
- PINTO, Ana Luísa: As buscas não domiciliárias no direito processual português, Revista do Ministério Público, n.º 109, 2007.

- RODRIGUES, Benjamim Silva: Da Prova Penal, Tomo II, 1.ª Edição, 2010, Rei dos Livros.

- SANTOS, M. SIMAS, LEAL-HENRIQUES, M., Código de Processo Penal anotado, vol. I, 2.ª edição (reimpressão actualizada), Lisboa, Editora Rei dos Livros, 2003.

- SILVA, Germano Marques: Curso de Processo Penal I, II, III, Editorial Verbo, 2000, 1999, 2000.

- TABORDA, Raul Gonçalves, Da identificação do suspeito e consequências da recusa de identificação, Revista da Ordem dos Advogados, ano 69, Lisboa.

- VALENTE, Manuel Monteiro Guedes, Processo Penal, tomo I, 3.ª edição, Coimbra, Almedina, 2010.

- VALENTE, Manuel Monteiro Guedes, in Teoria Geral do Direito Policial, 2.ª Edição, Almedina, Outubro 2009.

CENTRO
DE ESTUDOS
JUDICIÁRIOS

8.

Medidas cautelares e de polícia. Enquadramento jurídico, prática e gestão processual

Vera Lúcia Quadros de Oliveira e Santos

CENTRO
DE ESTUDOS
JUDICIÁRIOS

8. MEDIDAS CAUTELARES E DE POLÍCIA. ENQUADRAMENTO JURÍDICO, PRÁTICA E GESTÃO PROCESSUAL

Vera Lúcia Quadros de Oliveira e Santos*

I. Introdução

O presente trabalho "Medidas Cautelares e de Polícia. Enquadramento jurídico, prática e gestão processual" aborda os actos cautelares necessários e urgentes praticados pelos Órgãos de Polícia Criminal (OPC's).

Num primeiro momento, fazemos alusão às relações funcionais entre Ministério Público e Órgãos de Polícia Criminal, bem como às respectivas competências.

Depois, desenvolvemos a temática das medidas cautelares e de polícia.

Terminamos com a menção a alguns documentos hierárquicos do Ministério Público que podem ser úteis no âmbito desta matéria e que se afiguram de conhecimento relevante para os Magistrados do Ministério Público.

II. Objectivos

Este trabalho dirige-se, essencialmente, a Magistrados do Ministério Público, Magistrados Judiciais, Órgãos de Polícia Criminal e Auditores de Justiça.

* Agradecimentos
Pelo apoio incondicional, um especial agradecimento: À minha família.

As medidas cautelares e de polícia que se encontram previstas no Capítulo II do Título I do Livro VI (artigos 248.º a 253.º), do Código de Processo Penal e na Lei n.º 109/2009, de 15 de Setembro (Lei do Cibercrime), serão analisadas, de forma sintética e não exaustiva.
O presente trabalho versa sobre as relações entre as autoridades judiciárias (Ministério Público e Juiz) e os Órgãos de Polícia Criminal e a prática, por estes, de actos cautelares e de polícia.

Assim, visa-se explicitar todos os actos que podem ser praticados pelos Órgãos de Polícia Criminal, numa fase prévia ao inquérito (mas que também podem ocorrer durante o processo), que se encontram previstos na lei. Esses actos serão "fiscalizados" (validados e integrados no processo) pelo Ministério Público ou pelo Juiz.

Ao longo da nossa brevíssima dissertação, vamos esclarecendo como se integram os actos cautelares e de polícia no processo, abordando, assim, a vertente prática e de gestão processual.

III. Resumo

O trabalho encontra-se dividido em três partes: o Ministério Público e os Órgãos de Polícia Criminal, as medidas cautelares e de polícia e os documentos hierárquicos do Ministério Público.

Começamos por salientar a relação entre o Ministério Público e os Órgãos de Polícia Criminal e as respectivas competências, bem como identificamos as diversas entidades que compõem os Órgãos de Polícia Criminal.

Entrando na temática propriamente dita, elaboramos uma breve explicação sobre as medidas cautelares e de polícia e, através da análise que é efectuada a cada uma das normas que regulam esta matéria, procedemos à identificação dos actos que consubstanciam estas medidas, ao mesmo tempo que interligamos a prática e a gestão processual.

Por último, salientamos os documentos hierárquicos do Ministério Público, que consistem numa simples menção e identificação de pareceres, circulares e ordem de serviço sobre a presente temática que, sendo relevantes, devem ser do conhecimento dos Magistrados do Ministério Público.

1. O Ministério Público e os Órgãos de Polícia Criminal

"*Ao Ministério Público compete representar o Estado e defender os interesses que a lei determinar, bem como, com observância do disposto no número seguinte e nos termos da lei, participar na execução da política criminal definida pelos órgãos de soberania, exercer a acção penal orientada pelo princípio da legalidade e defender a legalidade democrática*", tal como consagrado no artigo 219.º, n.º 1, da Constituição da República Portuguesa.

Decorre deste normativo constitucional que compete ao Ministério Público o exercício da acção penal.

O Ministério Público é a entidade com legitimidade para promover o processo penal e competente para dirigir o inquérito, nos termos dos artigos 1.º, alínea b), 48.º a 53.º, 241.º e seguintes e 262.º e seguintes, do Código de Processo Penal. *Vide*, ainda, artigos 1.º e 3.º, n.º 1, alíneas b), c), h), i) e n) e n.º 3, do Estatuto do Ministério Público (Lei n.º 47/86, de 15 de Outubro).

Sucede que o Ministério Público é responsável pela direcção do inquérito, mas não actua sozinho, sendo auxiliado por Órgãos de Polícia Criminal (cfr. artigo 263.º, do Código de Processo Penal e artigo 2.º, n.ºs 1 e 2, da Lei n.º 49/2008, de 27 de Agosto, que aprovou a Lei de Organização da Investigação Criminal).

A actividade policial surgiu como forma de manter a ordem e preservar a segurança e a tranquilidade pública.

Desta forma, o artigo 272.º, n.º 1, da Constituição da República Portuguesa dispõe que "*A polícia tem por funções defender a legalidade democrática e garantir a segurança interna e os direitos dos cidadãos*.".

O n.º 2 prevê que "*As medidas de polícia são as previstas na lei, não devendo ser utilizadas para além do estritamente necessário*", acolhendo, assim, os princípios da legalidade, da tipicidade e da proporcionalidade ou da proibição do excesso (cfr. artigo 18.º, n.º 2, da Constituição da República Portuguesa).

Este normativo acolhe as medidas de polícia que se encontram previstas nos artigos 28.º e seguintes, da Lei n.º 53/2008, de 29 de Agosto, que aprovou a Lei de Segurança Interna.

