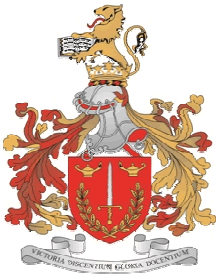
INSTITUTO SUPERIOR DE CIÊNCIAS POLICIAIS E SEGURANÇA INTERNA



André Francisco Dias Antunes

Aspirante a Oficial de Polícia

Dissertação de Mestrado Integrado em Ciências Policiais

XXIII Curso de Formação de Oficiais de Polícia

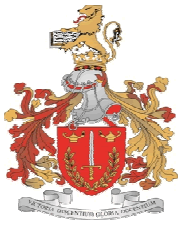
Recolha de Prova Digital – Correio Electrónico e Processo Penal

Da Problematização dos Regimes Aplicáveis e da Relevância da Actuação dos OPC's

Orientador:

Mestre João da Costa Andrade

LISBOA, 27 DE ABRIL DE 2011



Estabelecimento de Ensino	Instituto Superior de Ciências Policiais e Segurança Interna
Curso	XXIII CFOP
Orientador	Mestre João da Costa Andrade
Título	Recolha de Prova Digital – Correio Electrónico e Processo Penal: da Problematização dos Regimes Aplicáveis e da Relevância da Actuação dos OPC's.
Autor	André Francisco Dias Antunes Aspirante a Oficial de Polícia
Local de Edição	Lisboa
Data de Edição	Abril de 2011

Aos meus Pais,

"Simplesmente" por TUDO...

Agradecimentos

Os meus agradecimentos, longe de serem exaustivos e completos, são:

Aos meus pais, por lhes dever a exemplar educação, o amor, carinho, apoio, compreensão e ajuda que sempre me deram. Ao Pedro por ser o irmão forte e corajoso em lutar por aquilo que quer, e pela sua habilidade em superar todos os obstáculos.

Aos meus avós Luzia e Augusto, ao tio Quim-Tó e ao primo Carlos Vítor, pela cooperação, amparo, preocupação e orgulho que depositam em mim.

De igual modo agradeço à Joana, luz dos meus olhos, por ser o confortante alicerce a que recorri vezes sem conta, sem que nunca deixasse de ser a força dos meus passos e a fonte da minha inspiração: obrigado pelo amor, paciência e tolerância...

Ao meu Orientador, Mestre João da Costa Andrade, pela simplicidade, preocupação, disponibilidade e sabedoria com que me guiou na elaboração deste trabalho.

Aos Professores Doutores Germano Marques da Silva e Manuel da Costa Andrade, não só por me privilegiarem com os seus conhecimentos e dispensarem o seu tempo, bem como pela abertura e simplicidade com que guiaram as minhas entrevistas.

Ao Dr. Pedro Verdelho e ao Subintendente Dário Prates, pela sua reconhecida visão prática e legal sobre o tema, e pelos sábios conhecimentos e informações partilhadas.

Ao Subcomissário Celso Marques, pela incansável colaboração, experiência e disponibilidade, as quais sempre se fizeram sentir pela sua tão patente "amizade paternal".

Ao Subcomissário Paulo Mendes, Subcomissário Valverde e Chefe Camisa Pedro, por todos os conhecimentos e vivências "de terreno" que me transmitiram, e bem assim pelas ajudas que me prestaram ao longo do corrente ano.

Ao ISCPSI, pela formação e complemento educacional, único desta Casa.

Ao meu Curso, XXIII CFOP – "VT ADVENAE VENIMVS, VT FRATERI EXIMVS", pelos 5 primeiros anos de longos e inquebráveis laços de amizade. Agradeço em particular ao Rocha, por desde sempre o considerar um exemplo a seguir, pelos sábios conselhos, apoio e experiências partilhadas, e também a todos os que, de forma mais ou menos vincada, me presentearam com as suas "particularidades".

Termino agradecendo à Andreia Parente e ao *urubu* Ricardo Santos, por os considerar "familiares" exemplares e pela sempre respeitosa e humilde conduta que tiveram no cumprimento das minhas solicitações.

A Todos, **muito obrigado**!

Resumo

A obtenção de prova digital pode consubstanciar, nos dias de hoje, uma excelente forma de fazer justiça, sendo o correio electrónico a peça *sine qua non* seria inglório fazer referência a estes novos métodos de investigação. Os *e-mails* são, assim, o caminho que as polícias têm de desbastar para que se rompam as cortinas de alguns túmulos, ainda ocultos ou pouco desmistificados. O regime à luz do qual se regem estas matérias, terá de coar atentamente os valores a serem postos em causa, funcionando todo o enredo processual num desejável equilíbrio entre os aspectos constitucionais que protegem individualmente cada pessoa, e a própria luta contra a criminalidade.

Significa isto que a intercepção, acesso, ou apreensão de e-mails, podendo ou não configurar um meio oculto de investigação, revela-se como sendo um potente meio de (obtenção de) prova, importando que se esclareça um padrão de actuação, para que se afaste o carácter vago de algumas soluções legais.

Abstract

The acquisition of digital proof substantiates, in present day, an excellent form of providing justice, so long as e-mail is the tool that references these new investigative methods. E-mails are, therefore, the piece that police must unveil like the curtains covering some tombs, still hidden or barely demystified. The light regime that regulates these tools, must carefully tabulate the values being challenged, executing the procedural scenarios in a desirable balance between the constitutional aspects that individually protect each person, as well as the fight against crime.

This means that the interception, access, or apprehension of e-mails, if it can be set up as a concealed means of investigation, reveals itself to be a powerful method of (obtaining) proof, providing the existence of a clear action plan, in order to set aside the obscurity of certain legal solutions.

Palavras – Chave: Prova digital; correio electrónico; recolha; apreensão; intercepção.