Para além das funções de repressão e prevenção criminal atribuídas às polícias, a Constituição da República Portuguesa reconhece as medidas de polícia que se traduzem em actos de iniciativa própria dos Órgãos de Polícia Criminal e que se encontram previstas nos artigos 248.º a 253.º, do Código de Processo Penal, no capítulo correspondente às medidas cautelares e de polícia, e na Lei n.º 109/2009, de 15 de Setembro (Lei do Cibercrime).

Antes de avançarmos, é de salientar que as autoridades judiciárias[1] - Ministério Público, Juiz e Juiz de Instrução - (cfr. artigos 1.º, alínea b), 263.º, n.º 1 e 288.º, n.º 1, do Código de Processo Penal) são coadjuvadas pelos Órgãos de Polícia Criminal (doravante, OPC's). Conforme o disposto no artigo 55.º, n.º 1, do Código de Processo Penal, "*Compete aos órgãos de polícia criminal coadjuvar as autoridades judiciárias com vista à realização das finalidades do processo*".

[1] Artigo 1.º, alínea b), do Código de Processo Penal: "*«Autoridade judiciária» o juiz, o juiz de instrução e o Ministério Público, cada um relativamente aos actos processuais que cabem na sua competência*".

O artigo 1.º, alínea c), do Código de Processo Penal define os órgãos de polícia criminal como "*todas as entidades e agentes policiais a quem caiba levar a cabo quaisquer actos ordenados por uma autoridade judiciária ou determinados por este Código*.".

Existem OPC's com competência genérica, tal como previsto na Lei de Organização da Investigação Criminal. Assim, Polícia Judiciária, Guarda Nacional Republicana e Polícia de Segurança Pública (artigo 3.º, n.º 1, daquele diploma legal).

Para além destes OPC's, outros têm competências específicas:

– Polícia Judiciária Militar – Lei n.º 97-A/2009, de 3 de Setembro, Lei n.º 100/2003, de 15 de Novembro, Decreto-Lei n.º 200/2001, de 13 de Julho (artigos 18.º a 35.º) e Circular da Procuradoria-Geral da República n.º 14/2004, de 05-11-2004;

– Serviço de Estrangeiros e Fronteiras – Decreto-Lei n.º 252/2000, de 16 de Outubro, Lei n.º 23/2007, de 4 de Julho e Decreto-Lei n.º 290-A/2001, de 17 de Novembro;

– Funcionários Judiciais – Decreto-Lei n.º 343/99, de 26 de Agosto (Mapa I);

– Polícia Marítima – Decreto-Lei n.º 248/95, de 21 de Setembro, Decreto-Lei n.º 43/2002, de 2 de Março e Decreto-Lei n.º 44/2002, de 2 de Março;

– Autoridade de Segurança Alimentar e Económica – Decreto-Lei n.º 194/2012, de 23 de Agosto e Portaria n.º 35/2013, de 30 de Janeiro;

– Inspecção-Geral da Agricultura, do Mar, do Ambiente e do Ordenamento do Território – Decreto-Lei n.º 23/2012, de 1 de Fevereiro;

– Administração Tributária e Aduaneira – Lei n.º 15/2001, de 5 de Junho (Regime Geral das Infracções Tributárias), Decreto-Lei n.º 118/2011, de 15 de Dezembro, Decreto-Lei n.º 117/2001, de 15 de Dezembro e Portaria n.º 320-A/2011, de 30 de Dezembro;

– Administração da Segurança Social – Lei n.º 15/2001, de 5 de Junho (Regime Geral das Infracções Tributárias), Decreto-Lei n.º 167-A/2013, de 31 de Dezembro, Decreto-Lei n.º 83/2012, de 30 de Março, Portaria n.º 135/2012, de 8 de Maio (alterada pela Portaria n.º 160/2016, de 9 de Junho), Decreto-Lei n.º 131/2012, de 25 de Junho;

– Polícias Municipais – Lei n.º 19/2004, de 20 de Maio, Decreto-Lei n.º 197/2008, de 7 de Outubro, Decreto-Lei n.º 239/2009, de 16 de Setembro e Decreto-Lei n.º 39/2000, de 17 de Março (capítulo IV e anexos II, III e IV).

Os OPC's auxiliam as autoridades judiciárias. Estão numa posição de coadjutores, mas praticam actos que cabem nas funções dos órgãos principais.

Tal como refere José Manuel Damião da Cunha[2] "*Compete, portanto, aos órgãos de polícia criminal, no exercício da sua competência coadjuvatória, praticar todos aqueles actos que sejam necessários à realização das finalidades processuais penais, ao lado dos órgãos principais, i.e., as autoridades judiciárias*".

Paulo Dá Mesquita[3] menciona que "*A actividade dos órgãos de polícia criminal como coadjuvantes existe em função das finalidades do inquérito e é com esse desiderato que esses órgãos devem ainda que por iniciativa própria recolher notícias dos crimes, impedir outras consequências da sua prática, identificar os autores do crime e procurá-los e obter tudo o que possa servir a aplicação da lei penal*".

Durante o inquérito, os OPC's actuam no processo sob a direcção e dependência funcional do Ministério Público (cfr. artigos 56.º e 263.º, n.º 2, do Código de Processo Penal e artigo 2.º, n.º 4, da Lei de Organização da Investigação Criminal)[4].

Em certos momentos, os OPC's devem agir antes de existir intervenção de qualquer autoridade judiciária, tal como prevê o artigo 55.º, n.º 2, do Código de Processo Penal, segundo o qual "*Compete em especial aos órgãos de polícia criminal, mesmo por iniciativa própria, colher notícia dos crimes e impedir quanto possível as suas consequências, descobrir os seus agentes e levar a cabo os actos necessários e urgentes destinados a assegurar os meios de prova*". Confrontar, ainda, o artigo 272.º, n.º 2, da Constituição da República Portuguesa, como supra mencionado.

Entramos, assim, no âmbito das medidas cautelares e de polícia, previstas nos artigos 248.º a 253.º, do Código de Processo Penal e nos artigos 12.º, 15.º e 16.º, da Lei n.º 109/2009, de 15 de Setembro (Lei do Cibercrime).

2. As medidas cautelares e de polícia

As medidas cautelares e de polícia (artigos 248.º a 253.º, do Código de Processo Penal[5]) traduzem-se em actos cautelares necessários e urgentes praticados pelos OPC´s, aquando do conhecimento da prática de um crime (notícia do crime), e que se destinam a preservar meios e elementos probatórios, podendo ocorrer numa fase prévia e antecipatória do inquérito ou numa fase contemporânea do processo.

São actos praticados pelos OPC´s por sua própria iniciativa, no exercício da competência de coadjuvação ao Ministério Público, que serão, *a posteriori*, integrados no processo. No

[2] In *O Ministério Público e os Órgãos de Polícia Criminal no novo Código de Processo Penal*, UCP, Porto, 1993, pág. 112.
[3] *In Direcção do Inquérito Penal e Garantia Judiciária*, Coimbra Editora, 2003, pág. 131.
[4] Sobre a questão de orientação e dependência funcional dos OPC's *vide*, entre outros, José Damião da Cunha in *O Ministério Público e os Órgãos de Polícia Criminal no novo Código de Processo Penal*, UCP, Porto, 1993, págs. 114 a 119, 155 e 156; Henrique Pereira Teotónio in *Titularidade do Inquérito e Dependência Funcional das Polícias*, Cadernos da Revista do Ministério Público, n.º 4, págs. 93 a 99.
[5] Doravante, todas as normas sem menção expressa ao diploma legal referem-se ao Código de Processo Penal.

entanto, estamos perante actos que se encontram restringidos aos pressupostos da necessidade e da urgência, uma vez que estes actos são praticados pelos OPC´s antes da intervenção da autoridade judiciária competente[6].

Nos casos em que já existe intervenção da autoridade judiciária, os OPC's têm a obrigação de assegurar os novos meios de prova de que tenham conhecimento e devem dar notícia imediata à respectiva autoridade judiciária (nos termos do n.º 3 do artigo 249.º).

2.1. Natureza das medidas cautelares e de polícia

Alguns autores consideram que as medidas cautelares e de polícia são actos pré-processuais e não actos processuais, cuja integração no processo depende de uma decisão da autoridade judiciária (Ministério Público ou juiz de instrução), tal como refere Paulo Dá Mesquita, Germano Marques da Silva e Paulo Pinto de Albuquerque.

Outros, como Damião da Cunha[7], entendem que estamos perante actos processuais ("*actos com relevância processual penal*") que integram o processo. Ainda assim, estão sujeitos a uma avaliação pelos titulares competentes do processo.

2.2. Comunicação da notícia do crime

Os OPC's têm a obrigação de transmitir todas e quaisquer notícias do crime (mesmo que manifestamente infundadas) ao Ministério Público, no mais curto prazo possível, não podendo exceder os 10 dias, nos termos do artigo 248.º, n.ºs 1 e 2 e artigo 2.º, n.º 3, da Lei de Organização da Investigação Criminal. O Ministério Público terá de avaliar se a notícia do crime é ou não fundada.

Vários autores referem que o prazo limite de 10 dias para os OPC's transmitirem a notícia do crime ao Ministério Público é exagerado e, por isso, deve existir uma comunicação quase imediata, num prazo não superior a 24 horas, tendo em conta os meios de comunicação disponíveis actualmente (neste sentido, entre outros, Maia Costa e Paulo Pinto de Albuquerque[8]).

A comunicação da notícia do crime é realizada através do envio do auto de notícia ou do auto de denúncia, o que determina a abertura de inquérito, cfr. artigos 241.º e seguintes e 262.º, n.º 2.

---

[6] *Vide* Acórdão do STJ de 12-03-2009, Santos Cabral, Processo n.º 09P0395, *in* www.dgsi.pt.
[7] *In O Ministério Público e os Órgãos de Polícia Criminal no novo Código de Processo Penal*, UCP, Porto, 1993, págs. 142 e 143.
[8] Salienta que os artigos 243.º, n.º 3, 245.º e 248.º, n.º 1, do Código de Processo Penal são inconstitucionais por violarem os artigos 26.º, n.º 1, 32.º, n.ºs 1 e 5, e 219.º, n.º 1, "na medida em que permitem a dilação da comunicação da notícia do crime pelo órgão de polícia criminal ao Ministério Público por período até 10 dias contados desde o dia em que o órgão de polícia criminal teve a notícia do crime" – anotação n.º 5 ao artigo 248.º, *in Comentário do Código de Processo Penal à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem*, 3.ª edição actualizada, Lisboa: Universidade Católica Editora, 2009, págs. 647 e 648.

Em caso de urgência, a transmissão da notícia do crime pode ser efectuada por qualquer meio de comunicação disponível (n.º 3 do artigo 248.º).

Após a comunicação da notícia do crime, o Ministério Público pode "*a) delegar a realização de diligências pré-determinadas; b) ordenar que lhe seja imediatamente remetido o expediente (…); ou c) deixar ao órgão de polícia criminal o encargo da prática das primeiras diligências e investigações relativas ao inquérito*"[9].

2.3. Providências cautelares quanto aos meios de prova

Os OPC's têm competência própria para praticar todos os actos cautelares necessários e urgentes com vista a assegurar os meios e elementos de prova, que serão incorporados no processo criminal, nos termos do artigo 249.º, n.º 1. A integração destes actos passará pela validação (ou não) pela autoridade judiciária competente, tratando-se de um acto de controlo da legalidade da medida cautelar empreendida pelos OPC's[10].

Sucede que, os actos cautelares e urgentes que caiam na competência exclusiva do juiz de instrução e do Ministério Público não podem ser realizados pelos OPC's, cfr. artigos 268.º, 269.º, 270.º, n.º 2 e 290.º, n.º 2.

O n.º 2 do artigo 249.º contém um elenco, não exaustivo ("nomeadamente"), das medidas cautelares que podem ser praticadas pelos OPC's.

Mesmo que exista intervenção da autoridade judiciária, se surgir o conhecimento de novos meios de prova, os OPC's devem executar todos os actos cautelares necessários e urgentes com vista à respectiva preservação e devem dar notícia imediata à autoridade judiciária competente (artigo 249.º, n.º 3).

2.3.1. Exames dos vestígios do crime e protecção do estado das coisas e dos lugares

Os OPC's devem preservar os vestígios do crime, evitando que estes desapareçam ou se alterem, e assegurar a manutenção do estado das coisas e dos locais onde ocorreu a prática do crime, ao abrigo do disposto na alínea a) do n.º 2 do artigo 249.º.
Este normativo remete-nos para o meio de obtenção de prova – exame -, cfr. o disposto no n.º 2 do artigo 171.º e no artigo 173.º.

Nos termos do artigo 171.º, n.º 2, "*Logo que houver notícia da prática de crime, providencia-se para evitar, quando possível, que os seus vestígios se apaguem ou alterem antes de serem*

[9] Paulo Dá Mesquita *in Repressão Criminal e iniciativa própria dos órgãos de polícia criminal*, I Congresso de Processo Penal – Memórias – Coordenação de Manuel Monteiro Guedes Valente, Almedina, 2005, pág. 71.
[10] Sobre o depoimento de agentes de autoridade quanto às medidas cautelares praticadas *vide*, entre outros, Acórdão do STJ de 03-03-2010, Santos Cabral, Processo n.º 886/07.8PSLSB.L1.S1 e Acórdão do TRC de 16-06-2015, Cacilda Sena, Processo n.º 360/10.5EACBR.C1, todos *in* www.dgsi.pt.

examinados, proibindo-se, se necessário, a entrada ou o trânsito de pessoas estranhas no local do crime ou quaisquer outros actos que possam prejudicar a descoberta da verdade.".