Lista de Siglas

AJ – Autoridade Judiciária

APC – Autoridade de Polícia Criminal

CC – Código Civil

CCNURAL – Código de Conduta das Nações Unidas para os Responsáveis pela Aplicação das Leis

CDFUE – Carta dos Direitos Fundamentais da União Europeia

CP – Código Penal

CPP – Código de Processo Penal

CRP – Constituição da República Portuguesa

GNR – Guarda Nacional Republicana

JIC – Juiz de Instrução Criminal

LC – Lei do Cibercrime

LCE – Lei das Comunicações Electrónicas

LOIC – Lei de Organização da Investigação Criminal

LOPSP – Lei Orgânica da PSP

LOPOPC – Lei que define os Objectivos, Prioridades e Orientações de Política Criminal

LSI – Lei de Segurança Interna

MP – Ministério Público

OPC – Órgão de Polícia Criminal

PJ – Polícia Judiciária

PSP – Polícia de Segurança Pública

RMP – Revista do Ministério Público

ISP – Internet Service Provider

mms – Multimedia message service

sms – Short message service

VoIP – Voice over Internet Protocol

Índice

Agradecimentos ..... **III**

Resumo ..... **IV**

Abstract ..... **IV**

Lista de Siglas ..... **V**

Índice de anexos ..... **VIII**

Introdução **1**

Apresentação e justificação do tema 1

O objecto de estudo, os objectivos e as hipóteses 2

Metodologia Adoptada 3

Capítulo 1 – A Actividade Probatória em Processo Penal **4**

1.1 Introdução Capitular 4

1.2 Objectivos da Actividade de Recolha de Prova versus Direitos Fundamentais 5

1.3 Princípio da Atipicidade da Prova, Proibições de Prova e Princípio da Legalidade 8

1.4 Meios de Prova e Meios de Obtenção de Prova 11

1.5 Meios de Obtenção de Prova implicados nas Comunicações Electrónicas – Análise geral 14

1.5.1 O Regime das Buscas 15

1.5.2 O Regime da Apreensão de Correspondência 18

1.5.3 O Regime das Escutas Telefónicas 20

1.6 Conclusão Capitular 22

Capítulo 2 – Do Correio Electrónico e seu Enquadramento Jurídico em Geral **23**

2.1 Introdução Capitular 23

2.2 Correio Electrónico – Especificação Conceitual 24

2.2.1 Noção 24

2.2.2 Delimitação face a realidades próximas 27
2.2.3 Momentos de diferente valência axiológico-material 29
2.3 Breve Comentário às Alterações Introduzidas na Reforma do Código de Processo Penal de 2007 31
2.4 Valor e Validade da Prova Electrónico-Digital 35
2.5 Conclusão Capitular 38

Capítulo 3 – Regimes Aplicáveis ao Correio Electrónico e Relevância da Actuação dos OPC's 40
3.1 Introdução Capitular 40
3.2 A Expressão "qualquer outra correspondência" no Artigo 179.º do CPP – sua relevância 41
3.3 O Artigo 189.º do CPP – Ponderação à sua Proficiência 43
3.4. Do Momento Posterior à Comunicação e não da Intercepção 46
3.4.1 *E-mails* simplesmente recebidos *VS e-mails* recebidos e abertos 47
3.4.2 *E-mails* recebidos e impressos 49
3.5 As Soluções da Lei n.º 109/2009, de 15 de Setembro 50
3.6 O Papel dos OPC's na Actividade de Investigação Criminal 53
3.6.1 A missão de coadjuvação com as Autoridades Judiciárias 53
3.6.2 A PSP enquanto promotora de diligências fundamentais na preservação e recolha de prova digital – análise à luz das suas capacidades operacionais 56
3.6.3 A LOIC e o seu cunho de normativo orientador 58
3.7 Conclusão Capitular 60

Conclusão 61

Bibliografia 64

Índice de anexos

ANEXO 1 – Guião de entrevista a aplicar aos entrevistados civis 72

ANEXO 2 – Guião de entrevista a aplicar ao entrevistado polícia 73

ANEXO 3 – Entrevista ao Professor Doutor Manuel da Costa Andrade 74

ANEXO 4 – Entrevista ao Professor Doutor Germano Marques da Silva 82

ANEXO 5 – Entrevista ao Dr. Pedro Verdelho 88

ANEXO 6 – Entrevista ao Subintendente Dário Prates 96

ANEXO 7 – Manual de Boas Práticas para Recolha e Apreensão de Prova Digital – Departamento de Investigação Criminal da PSP 101

ANEXO 8 – Guia para Recolha e Interpretação dos Cabeçalhos Técnicos dos *E-mails* - DIAP de Lisboa 130

Introdução

Apresentação e Justificação do Tema

Está na ribalta, actualmente, um turbulento fenómeno caracterizado por duas faces "diametralmente opostas": por um lado tem-se assistido a um progresso científico exponencial no que respeita às novas formas de comunicação; por outro, existe o imprevisível risco que "está estreitamente ligado à inovação"[1], e que dela directamente depende. De facto, comunicar é uma tarefa que vai muito além do contacto pessoal, em razão da distância e dos meios disponíveis, tornando-se em algo virtual e muito característico da era digital em que vivemos. Impera, portanto, que a Polícia se socorra de métodos tecnologicamente nivelados com as capacidades criminógenas dos delinquentes, pois, como refere PEDRO CLEMENTE, "o recurso às novas tecnologias de informação favorece a previsão e a contenção de comportamentos ilícitos"[2].

Acontece que, embora estas matérias sejam de reconhecida importância, o seu assento legal levanta ainda algumas perplexidades. Conforme refere CRISTINA MÁXIMO DOS SANTOS, citando Miguel Caronell, "en pocos campos como en el de las comunicaciones electrónicas tiene un impacto mayor la globalización y todas sus consecuencias. Basta mencionar el fenómeno Internet y toda la problemática jurídica que existe a su alrededor para ilustrar el tamaño de los retos a los que se enfrenta cualquier esfuerzo regulador en este campo"[3].