Ao abrigo do disposto no n.º 1 do artigo 173.º, o OPC competente (ou qualquer agente da autoridade, cfr. artigo 171.º, n.º 4, por remissão do artigo 173.º, n.º 2) pode determinar que as pessoas não se afastem do local do exame, podendo recorrer, se necessário, à força pública, para que permaneçam naquele local enquanto a presença se revelar indispensável e o exame não terminar[11].

2.3.2. Recolha de informações das pessoas

Algumas pessoas detêm informações relevantes no que concerne à identificação do(s) agente(s) do crime, à descrição dos factos, designadamente, do tempo, lugar, modo e outras circunstâncias que possam, inclusive, levar à reconstituição do crime, pelo que cabe aos OPC's a recolha dessas mesmas informações (cfr. alínea b) do n.º 2 do artigo 249.º).

2.3.3. Apreensões de objectos e respectiva conservação ou manutenção

No decurso de revistas e buscas, a título cautelar ou em caso de urgência e perigo na demora, os OPC's procedem às apreensões dos objectos que serviram a prática do crime, adoptando as medidas cautelares necessárias à sua conservação e manutenção, nos termos do artigo 249.º, n.º 2, alínea c), até que seja realizada a respectiva entrega à autoridade judiciária competente.

As apreensões encontram-se previstas no artigo 178.º, cuja redacção foi alterada pela Lei n.º 30/2017, de 20 de Maio.

Ao abrigo do disposto no n.º 1, "*São apreendidos os instrumentos, produtos ou vantagens relacionados com a prática de um facto ilícito típico, e bem assim todos os objectos que tiverem sido deixados pelo agente no local do crime ou quaisquer outros susceptíveis de servir a prova*.".

As apreensões podem ser autorizadas pela autoridade judiciária quando são solicitadas, anteriormente, pelos OPC's, ou ordenadas quando provêm de decisão por iniciativa da autoridade judiciária (cfr. artigo 178.º, n.º 3).

O n.º 4 do artigo 178.º remete-nos para o disposto no artigo 249.º, n.º 2, alínea c), pelo que, neste caso, há lugar a apreensões de objectos pelos OPC´s como medida cautelar necessária e urgente.

[11] Note-se que "*Se alguém pretender eximir-se ou obstar a qualquer exame devido ou a facultar coisa que deva ser examinada, pode ser compelido por decisão da autoridade judiciária competente*." – artigo 172.º, n.º 1, do Código de Processo Penal.

Além disso, os OPC's "*podem ainda efectuar apreensões quando haja fundado receio de desaparecimento, destruição, danificação, inutilização, ocultação ou transferência de instrumentos, produtos ou vantagens ou outros objectos provenientes da prática de um facto ilícito típico susceptíveis de serem declarados perdidos a favor do Estado*." (cfr. n.º 5 do artigo 178.º).

As apreensões realizadas pelos OPC's estão sujeitas a validação pela autoridade judiciária, no prazo máximo de setenta e duas horas (artigo 178.º, n.º 6). A validação das apreensões pela autoridade judiciária serve para apreciar e controlar a legalidade daqueles actos.

No inquérito, o Ministério Público procede à validação das apreensões efectuadas pelos OPC's, proferindo despacho.

2.4. Identificação de suspeito e pedido de informações

A medida cautelar prevista no artigo 250.º delimita os actos que podem ser praticados pelos OPC´s com vista à identificação de suspeitos e pedido de informações.

Os OPC's só podem proceder à identificação de uma pessoa que se encontre num local público, aberto ao público ou sujeito a vigilância policial, se sobre ela recaírem "*fundadas suspeitas da prática de crimes, da pendência de processo de extradição ou de expulsão, de que tenha penetrado ou permaneça irregularmente no território nacional ou de haver contra si mandado de detenção*" (n.º 1 do artigo 250.º). Só nestes casos taxativamente previstos na lei é que se afigura legítima a intervenção dos OPC´s com vista à identificação de suspeitos.

Por isso, os OPC's têm de comunicar ao suspeito as circunstâncias que fundamentam a obrigação de identificação (n.º 2 do artigo 250.º), devendo constar no relatório o respectivo motivo (cfr. artigo 253.º).

Ao abrigo do disposto no n.º 3 do artigo 250.º, o suspeito pode identificar-se através da apresentação dos seguintes documentos:

– Se for cidadão português, bilhete de identidade/cartão do cidadão ou passaporte;

– Se for cidadão estrangeiro, título de residência, bilhete de identidade, passaporte ou documento que substitua o passaporte.

Caso não seja possível apresentar um destes documentos, "*o suspeito pode identificar-se mediante a apresentação de documento original, ou cópia autenticada, que contenha o seu nome completo, a sua assinatura e a sua fotografia*." (n.º 4 do artigo 250.º).

Pode, ainda, suceder que o suspeito não detenha qualquer documento identificativo. Assim, nos termos do artigo 250.º, n.º 5, o suspeito pode identificar-se através de um dos seguintes meios:

"*a) Comunicação com uma pessoa que apresente os seus documentos de identificação;*

b) Deslocação, acompanhado pelos órgãos de polícia criminal, ao lugar onde se encontram os seus documentos de identificação;

c) Reconhecimento da sua identidade por uma pessoa identificada nos termos do n.º 3 ou do n.º 4 que garanta a veracidade dos dados pessoais indicados pelo identificando.".

Nesta última circunstância, prevista na alínea c), em caso de mentira ou omissão pela pessoa que garanta a veracidade dos dados pessoais do suspeito, tal não lhe acarretará qualquer sanção criminal.

Se todos os meios de identificação anteriores falharem, nos termos do n.º 6 do artigo 250.º, os OPC's podem deter o suspeito e conduzi-lo ao posto policial mais próximo a fim de procederem à respectiva identificação. Podem ser realizadas, "*em caso de necessidade, provas dactiloscópicas, fotográficas ou de natureza análoga*" e o suspeito pode ser convidado "*a indicar residência onde possa ser encontrado e receber comunicações*"[12][13].

Esta detenção não corresponde a uma medida de coacção, nem à detenção prevista no artigo 254.º, tratando-se, apenas, de uma medida cautelar que tem protecção constitucional no artigo 27.º, n.º 3, alínea g), da Constituição da República Portuguesa[14].

O suspeito deve permanecer no posto policial pelo tempo estritamente indispensável à sua identificação e por período nunca superior a seis horas, tenha ou não existido a respectiva identificação. O período de seis horas tem início desde o momento em que o suspeito é abordado e não da entrada no posto policial.

Deve ser elaborado auto de detenção, onde conste "*a hora e o local da abordagem do suspeito no «lugar público», a hora de entrada do suspeito no posto policial e a hora de saída do suspeito do posto policial*"[15].