Foi com sustento neste pensamento que encontrámos pertinência e interesse em estudar a forma como o correio electrónico pode ou deve ser usado em processo penal, no âmbito de uma investigação criminal. Até porque, consultado inicialmente o Código de Processo Penal (CPP) – nomeadamente no que se refere aos artigos 189.º e 179.º - e questionadas algumas pessoas com assento opinativo sobre estas matérias[4], verificou-se

[1] Anthony Guiddens (2006), *O mundo na era da globalização*, 6.ª edição, Editorial Presença, Lisboa, p. 17.
[2] Pedro Clemente (2009), "Polícia – O Caminho…", *in Estudos Comemorativos dos 25 Anos do Instituto Superior de Ciências Policiais e Segurança Interna em Homenagem ao Superintendente-Chefe Afonso de Almeida*, Novembro de 2009, Almedina, Coimbra p. 96.
[3] Cfr. "Notas sobre la regulación constitucional de los médios electrónicos de comunicación", *in Boletín Mexicano de Derecho Comparado*, n.º 104, ano XXXV, Maio-Agosto, 2002, p.373, *apud* Cristina Máximo dos Santos (2004), "As novas tecnologias da informação e o sigilo das telecomunicações" *in RMP*, Ano 25, n.º 99, Julho – Setembro, p. 90.
[4] QUIVY e CAMPENHOUDT consideram esta recolha de opinião com sendo entrevistas exploratórias informais – pelo facto de não integrarem textualmente o estudo, mas servindo-lhe de projecção inicial, cfr. Raymond Quivy e Luc Van Campenhoudt (1998), *Manual de Investigação em Ciências Sociais*, Gravida, Lisboa, p. 69.

que não existe um entendimento pacífico sobre como devem actuar os elementos policiais em matéria de correio electrónico – e de prova digital em geral.

Neste encadeamento, surgiu a seguinte questão (fruto do factor dúvida) como sendo o mote ou problema de investigação do presente trabalho: *Mediante que regime deverão actuar os OPC perante a possibilidade / necessidade de recolha de prova digital – em particular o correio electrónico – em sede de investigação criminal?*

O Objecto de Estudo, os Objectivos e as Hipóteses

Olhando à especificidade do correio electrónico enquanto matéria susceptível de tutela jurídico-penal, considera-se como objecto de estudo deste trabalho os artigos 189.º e 179.º do CPP, porquanto se constatar que o primeiro alarga o regime das intercepções telefónicas "às conversações ou comunicações transmitidas por qualquer meio técnico diferente do telefone, designadamente correio electrónico (…), mesmo que se encontrem guardadas em suporte digital"; e por se verificar que o segundo se poderá também referir ao correio electrónico, por constar na sua redacção que "o juiz pode autorizar ou ordenar, por despacho, a apreensão, mesmo nas estações de correios e de telecomunicações, de cartas, encomendas, valores, telegramas ou qualquer outra correspondência".

Pelo exposto, estabelecem-se os seguintes objectivos a atingir: compreender a dimensão penal e processual penal que o correio electrónico assume no ordenamento jurídico português; diferenciar possibilidades de cenários relativos ao correio electrónico investigado: *e-mail* por abrir *versus e-mail* aberto; *e-mail* guardado em computador *versus e-mail* impresso em papel; dar um contributo para a superação do arquétipo legal existente sobre o uso de mensagens de correio electrónico em processo penal, designadamente atendendo à confusa convergência de regimes, coando os seus pontos de principal aplicabilidade prática; e, por último, compreender, em jeito de "sinopse operacional", como se devem regular os Órgãos de Polícia Criminal (OPC's) e as Autoridades Judiciárias (AJ's) em matérias probatórias de tão sensível ingerência.

Para responder à pergunta de partida *supra* enunciada, tomam-se as seguintes hipóteses como ponto de partida:

1. O regime aplicável ao correio electrónico enquanto meio de obtenção de prova encontra-se consagrado no artigo 189º do CPP, funcionando em regime análogo ao das escutas telefónicas;

2. O regime aplicável ao correio electrónico enquanto meio de obtenção de prova cinge-se ao artigo 179º do CPP – apreensão de correspondência – porquanto o conceito de correio electrónico assim pode ser considerado;
3. Existe um regime especial, extravagante ao CPP, que é idóneo e apropriado à utilização de correio electrónico como prova penal;
4. Em matéria de correio electrónico deve optar-se por um regime tripartido, conforme se trate de "intercepção", de acesso quando o *e-mail* já está recebido, ou quando tenha havido uma impressão física do *e-mail*.

Metodologia Adoptada

O presente trabalho, cuja natureza é a de uma investigação teórica e descritiva, assenta numa arquitectura metodológica simples e bipartida.

Num primeiro momento, de recolha de informação através de um método teórico – revisão da literatura – contextualiza-se a problemática, trazendo à colação os conteúdos bibliográficos de referência, as legislações implicadas, a análise de doutrina e jurisprudência, bem como trabalhos, publicações e artigos que demonstrem especial relevância e interesse na matéria deste trabalho.

Num segundo momento, que primará pelo carácter de complementaridade e suporte qualitativo, recolheram-se impressões e pareceres de algumas entidades especialistas em Direito Penal e Processual Penal com especial domínio na área e no objecto de estudo desta dissertação – através da realização de entrevistas – para se tentar amenizar a complexa mescla legislativa em torno da problemática do correio electrónico[5].

Relativamente à estrutura do trabalho, esta segue três partes essenciais: a Introdução, o Desenvolvimento e a Conclusão. O Desenvolvimento subdivide-se, por seu turno, em três capítulos chave que afunilam a matéria do geral para o particular.

No primeiro capítulo aborda-se a actividade de recolha de prova em geral, fazendo-se referência a alguns meios particulares implicados nas comunicações electrónicas. No segundo capítulo, essencialmente conceptual, concretizam-se esclarecimentos sobre a natureza jurídica do correio electrónico e sua validade. O terceiro capítulo, por ser o último, versa concretamente sobre o objecto de estudo, fazendo a ponte para a concreta actuação dos OPC's.

[5] Assim se fez, dotando este método do importantíssimo factor presencial, auferindo-se o carácter pessoal que lhe está subjacente. Para tal, foram elaborados dois guiões de entrevista individuais – um direccionado para os entrevistados civis e o outro para o entrevistado policial.