Todos os actos de identificação são reduzidos a auto (n.º 7 do artigo 250.º).

---

[12] SILVA, Germano Marques da, Direito Processual Penal Português: Do Procedimento (Marcha do Processo), Vol. III, Lisboa: Universidade Católica Editora, 2015, pág. 66.

[13] Cfr.: Artigo 1.º, da Lei n.º 67/2017, de 9 de Agosto (que Regula a identificação judiciária lofoscópica e fotográfica, adaptando a ordem jurídica interna às Decisões 2008/615/JAI e 2008/616/JAI do Conselho, de 23 de Junho de 2008): "*A presente lei regula a identificação judiciária lofoscópica e fotográfica para efeitos de prevenção e investigação criminal, bem como o tratamento da informação respectiva, em especial quanto ao ficheiro central de dados lofoscópicos (FCDL)*".

Artigo 3.º, n.º 1, alínea d), da Lei n.º 67/2017, de 9 de Agosto: "*São sujeitos a identificação judiciária os indivíduos (…) Suspeitos, nos termos do n.º 1 do artigo 250.º do Código de Processo Penal, que não sejam portadores de documento de identificação, não possam identificar-se por qualquer dos meios previstos nos n.ºs 3, 4 e 5 daquele artigo, ou recusem identificar-se perante autoridades ou órgãos de polícia criminal, nos termos aí prescritos*".

[14] Direito à liberdade e à segurança – "*Exceptua-se deste princípio a privação da liberdade, pelo tempo e nas condições que a lei determinar, nos casos seguintes: Detenção de suspeitos, para efeitos de identificação, nos casos e pelo tempo estritamente necessários*".

[15] *In* ALBUQUERQUE, Paulo Pinto de, *Comentário do Código de Processo Penal à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem*, 3.ª edição actualizada, Lisboa: Universidade Católica Editora, 2009, pág. 666.

Se a suspeita não se confirmar, o identificando é libertado imediatamente e pode solicitar a destruição das provas de identificação. Paulo Pinto de Albuquerque refere que "*Não se vê em que circunstância a destruição de documentos de identificação possa ter cabimento. Por outro lado, o auto propriamente dito nunca pode ser destruído, mesmo que o identificando o peça e a suspeita se não confirme. Em nenhuma circunstância, um auto de detenção pode ser destruído pelo órgão de polícia criminal sem autorização prévia do Ministério Público, sob pena de violação grave do poder de direcção do inquérito pelo Ministério Público*"[16].

Se no decurso da prestação de informações pelo suspeito surgir fundada suspeita da prática de crime por ele cometido, o OPC deve suspender imediatamente a recolha de informações e deve proceder à constituição como arguido[17], ao abrigo do disposto nos artigos 250.º, n.º 8, 59.º e 58.º, n.ºs 2, 3 e 4.

Os OPC's podem, ainda, pedir informações a quaisquer pessoas que possuam informações úteis, cfr. n.º 8 do artigo 250.º. Estas pessoas não são testemunhas, mas, se pretenderem prestar depoimento, estão sujeitas ao regime de prestação da prova testemunhal (cfr. Paulo Pinto de Albuquerque).

Em qualquer destas situações supra descritas, o identificando tem a possibilidade de contactar com pessoa da sua confiança, nos termos do artigo 250.º, n.º 9.

Todos os procedimentos que foram concretizados pelos OPC's têm de ser mencionados no relatório que é enviado à autoridade judiciária competente (artigo 253.º).

2.5. Revistas e Buscas

As revistas e buscas são meios de obtenção de prova que encontram previsão legal nos artigos 174.º a 177.º.

Se existirem indícios de que uma pessoa oculta objectos relacionados com um crime ou que possam servir de prova é ordenada revista. Se esses objectos se encontrarem num lugar reservado ou de não livre acesso ao público é ordenada busca (cfr. artigo 174.º, n.ºs 1 e 2).

Por regra, as revistas e as buscas são autorizadas ou ordenadas por despacho da autoridade judiciária competente, nos termos do artigo 174.º, n.º 3. O despacho da autoridade judiciária que autoriza ou ordena as revistas e/ou as buscas tem um prazo de validade máxima de 30 dias, sob pena de nulidade, cfr. n.º 4 do artigo 174.º.

Durante o inquérito, o Ministério Público é a autoridade judiciária competente para autorizar as revistas e as buscas, pelo que também tem competência para as apreciar e validar.

[16] *In Comentário do Código de Processo Penal à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem*, 3.ª edição actualizada, Lisboa: Universidade Católica Editora, 2009, pág. 666.
[17] Sobre o momento da constituição de arguido e a reprodução em audiência de julgamento das "conversas informais", confrontar, entre outros, o Acórdão do TRL de 22-06-2017, Filipa Costa Lourenço, Processo n.º 320/14.7GCMTJ.L1-9, *in* www.dgsi.pt.

No entanto, existem algumas excepções que se encontram previstas nas alíneas do n.º 5 do artigo 174.º, segundo o qual, os OPC's podem efectuar revistas e buscas nos seguintes casos:

"*a) De terrorismo, criminalidade violenta ou altamente organizada, quando haja fundados indícios da prática iminente de crime que ponha em grave risco a vida ou a integridade de qualquer pessoa* (cfr. artigo 1.º, alíneas i), j), l) e m));

b) Em que os visados consintam, desde que o consentimento prestado fique, por qualquer forma, documentado; ou

c) Aquando de detenção em flagrante por crime a que corresponda pena de prisão" (cfr. artigos 255.º e 256.º).

Basta o preenchimento de um dos requisitos previstos nestas alíneas para que os OPC's procedam à realização de revista a pessoa que encubra objectos relacionados com a prática de um crime e/ou de busca em lugar reservado ou não livremente acessível ao público.

Nos casos previstos da alínea a), a realização da diligência é, sob pena de nulidade, imediatamente comunicada ao juiz de instrução, a fim de ser apreciada e validada, ao abrigo do disposto no n.º 6 do artigo 174.º.

Para além destas excepções, o artigo 251.º prevê que os OPC's, por sua iniciativa e sem prévia autorização da autoridade judiciária, podem, em situações urgentes, proceder a revistas e a buscas.

Aplica-se aqui o regime das revistas e buscas, previsto nos artigos 174.º a 176.º, cumprindo-se, com as necessárias adaptações, as respectivas formalidades.

Assim, ao abrigo do disposto na alínea a) do n.º 1 do artigo 251.º, os OPC's procedem "*À revista de suspeitos em caso de fuga iminente ou de detenção e a buscas no lugar em que se encontrarem, salvo tratando-se de busca domiciliária*[18]*, sempre que tiverem fundada razão para crer que neles se ocultam objectos relacionados com o crime, susceptíveis de servirem a prova e que de outra forma poderiam perder-se*"[19].

Os OPC's efectuam a revista de suspeitos, em caso de fuga iminente ou de detenção fora de flagrante delito, se existirem indícios de que ocultam na sua pessoa objectos relacionados com o crime ou que possam servir de prova, nos termos do disposto nos artigos 174.º, n.º 1 e 251.º, n.º 1, alínea a).

Devem ser respeitados os direitos à integridade moral, à identidade pessoal e à intimidade da vida privada do suspeito (cfr. artigos 25.º, n.º 1 e 26.º, n.º 1, da Constituição da República Portuguesa e artigo 175.º, n.º 2, do Código de Processo Penal).

[18] Cfr. artigo 177.º, do Código de Processo Penal – Busca domiciliária.
[19] *Vide* Acórdão do TRL de 06-11-2007, Emídio Santos, Processo n.º 4746/2007-5, *in* www.dgsi.pt.

Nos termos do artigo 174.º, n.º 2 e do artigo 251.º, n.º 1, alínea a), as buscas não domiciliárias estão sujeitas aos seguintes pressupostos:

– Não podem conflituar com o âmbito das buscas domiciliárias, previstas no artigo 177.º (não podem ocorrer em espaços qualificados como domicílio – "casa habitada" e respectivas "dependências fechadas" – artigo 34.º, da Constituição da República Portuguesa);

– Sobre o suspeito deve recair a suspeita de fuga iminente ou de detenção fora de flagrante delito;

– Deve existir fundada razão de que no local se ocultam objectos relacionados com o crime;

– Os objectos servem como meios de prova; e

– A não realização da busca determinaria a perda desses meios de prova.

Nos termos da alínea b) do n.º 1 do artigo 251.º, os OPC's procedem "*À revista de pessoas que tenham de participar ou pretendam assistir a qualquer acto processual ou que, na qualidade de suspeitos, devam ser conduzidos a posto policial, sempre que houver razões para crer que ocultam armas ou outros objectos com os quais possam praticar actos de violência.*". Trata-se de uma medida com carácter preventivo de condutas criminosas, afastando-se de uma finalidade cautelar de obtenção de um meio de prova.

Todos estes actos cautelares têm de ser documentados pelos OPC's e devem ser comunicados imediatamente à autoridade judiciária competente, a fim de proceder à respectiva validação[20].

Apesar de o n.º 2 do artigo 251.º remeter para o n.º 6 do artigo 174.º, segundo o qual a comunicação para validação das diligências é transmitida ao juiz de instrução, há quem considere que tal interpretação deve ser restritiva.

Estando perante actos ocorridos numa fase prévia ou durante o inquérito, cabe ao Ministério Público a validação da revista de suspeito em caso de fuga iminente ou de detenção fora de flagrante delito e da busca não domiciliária (cfr. artigo 270.º, n.º 2, alínea d)). Se os actos ocorreram na fase da instrução, a validação é efectuada pelo juiz de instrução (cfr. artigos 268.º e 269.º)[21].

[20] Confrontar Acórdão do TRP de 21-01-2015, Maria dos Prazeres Silva, Processo n.º 27/14.5PEVNG-A.P1, *in* www.dgsi.pt.

[21] Neste sentido, Paulo Pinto de Albuquerque in *Comentário do Código de Processo Penal à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem*, 3.ª edição actualizada, Lisboa: Universidade Católica Editora, 2009, págs. 650 e 668; Maia Costa in *Código de Processo Penal Comentado*, 2.ª Edição Revista, Coimbra, Almedina, 2016, pág. 894; Germano Marques da Silva in *Direito Processual Penal Português: Do Procedimento (Marcha do Processo)*, Vol. III, Lisboa: Universidade Católica Editora, 2015, pág. 67; Paulo Soares in *Meios de Obtenção de Prova no Âmbito das Medidas Cautelares e de Polícia*, 2.ª Edição, Coimbra, Almedina, 2017, págs. 211 a 213.

2.6. Apreensão de correspondência

A intromissão na correspondência pode conflituar com a reserva da intimidade da vida privada, constitucionalmente protegida no artigo 26.º, da Constituição da República Portuguesa.

O sigilo da correspondência e de outros meios de comunicação privada são invioláveis, bem como a ingerência das autoridades públicas na correspondência e nas comunicações é proibida, ao abrigo do disposto no artigo 34.º, n.ºs 1 e 4, da Constituição da República Portuguesa. Contudo, o n.º 4 deste normativo constitucional apresenta a excepção a essa proibição de ingerência nos "*casos previstos na lei em matéria de processo criminal*".

Ao abrigo do disposto no artigo 179.º, n.º 1, o juiz determina "*a apreensão, mesmo nas estações de correios e de telecomunicações, de cartas, encomendas, valores, telegramas ou qualquer outra correspondência, quando tiver fundadas razões para crer que:*

a) A correspondência foi expedida pelo suspeito ou lhe é dirigida, mesmo que sob nom diverso ou através de pessoa diversa;

b) Está em causa crime punível com pena de prisão superior, no seu máximo, a 3 anos; e

c) A diligência se revelará de grande interesse para a descoberta da verdade ou para a prova.".

A apreensão de correspondência é sempre ordenada ou autorizada pelo juiz, nos termos das disposições dos artigos 269.º, n.º 1, alínea d), 179.º, n.º 1 e 252.º, n.º 1. Os OPC's só podem efectuar a apreensão de correspondência mediante despacho prévio proferido pelo juiz que ordene ou autorize essa apreensão.

Toda a correspondência apreendida é transmitida intacta ao juiz, que é o primeiro a ter conhecimento do respectivo conteúdo (cfr. artigos 179.º, n.º 3, 268.º, n.º 1, alínea d) e 252.º, n.º 1). O juiz decide da junção ou não dessa correspondência ao processo.

Se os OPC's tiverem fundadas razões para crer que encomendas ou valores fechados contêm informações úteis à investigação ou possam conduzir à descoberta de um crime e que podem perder-se em caso de demora, devem informar, pelo meio mais rápido, o juiz que, neste caso, poderá autorizar a abertura imediata daquela correspondência (n.º 2 do artigo 252.º).

Os OPC's, com base nos fundamentos anteriores, podem, como medida cautelar, ordenar a suspensão da remessa de correspondência nas estações de correios e de telecomunicações. Contudo, esta ordem tem de ser convalidada por despacho fundamentado do juiz, no prazo máximo de 48 horas, sob pena de a correspondência ser remetida ao destinatário (n.º 3 do artigo 252.º).