Capítulo 1 – A Actividade Probatória em Processo Penal

"O Direito não pode esquecer a realidade concreta que o justifica e para a qual existe, sob pena de o divórcio entre o Direito e a Vida provocar aquilo a que um Jurista chamou de a 'revolta dos factos contra o código'"[6].

1.1 Introdução Capitular

O propósito do presente capítulo assenta essencialmente numa abordagem sumária das questões relativas ao instituto da prova em processo penal. Para tal, aborda-se inicialmente a incontornável dicotomia existente entre a actividade de recolha de prova e os direitos fundamentais dos cidadãos, sendo este o mote principal da actividade de prossecução da justiça penal de um Estado de Direito Democrático. Seguidamente, alude-se à questão dos meios de prova e de obtenção de prova, porquanto ser uma distinção essencial para a compreensão do enquadramento jurídico do correio electrónico, a discutir em capítulo próprio no presente trabalho.

Não menos importante será a referência ao princípio da atipicidade da prova, qualidade esta que permite a admissibilidade de qualquer meio de prova, mesmo que não previsto expressamente na lei, no pressuposto de não ofender os valores prestigiados pelo ordenamento jurídico, e bem assim às questões de legalidade e de proibição de prova que também importam analisar nesta senda.

Depois, definem-se e esclarecem-se os regimes de obtenção de prova implicados nas comunicações electrónicas, por ser óbvia e essencial a problematização dos limites em que poderão convergir em matéria de recolha de prova digital. Neste âmbito, não será, pois, nosso intuito, analisar profundamente cada um dos meios de obtenção de prova referidos. Há, antes, a necessidade de trazer à colação as suas normas e requisitos de aplicação, para que adiante se tente esclarecer qual ou quais poderão estar verdadeiramente relacionados com o problema em estudo.

[6] Fernando Pinto Monteiro *in* prefácio à obra *A Prova do Crime* de Fernando Gonçalves e Manuel João Alves (2009).

1.2 Objectivos da Actividade de Recolha de Prova versus Direitos Fundamentais

Conforme tem referido a doutrina, "o processo penal, como, aliás, os restantes processos, de um Estado de Direito Democrático, baseado na dignidade da pessoa humana, no respeito e na garantia de efectivação dos direitos e liberdades fundamentais do cidadão, como o nosso, numa perspectiva jurídico-processual, visa a aplicação da lei penal aos casos concretos, procurando garantir que nenhum responsável passe sem punição (*impunitum non relinqui facinus*) nem que nenhum inocente seja condenado (*innocentum non condennari*)"[7;8]. O que está em causa é toda uma estrutura legal de equilíbrio entre o direito de punir do Estado, os direitos dos indivíduos, a sua liberdade e segurança.

É com este espírito que iniciamos este registo, na certeza de que nenhum outro meio processual poderá trazer mais certezas a um concreto julgamento que uma prova bem substanciada, capaz de cimentar a convicção do julgador na sua tomada de decisão. É aliás a isto que remete a própria origem da palavra *probatio*, que por sua vez deriva do verbo *probare*, com o significado de demonstrar, reconhecer, formar juízo de algo. A actividade de recolha de prova trata-se, então, de um esforço de demonstração da existência ou veracidade daquilo que se alega como razão do direito que se defende, ou como argumento do direito que se contesta[9].

No entanto, para que efectivamente esta relação entre a construção da prova e o não bulir na esfera dos direitos humanos[10] se cumpra, impera a necessidade de o Estado "não apenas 'respeitar' os direitos e liberdades fundamentais, mas também 'garantir a sua efectivação'"[11]. A verdade processual, produto que se busca com a actividade de recolha de prova, não pode, pois, ser obtida a todo e qualquer custo. GERMANO MARQUES DA SILVA sustenta que a verdade que se busca em processo penal "é o resultado probatório processualmente válido, isto é, a convicção de que certa alegação singular de facto é

[7] Fernando Gonçalves e Manuel João Alves (2009), *A Prova do Crime – Meios Legais para a sua Obtenção*, Almedina, Coimbra, p.13.
[8] Neste sentido atente-se o artigo 11.º n.º 1 da Declaração Universal dos Direitos do Homem (princípio *in dubio pro reo*).
[9] Refere-se neste sentido o artigo 124.º do Código de Processo Penal (CPP), que, apesar de não definir explicitamente o conceito de prova, dá-nos uma noção de objecto de prova como sendo "todos os factos juridicamente relevantes para a existência ou inexistência do crime, a punibilidade ou não punibilidade do arguido e a determinação da pena ou da medida de segurança aplicáveis".
[10] A fórmula "*direitos humanos*", devido à tradução literal do inglês *human rights*, está generalizada como sinónimo de "*direitos do homem*", sendo esta a expressão que em português correcto se deverá usar.
[11] J.J. Gomes Canotilho e Vital Moreira (2007), *Constituição da República Portuguesa Anotada*, Vol. I, Coimbra Editora, Coimbra, p. 208.

justificadamente aceitável como pressuposto da decisão, por ter sido obtido por meios válidos" [12]. A verdade processual é, pois, uma certeza judicial e prática, não ontológica, sendo afastada a possibilidade da sua obtenção a todo o preço[13]. Acrescenta o Autor citado que não é fundamental a descoberta de uma *verdade absoluta*, sendo este o motivo principal para não existir um *poder ilimitado de produção de prova*. Refere ainda que "o *thema probandi* vai sendo delimitado em cada fase processual e limitados são também os meios de prova admissíveis no processo, os métodos para a sua obtenção e o momento e forma da sua produção"[14].