O disposto no artigo 252.º também se aplica ao correio electrónico, nos termos do artigo 17.º, da Lei n.º 109/2009, de 15 de Setembro (Lei do Cibercrime), segundo o qual "*Quando, no decurso de uma pesquisa informática ou outro acesso legítimo a um sistema informático, forem encontrados, armazenados nesse sistema informático ou noutro a que seja permitido o acesso legítimo a partir do primeiro, mensagens de correio electrónico ou registos de comunicações de natureza semelhante, o juiz pode autorizar ou ordenar, por despacho, a apreensão daqueles que se afigurem ser de grande interesse para a descoberta da verdade ou para a prova, aplicando-se correspondentemente o regime da apreensão de correspondência previsto no Código de Processo Penal*.".

É de salientar que a apreensão de correspondência que não cumpra os requisitos legais supra expostos, é um método proibido de prova, pelo que não poderá ser utilizada no processo, sendo proibida a sua valoração, nos termos do artigo 126.º, n.º 3[22].

2.7. Localização celular

A localização celular configura uma ingerência na intimidade da vida privada e nas telecomunicações, cfr. artigos 26.º e 34.º, n.º 4, da Constituição da República Portuguesa, mas tal ingerência é permitida pelo Código de Processo Penal, tal como referido em 2.6..

A localização celular é realizada através da "*detecção da localização física do telemóvel de uma pessoa ou do percurso efectuado pelo seu possuidor, através da ligação à rede móvel telefónica*"[23].

É uma medida cautelar que se encontra prevista no artigo 252.º-A e só pode ser aplicada pelas autoridades judiciárias[24] e pelas autoridades de polícia criminal[25] quando se afigurar necessária para afastar um perigo para a vida ou um perigo de ofensa à integridade física grave. Também só é de aplicar se se mostrar necessária, adequada e indispensável para localizar um suspeito ou uma vítima, com vista a remover aqueles perigos. "*O termo "para afastar perigo" significa que a acção que coloca os bens jurídicos sob ameaça iminente ainda não se consumou, pelo menos na íntegra, e que os bens jurídicos sob ameaça poderão vir a ser irremediavelmente sacrificados*"[26].

Se existir um processo em curso, os dados sobre a localização celular têm de ser comunicados ao juiz de instrução, no prazo máximo de 48 horas, para sua convalidação (n.º 2 do artigo

[22] Cfr. Acórdão TRC de 07-06-2017, Maria Pilar de Oliveira, Processo n.º 96/14.8EALSB-A.C1, *in* www.dgsi.pt.
[23] *In* SOARES, Paulo, *Meios de Obtenção de Prova no Âmbito das Medidas Cautelares e de Polícia*, 2.ª Edição, Coimbra, Almedina, 2017, pág. 261.
[24] Cfr. artigo 1.º, alínea b), do Código de Processo Penal, "*«Autoridade judiciária» o juiz, o juiz de instrução e o Ministério Público, cada um relativamente aos actos processuais que cabem na sua competência*".
[25] Cfr. artigo 1.º, alínea d), do Código de Processo Penal, "*«Autoridade de polícia criminal» os directores, oficiais, inspectores e subinspectores de polícia e todos os funcionários policiais a quem as leis respectivas reconhecerem aquela qualificação*".
[26] Fernando Manuel Castanheira de Brito *in Breve análise sobre a localização celular como «medida cautelar e de polícia» (art. 252.º-A do CPP)*, pág. 188.

252.º-A). O juiz deve proferir despacho fundamentado sobre a verificação do(s) perigo(s) e a necessidade de aplicação da medida, ordenando a junção dos dados aos autos.

Não existindo qualquer processo, a referida comunicação dos dados é dirigida ao juiz da sede da entidade competente para a investigação criminal (n.º 3 do artigo 252.º-A). Neste caso, o juiz deve ordenar a transmissão dos dados ao Ministério Público competente[27].

Os dados celulares obtidos em violação do disposto no artigo 252.º-A constituem nulidade, nos termos do n.º 4 deste normativo legal[28]. No entanto, alguns autores, como Paulo Pinto de Albuquerque e Maia Costa, entendem que estamos perante prova proibida, ao abrigo do disposto no artigo 126.º, n.º 3.

2.8. Lei do Cibercrime

A Lei n.º 109/2009, de 15 de Setembro (Lei do Cibercrime) também prevê medidas cautelares e de polícia, que obedecem aos pressupostos anteriormente explanados. Assim, sinteticamente:

– Preservação Expedita de Dados

Trata-se da obtenção de dados informáticos específicos (incluindo dados de tráfego), que se encontram armazenados num sistema informático, e em que haja receio de que se possam perder, alterar ou deixar de estar disponíveis (cfr. artigo 12.º, n.º 1, da Lei do Cibercrime).

Ora, a preservação destes dados, normalmente, é ordenada pela autoridade judiciária competente, mas *"pode também ser ordenada pelo órgão de polícia criminal mediante autorização da autoridade judiciária competente ou quando haja urgência ou perigo na demora, devendo aquele, neste último caso, dar notícia imediata do facto à autoridade judiciária e transmitir-lhe o relatório previsto no artigo 253.º do Código de Processo Penal*", ao abrigo do disposto no artigo 12.º, n.º 2, da Lei do Cibercrime.

– Pesquisa de Dados Informáticos

[27] Paulo Pinto de Albuquerque considera que o n.º 3 do artigo 252.º-A é uma norma de prevenção criminal, que permite a localização celular sem existir um processo em curso e não prevê qualquer prazo para comunicação dos dados ao juiz. Por isso, é inconstitucional, in *Comentário do Código de Processo Penal à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem*, 3.ª edição actualizada, Lisboa: Universidade Católica Editora, 2009, págs. 670 a 672.

[28] "A localização celular prevista no art. 252.º-A do CPP, e igualmente no art. 9.º, n.º 5, da Lei 32/2008, de 17-07, não se confunde com a intercepção prevista no art. 189.º, n.ºs l e 2, do CPP, ao permitir que as autoridades de polícia criminal e as judiciárias requeiram dados sobre a localização celular, se necessário a afastar um perigo à vida ou ofensa à integridade física grave, em qualquer momento, e, se respeitarem a um processo crime em curso, é obrigatória a sua comunicação ao juiz no prazo máximo de 48 h; não respeitando a processo em curso a comunicação é feita ao juiz da sede da entidade competente para a investigação criminal e a violação deste formalismo importa nulidade", Acórdão do STJ de 08-01-2014, Armindo Monteiro, Processo n.º 7/10.0TELSB.L1.S1, *in* www.dgsi.pt.

Também se deve ter em atenção à previsão da alínea b) do n.º 3 do artigo 15.º da Lei n.º 109/2009, de 15 de Setembro (Lei do Cibercrime), nos termos da qual "*O órgão de polícia criminal pode proceder à pesquisa* (de dados informáticos)*, sem prévia autorização da autoridade judiciária, nos casos de terrorismo, criminalidade violenta ou altamente organizada, quando haja fundados indícios da prática iminente de crime que ponha em grave risco a vida ou a integridade de qualquer pessoa*".