Neste sentido, a questão da aceitação (ou não) da prova recolhida em sede de Inquérito torna-se algo relativizada, em função da protecção, respeito e garantia dos direitos e liberdades fundamentais, uma vez que são estes a base e tarefa fundamental do próprio Estado [15]. Segundo MIGUEL JOSÉ FARIA, "a tarefa de garantir os direitos fundamentais expande-se pelos diversos órgãos de soberania e entidades públicas que neles se integram ou deles dependem, subordinando-os a todos ao mesmo fim, qual seja o de preservar a '*legalidade democrática*', o respeito pelos preceitos constitucionais e seu espírito. Para tanto, um sistema de complementaridade e dependência foi estabelecido pela Constituição de modo a que as leis, para serem válidas e eficazes, tenham de se conformar com a intervenção e fiquem sujeitas à fiscalização dos outros órgãos. Assim, essa vigilância e condicionamento mútuo funcionarão como garantia dos cidadãos contra a tentação do poder para desrespeitar os direitos fundamentais"[16]. O que importa será, então, a existência a todo o tempo de um equilíbrio entre esta tarefa do Estado e a finalidade primordial do processo penal: a procura da realização da justiça[17].

Em frágil tese, a questão dos Direitos Fundamentais apenas poderia constar como "fonte inibidora" do poder repressivo (e de justiça) do Estado, em situações em que concretamente existisse dúvida na adequação da pena à hipotética conduta criminal do arguido. Acontece que tal cenário apresenta inúmeras lacunas, visto apenas prever uma

[12] João de Castro Mendes, *Do Conceito de Prova em Processo Civil*, p.741, *apud* Germano Marques da Silva (2008), *Curso de Processo Penal* II, 4.ª edição, Editorial Verbo, Lisboa, p. 130.
[13] Germano Marques da Silva, *op. cit.*, p. 130
[14] *Idem, ibidem.*
[15] Cfr. os artigos 2.º e 9.º al. *b)* da CRP.
[16] Miguel José Faria (2001), *Direitos Fundamentais e Direitos do Homem*, volume I, 3.ª Edição Revista e Ampliada, Instituto Superior de Ciências Policiais e Segurança Interna, Lisboa.
[17] Por exemplo, a utilização de diários pessoais como meio de prova está dependente do conteúdo dos mesmos, sendo necessário efectuar uma ponderação entre os direitos fundamentais do autor e o interesse do Estado e da sociedade na descoberta da verdade e na realização da justiça. Tal ponderação deve ter em conta os princípios da necessidade e da proporcionalidade, bem como a gravidade do crime e a existência de outros meios de prova.

supra protecção dos indivíduos no pós recolha de prova e constatação da sua aparente insuficiência. Este regime jamais se poderia enquadrar na maturidade social e jurídica de uma democracia social como a nossa, pois a tutela dos direitos fundamentais é uma constante protecção do Homem, antes e depois da actividade de recolha de prova. Ensina JOSÉ CARLOS VIEIRA DE ANDRADE que os direitos fundamentais são hoje, por maioria de entendimento, os postulados elementares de uma vida livre e digna, tanto para o indivíduo – isoladamente – como para a sua vivência em comunidade[18].

Feita esta primeira aproximação aos desígnios humanos e constitucionais que se projectam como garantia do respeito e legalidade ínsitos a qualquer actividade de recolha de prova, parece-nos oportuno fazer uma brevíssima referência a algumas esferas de protecção implicadas directamente nas comunicações electrónicas (onde ocupa lugar cimeiro o correio electrónico), enquanto parte de um gigantesco novelo chamado *Informática*, ou, se quisermos ser mais precisos, *Internet*[19]. Salientam-se então como pano de fundo alguns direitos, tais como: i) o direito à privacidade ou direito *ao respeito pela vida privada* dos cidadãos conforme define o artigo 7.º da Carta dos Direitos Fundamentais da União Europeia (CDFUE). Também o artigo 26.º da CRP a todos reconhece o direito à reserva da intimidade da vida privada e familiar[20]; ii) a salvaguarda da inviolabilidade das comunicações[21], também como direito garantido aos cidadãos no texto constitucional: "O domicílio e o sigilo da correspondência e dos outros meios de comunicação privada são

[18] José Carlos Vieira de Andrade (2009), *Os Direitos Fundamentais na Constituição Portuguesa de 1976*, 4.ª Edição, Almedina, Coimbra.

[19] Relativamente à *Internet*, diz-nos BENJAMIM SILVA RODRIGUES que "só com a Internet se dá uma 'revolução' como nunca se havia verificado anteriormente. A Internet surge como o 'instrumento chave e o símbolo deste novo sistema tecnológico' que invade todos os aspectos da nossa vida. A Internet surge como uma parte única e específica da actual infra-estrutura da informação, por quatro razões: i) é uma arquitectura aberta; ii) é uma arquitectura repartida: os diferentes conteúdos informacionais e serviços são fornecidos por diversas entidades, ao longo dos diversos modos da Internet; iii) é uma arquitectura com acesso tendencialmente gratuito: ainda que se tenha que pagar por um certo hardware ou software para possuir os meus de aderir à Internet, todavia, aí instalados, pode viajar-se e aceder-se à informação de forma gratuita; iv) a lógica do '*pay-as you-go-use*': os utilizadores não sofrem custos financeiros pelo uso directo da Internet, tendo a mesma deixado de se limitar ao universo dos investigadores e universidades, onde originariamente nasceu para se 'democratizar' e estender a sua utilização a qualquer individuo que possua os meios técnicos para a ela aceder. Mas a Internet é também uma 'relação de relações', ou melhor, um n de relações", cfr. Benjamim Silva Rodrigues (2008), *Das Escutas Telefónicas – A Monitorização dos Fluxos Informacionais e Comunicacionais*, Tomo I, Coimbra Editora, Coimbra, p.42.

[20] Originariamente o direito à privacidade tem a sua consagração expressa em 1966 no artigo 80.º do Código Civil (CC), o qual, epigrafado de "Direito à reserva sobre a intimidade da vida privada", consagrou, no seu n.º 1, que "Todos devem guardar reserva quanto à intimidade da vida privada de outrem".

[21] Sobre este preceito veja-se com grande especificidade o artigo 4.º da Lei n.º 41/2004 de 18 de Agosto (que transpõe para a ordem jurídica nacional a Directiva n.º 2002/58/CE, do Parlamento Europeu e do Conselho, de 12 de Julho, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas).

invioláveis" – artigo 34.º da CRP; iii) o direito à palavra[22]; iv) por último o direito à autodeterminação informacional. GOMES CANOTILHO E VITAL MOREIRA admitem que o direito à autodeterminação informacional se traduz numa densificação de feixe de direitos através dos quais se pretende impedir que o homem se transforme num "simples objecto de informações"[23], dando a possibilidade a cada pessoa de controlar a informação disponível a seu respeito.

Citamos de seguida parte do relatório do Acórdão (ACR) do Tribunal da Relação de Coimbra n.º 1265/06 de 17 de Maio, pois reforça o uso destas prerrogativas: "(…) Na medida em que os registos cuja obtenção se pretende respeitam a telecomunicações, que estas estão abrangidas por uma garantia de inviolabilidade e sigilo e por uma garantia de reserva de decisão judicial, com consagração constitucional e legal artigos 32.º, n.º 4, e 34.º, nºs 1 e 4, da Constituição da República Portuguesa (CRP), artigo 17.º, n.º 2, da Lei no 91/97, de 1 de Agosto, e artigo 4º da Lei n.º 41/2004, de 18 de Agosto e que a obtenção de tais registos, relativos a dados de tráfego, se traduz numa ingerência nas comunicações, devem os mesmos ser obtidos de acordo com o regime decorrente dos artigos 187.º a 190.ºe 269.º, n.º 1, al. c), do Código de Processo Penal"[24].

1.3 Princípio da Atipicidade da Prova, Proibições de Prova e Princípio da Legalidade[25]

Não há dúvida que o princípio da investigação ou da verdade material, sem prejuízo da estrutura acusatória do processo penal, tem valor constitucional. Porém, e como já referimos anteriormente, só a verdade material, obtida de forma processualmente válida, interessa ao Estado de Direito. O instituto da prova, assumido que é o vastíssimo leque de questões que pode abarcar, dota-se, pois, de regras muito próprias no que concerne ao seu assento legal. Vem desde logo estatuído na alínea *d)* do n.º 3 do

[22] MANUEL DA COSTA ANDRADE defendia antes das alterações introduzidas pela Lei n.º 59/98, de 25 de Agosto, que o alargamento das escutas telefónicas só se poderia dar até onde se tratasse de formas de comunicação oral, que possibilitassem a emissão e a recepção da própria palavra falada, excluindo-se, assim, "formas de comunicação como o *telegrafo* ou o *telefax*. (…) Isto por ser manifesto que a intromissão indevida nas comunicações telegráficas não actualiza o atentado ao *direito à palavra*, que constitui um dos coeficientes de maior peso da danosidade social das escutas telefónicas" – cfr. Manuel da Costa Andrade (1992), *Sobre as Proibições de Prova em Processo Penal*, Coimbra Editora, Coimbra, pp. 271 e 275.

[23] J.J. Gomes Canotilho e Vital Moreira (2007), *op. cit.*, p. 551.

[24] Consultável em: http://www.dgsi.pt/jtrc.nsf/0/2a93252854f5d54c8025717d00377214?OpenDocument.

[25] Aludimos a estas questões, embora que de forma breve e algo teórica, por ser manifesta a possibilidade de ingerência em métodos ocultos ou proibidos de investigação em sede de recolha e tratamento de prova digital – designadamente no que se refere ao correio electrónico como parcela maioral das comunicações electrónicas.

artigo 61.º do CPP, que, "recaem em especial sobre o arguido os deveres de sujeitar-se a diligências de prova (…) ordenadas e efectuadas por entidade competente", isto é, "a todas as que se entenderam como necessárias para a descoberta da verdade e a realização da justiça – sendo a regra a da atipicidade das diligências da prova – desde que não estejam proibidas por lei – cfr. artigo 125.° do CPP"[26]. Este artigo, por sua vez, consagra o princípio da legalidade em matéria de prova, desde logo através da sua clara epígrafe: "Legalidade da prova". Sem prejuízo deste princípio, constituem objecto de prova todos os factos juridicamente relevantes para a existência ou inexistência do crime, a punibilidade ou não punibilidade do arguido e a determinação da pena ou da medida de segurança aplicáveis – artigo 124.º do CPP.

Ora, quando se aborda tão complexo e vasto assunto como é o das proibições de prova, é inevitável começar por citar o Autor que em Portugal tem estudado o tema com profundidade, e segundo o qual, "em nome de uma 'exigência de superioridade ética' do Estado, das suas 'mãos limpas' na veste de promotor da justiça penal, a violação da proibição de provas – que significaria o 'encurtamento da diferença ética que deve existir entre a perseguição do crime e o próprio crime' – é hoje uma questão de actual e de premente abordagem, uma vez que, sob a égide de uma justiça penal eficaz, se vem mobilizando a doutrina e a jurisprudência para um 'estado de necessidade de investigação'"[27].

Neste sentido, as proibições de prova são autênticos limites à descoberta da verdade material, sendo certo que a gravidade do crime a perseguir não será, por si só e enquanto tal, razão suficiente para legitimar a danosidade social da violação das proibições de prova.

Nos termos do artigo 126.º n.º 1 do CPP, que repete o artigo 32.º n.º 8 da CRP, são inadmissíveis e, por isso, nulas as provas obtidas mediante tortura, coacção ou, em geral, ofensa da integridade física ou moral das pessoas. MANUEL DA COSTA ANDRADE considera este artigo (ou o assunto a que se refere) como a "manifestação mais inequívoca e normativamente mais consistente e congruente (na relação: *proibição de produção – proibição de valoração*) de proibição de prova"[28].