"*…A realização da diligência é, sob pena de nulidade, imediatamente comunicada à autoridade judiciária competente e por esta apreciada em ordem à sua validação*" e "*é elaborado e remetido à autoridade judiciária competente o relatório previsto no artigo 253.º do Código de Processo Penal*", nos termos do artigo 15.º, n.º 4, alíneas a) e b), da Lei do Cibercrime.

– Apreensão de Dados Informáticos

Existindo dados ou documentos informáticos necessários à produção de prova, "*o órgão de polícia criminal pode efectuar apreensões, sem prévia autorização da autoridade judiciária, no decurso de pesquisa informática legitimamente ordenada e executada nos termos do artigo anterior, bem como quando haja urgência ou perigo na demora*", nos termos do artigo 16.º, n.º 2, da Lei do Cibercrime.

As apreensões efectuadas pelos OPC's estão sempre sujeitas a validação pela autoridade judiciária competente, no prazo máximo de 72 horas (n.º 4 do artigo 16.º da Lei do Cibercrime).

É de salientar que, ao abrigo do disposto no n.º 3 do artigo 16.º da Lei do Cibercrime, "*caso sejam apreendidos dados ou documentos informáticos cujo conteúdo seja susceptível de revelar dados pessoais ou íntimos, que possam pôr em causa a privacidade do respectivo titular ou de terceiro, sob pena de nulidade esses dados ou documentos são apresentados ao juiz, que ponderará a sua junção aos autos tendo em conta os interesses do caso concreto*".

2.9. Relatório

Os OPC's têm de elaborar relatório sobre as medidas cautelares e de polícia adoptadas, onde se descrevem as investigações levadas a cabo, os respectivos resultados, a descrição dos factos apurados e as provas recolhidas.

O relatório será remetido ao Ministério Público ou ao juiz de instrução, conforme a autoridade judiciária competente (para ordenar ou autorizar a medida) e a fase em que o processo se encontrar (inquérito ou instrução), nos termos do disposto no artigo 253.º, do Código de Processo Penal. Trata-se de um instrumento de controlo da actividade dos OPC's pela autoridade judiciária.

O relatório que contenha actos previstos nos artigos 252.º e 252.º-A, n.ºs 2 e 3, é sempre remetido ao juiz de instrução.

3. Documentos hierárquicos do Ministério Público

No âmbito da presente temática, indicam-se alguns documentos hierárquicos do Ministério Público que se afiguram relevantes:

– Parecer do Conselho Consultivo da Procuradoria-Geral da República n.º 15/95 e Circular da Procuradoria-Geral da República n.º 7/95, de 12 de Junho de 1995;

– Circular da Procuradoria-Geral da República n.º 8/2000, de 08-08-2000;

– Parecer do Conselho Consultivo da Procuradoria-Geral da República n.º 21/2000, de 28-08-2000;

– Circular da Procuradoria-Geral da República nº 6/2002, de 11-03-2002;

– Parecer do Conselho Consultivo da Procuradoria-Geral da República n.º 1/2008, de 11-01-2008;

– Parecer do Conselho Consultivo da Procuradoria-Geral da República n.º 28/2008, de 12-08-2008;

– Parecer do Conselho Consultivo da Procuradoria-Geral da República n.º 45/2012;

– Parecer do Conselho Consultivo da Procuradoria-Geral da República de 04-01-2013;

– Ordem de Serviço da Procuradoria-Geral da República n.º 4/2015.

IV. Hiperligações e referências bibliográficas

Hiperligações

Centro de Estudos Judiciários
www.dgsi.pt
www.ministeriopublico.pt

Referências bibliográficas

– ALBUQUERQUE, Paulo Pinto de, Comentário do Código de Processo Penal à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem, 3.ª edição actualizada, Lisboa: Universidade Católica Editora, págs. 646 a 673.

– ALMEIDA, Carlos Alberto Simões de, Medidas Cautelares e de Polícia do Processo Penal em Direito Comparado, Coimbra, Almedina, 2006, págs. 11 a 52.

– BRAZ, José, Investigação Criminal. A organização, o método e a prova: Os desafios da nova criminalidade, Coimbra, Almedina, 2009, págs. 197 a 238.

– BRITO, Fernando Manuel Castanheira de, Breve análise sobre a localização celular como «medida cautelar e de polícia» (art. 252.º-A do CPP), págs. 184 a 207.

– CUNHA, José Damião da, O Ministério Público e os Órgãos de Polícia Criminal no novo Código de Processo Penal, UCP, Porto, 1993, págs. 99 a 170.

– CUNHA, José Damião da, O Relacionamento entre Autoridades Judiciárias e Polícias no Processo Penal, *in* I Congresso de Processo Penal – Memórias – Coordenação de Manuel Monteiro Guedes Valente, Almedina, 2005, págs. 99 a 112.

– GASPAR, António da Silva Henriques, CABRAL, José António Henriques dos Santos, COSTA, Eduardo Maia, MENDES, António Jorge de Oliveira, MADEIRA, António Pereira, GRAÇA, António Pires Henriques da, Código de Processo Penal Comentado, 2.ª Edição Revista, Coimbra, Almedina, 2016, págs. 667 a 687, 699 a 705 e 888 a 897.

– Magistrados do Ministério Público do Distrito Judicial do Porto, Código de Processo Penal, Comentários e notas práticas, Coimbra Editora, 2009, págs. 620 a 623.

– MESQUITA, Paulo Dá, Direcção do Inquérito Penal e Garantia Judiciária, Coimbra Editora, 2003, págs. 121 a 163.

– MESQUITA, Paulo Dá, Repressão Criminal e iniciativa própria dos órgãos de polícia criminal, *in* I Congresso de Processo Penal – Memórias – Coordenação de Manuel Monteiro Guedes Valente, Almedina, 2005, págs. 55 a 87.

– SILVA, Germano Marques da, Direito Processual Penal Português: Do Procedimento (Marcha do Processo), Vol. III, Lisboa: Universidade Católica Editora, 2015, págs. 61 a 69.

– SOARES, Paulo, Meios de Obtenção de Prova no Âmbito das Medidas Cautelares e de Polícia, 2.ª Edição, Coimbra, Almedina, 2017.

– TEOTÓNIO, Henrique Pereira, Titularidade do Inquérito e Dependência Funcional das Polícias, Cadernos da Revista do Ministério Público, n.º 4, págs. 93 a 111.

– VALENTE, Manuel Monteiro Guedes, Teoria Geral do Direito Policial, 2.ª Edição, Coimbra, Almedina, 2009, págs. 239 a 270.

Título:
Meios de obtenção de prova e medidas cautelares e de polícia

Ano de Publicação: 2019

ISBN: 978-989-8908-54-4

Série: Formação Ministério Público

Edição: Centro de Estudos Judiciários

Largo do Limoeiro

1149-048 Lisboa

cej@mail.cej.mj.pt