Nos ensinamentos do Autor, o caso específico da *tortura* não deve suscitar dúvidas quanto à sua "proscriação invencível (…) que, como MAIHOFER acentua, atinge no coração

[26] Cfr. ACR do Tribunal da Relação do Porto, n.º 0844093 (JTRP00041933), de 10-12-2008. Negrito nosso. Consultável em: http://www.dgsi.pt/jtrp.nsf/0/673fcb5dc0168da6802575220056a553?OpenDocument.
[27] Manuel da Costa Andrade, *op. cit.*, p. 73.
[28] *Idem*, p. 209.

as exigências de uma *praxis* jurídico-penal formalizada e conforme à justiça *justizförmige*. Seja qual for a dignidade do fim invocado, argumenta na mesma linha HASSEMER, ao lançar mão da tortura, 'o Estado serve-se de um meio que degrada moralmente o arguído, o objectiviza e funcionaliza. O torturado é degradado à categoria de mera fonte de informações, deixando de ser encarado e tratado como portador de direitos. O Estado comporta-se como um qualquer outro que utiliza o poder fáctico para a imposição dos seus interesses"[29]. Considerações idênticas poderiam adiantar-se a propósito do sem número de outros métodos de prova legalmente inadmissíveis.

Em matéria de sujeitos processuais activos neste sector dos métodos proibidos de prova, encontram-se os agentes do Estado e também qualquer particular que seja interveniente. Quanto aos sujeitos passivos, temos não só o arguido e as testemunhas, mas também o assistente, partes civis, o perito ou o intérprete.

Fazendo a ponte para o n.º 2 do artigo 126.º, esclarece-se o que se deve entender por métodos de prova ofensivos da integridade física ou moral das pessoas, que a lei proíbe, ainda que consentidos pelo visado.

Já a redacção do n.º 3 do artigo 126.º do CPP, resultante da reforma processual de 2007, começa por fazer uma ressalva de permissão para "os casos previstos na lei". Assim, não são meios proibidos de prova as buscas domiciliárias, as apreensões de correspondência, as escutas telefónicas, o registo de voz e imagem, o tratamento de dados pessoais para fins de investigação policial, a quebra do dever de segredo profissional, desde que respeitados os pressupostos muito rigorosos da lei processual penal, de cariz materialmente constitucional. Numa outra leitura, verifica-se como propósito deste n.º 3 clarificar que as proibições de prova relativas às intromissões não consentidas na vida privada, domicílio, correspondência ou telecomunicações, têm a mesma força e efeito que as previstas nos n.º 1 e 2 do mesmo artigo; a ausência, no antigo n.º 3, do segmento "não podendo ser utilizadas", que sempre constou do n.º 1, e que a reforma acrescentou ao dito n.º 3, tornou claro e definitivo o que, em nosso entender, já se encontrava no anterior espírito da lei.

Nestes casos, contrariamente aos previstos no n.º 2, se o consentimento do titular dos direitos afectados for válido, jamais se poderá falar sobre nulidade de prova, designadamente por *intromissão na vida privada*, no *domicílio*, na *correspondência* ou nas *comunicações*. É o que acontece, por exemplo, nos casos das mensagens voluntariamente

[29] Maihofer e Hassemer, *apud* Manuel da Costa Andrade, *op. cit.*, p. 210.

gravadas num *voice-mail* alheio[30]. Nesses casos, como refere MANUEL DA COSTA ANDRADE, "a gravação *consentida* (ou a sua utilização) configura a forma paradigmática de exclusão do ilícito típico (…) não por força de qualquer *justificação*, *ex vi* consentimento, da lesão do bem jurídico", mas antes pela "exclusão da tipicidade por força de insuprível ausência de lesão do bem jurídico"[31].

Porém, o consentimento, para além de abranger as situações em que o direito lesado é livremente disponível, pressupõe a efectiva intervenção do respectivo titular e não da pessoa que tiver disponibilidade sobre ele[32].

Nesta conformidade, podemos desde já concluir que o regime da legalidade da prova, enquanto "imperativo de integridade judiciária", que tanto versa sobre os meios de prova, como os meios de obtenção de prova, vem assim comprimir o princípio da livre apreciação da prova decorrente do artigo 127.º do CPP, estabelecendo as correspondentes proibições de produção ou de valoração de prova.

Por outro lado e como segunda conclusão, "tratando-se de prova proibida, a mesma deve ser oficiosamente conhecida e declarada em qualquer fase do processo, surgindo como autênticas nulidades insanáveis", a par daquelas que expressamente integram o catálogo do artigo 119.º[33].

1.4 Meios de Prova e Meios de Obtenção de Prova

Os meios de prova, enquanto disciplina presente no CPP, ocupam o Título II, do Livro III, previstos nos artigos 128.º a 170.º[34], constituem um leque de meios que a lei disponibiliza ao intérprete para que este possa atingir um determinado resultado, sendo este, por sua vez, fruto da demonstração da realidade dos factos, isto é, fruto da *prova*. Para FERNANDO GONÇALVES e MANUEL ALVES, "a *prova* consiste (…) numa actividade apta a

[30] Cfr. ACR da Relação do Porto de 17/12/1997, ACR da Relação de Évora de 4/12/2001 e de 05/02/2003.
[31] Manuel da Costa Andrade, *op. cit.*, p. 251.
[32] Nesse sentido, o ACR do Tribunal Constitucional n.º 507/94, de 14 de Julho, que julgou inconstitucional a interpretação segundo a qual a busca domiciliária em casa habitada e as subsequentes apreensões efectuadas durante aquela diligência podem ser realizadas por OPC, desde que se verifique o consentimento de quem, não sendo visado por tais diligências, tiver a disponibilidade do lugar de habitação em que a busca seja efectuada.
[33] Cfr. ACR do Tribunal da Relação do Porto n.º 0715930 de 26-03-2008. Consultável em: http://www.dgsi.pt/jtrp.nsf/c3fb530030ea1c61802568d9005cd5bb/24cd01e84ff51ff88025741e0034cc7e?OpenDocument&Highlight=0,imagens,v%C3%ADdeo,prova.
[34] Dispõe também o artigo 340.º do CPP, no n.º 1, que, "O tribunal ordena, oficiosamente ou a requerimento, a produção de todos os meios de prova cujo conhecimento se lhe afigure necessário à descoberta da verdade e à boa decisão da causa".

produzir no juiz a convicção da verdade ou não de uma afirmação[35]. Ainda assim, e indo ao encontro do conceito de *meios de prova*, JOSÉ MARIA ASENCIO MELLADO, citado por Germano Marques da Silva, defende que para além de actividade, a *prova* "é também garantia de realização de um processo justo, de eliminação do arbítrio, quer enquanto a demonstração da realidade dos factos não há-de procurar-se a qualquer preço, mas apenas através de meios lícitos, quer enquanto através da obrigatoriedade de fundamentação das decisões de facto permite a sua fiscalização através dos diversos mecanismos de controlo de que dispõe a sociedade"[36].

Desta forma, os meios de prova são todos "os elementos de que o julgador se pode servir para formar a sua convicção acerca de um facto"[37], quer seja através do recurso a prova pessoal ou prova real, no sentido em que podem existir meios de prova resultantes de uma ou várias pessoas – i.e. declarações de testemunhas – e meios de prova advenientes de coisas ou objectos, designadamente pela observação de instrumentos ou documentos envolvidos num determinado crime[38].

Actualmente podemos encontrar o instituto dos meios de prova subdividido em 6 grandes áreas: i) a prova testemunhal; ii) a prova por acareação; iii) a prova por reconhecimento de pessoas ou objectos; iv) a prova por reconstituição do facto; v) a prova pericial; vi) a prova documental.

A primeira, com grande importância para todo o processo penal, constitui-se essencialmente como sendo na expressão de Bentham, "os olhos e os ouvidos da justiça. É por meio delas que o juiz vê e ouve os factos que aprecia"[39]. Assim, a prova testemunhal tem essencialmente como objecto os "factos juridicamente relevantes" [40] de que a testemunha tenha conhecimento ou memória.

A segunda, tendo por fundamento a existência anterior de depoimentos antinómicos e a necessidade de descoberta da verdade, é um "meio de prova que consiste no confronto directo e pessoal entre as pessoas que prestaram declarações contraditórias no processo, e

[35] Fernando Gonçalves e Manuel João Alves, *op.cit.*, p. 123.
[36] José Maria Asencio Mellado, *Prueba Prohibida y Prueba Preconstituida*, p. 16, *apud* Germano Marques da Silva, *op. cit.*, p. 111.
[37] Antunes Varela, J. Miguel Bezerra e Sampaio e Nora, "Manual de Processo Civil", p. 452, citado em Magistrados do Ministério Público do Distrito Judicial do Porto (2009), *Código de Processo Penal – Comentários e Notas Práticas*, Coimbra Editora, Coimbra, p. 437.
[38] Por exemplo, no caso de uma busca, o meio de prova não é o acto da busca em si mesmo, mas os objectos a cuja apreensão a mesma se destina.
[39] José da Cunha Navarro de Paiva, Tratado Theorico e Prático das Provas no Processo Penal, p.33, *apud* Germano Marques da Silva, *ob. cit.*, p. 162.
[40] Fernando Gonçalves e Manuel João Alves, *op. cit.*, p. 151.

tem por finalidade esclarecer depoimentos divergentes sobre um ou mais factos"[41]. Já a prova por reconhecimento baseia-se na convicção da pessoa que vai reconhecer, de que está perante um indivíduo ou coisa previamente conhecida, e que apenas trará à colação a reafirmação de um elemento de prova previamente admitido no processo[42].

A reconstituição do facto, embora que um pouco menos fiel, baseia-se num esforço de reprodução das condições prováveis em que os factos terão ocorrido, de modo a adquirir o máximo de certezas relativamente ao resultado que os factos produziram[43], e a perícia "(…) tem lugar quando a percepção ou a apreciação dos factos exigirem especiais conhecimentos técnicos, científicos ou artísticos"[44].

Por último, a prova documental resume-se à junção ao processo de documento[45] capaz de sustentar e validar uma convicção ou de fazer fé de determinada conduta.

Em determinado tipo de matérias, assume especial importância aludir às providências cautelares quanto aos meios de prova, em razão da sua especificidade e risco de perda. Neste âmbito, trazemos à colação o artigo 249.º do CPP, segundo o qual "compete aos órgãos de polícia criminal, mesmo antes de receberem ordem da AJ competente para procederem a investigações, praticar os actos cautelares[46] necessários e urgentes para assegurar os meios de prova". Mais uma vez verifica-se aqui, como fim principal da norma, o assegurar dos meios de prova, por estes serem, por si mesmos, fonte de convencimento do tribunal. Nos ensinamentos de GERMANO MARQUES DA SILVA, esta é uma das fontes de diferenciamento entre os meios de prova e os meios de obtenção de prova – visto os segundos serem apenas os instrumentos que permitem a obtenção daqueles meios ou elementos de convicção (perspectiva lógica).

---

[41] *Idem*, p. 174.

[42] Relativamente às formalidades exigidas no artigo 147.º do CPP, a sua omissão "não constitui uma nulidade insanável, mas antes um meio de prova que padece do vício de inexistência, pelo que o mesmo não pode ser valorado por não ter o valor probatório que legalmente lhe é exigido" *in* ACR do Tribunal da Relação do Porto n.º 0514155 de 15-02-2006. Disponível para consulta em: http://www.dgsi.pt/jtrp.nsf/d1d5ce625d24df5380257583004ee7d7/f0bc5863ddd1c7618025711b004fae50?OpenDocument.

[43] *Vide* artigo 150.º n.º 1 do CPP)

[44] Cfr. artigo 151.º do CPP. No mesmo sentido diz-nos GERMANO MARQUES DA SILVA que *perícia* é a "actividade de percepção ou apreciação dos factos probandos efectuada por pessoas dotadas de especiais conhecimentos técnicos, científicos ou artísticos" – *ob. cit.*, p. 197.

[45] O artigo 164.º n.º 1 do CPP define documento como a "declaração, sinal ou notação corporizada em escrito ou qualquer outro meio técnico, nos termos da lei penal".

[46] Esclarece MANUEL GONÇALVES que "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 AJ competente." Cfr. Manuel Lopes Maia Gonçalves (2009), *Código de Processo Penal Anotado*, 17.ª edição, Almedina, Coimbra, p. 598.

Num outro apontamento, importa analisar, ainda que de forma breve, os meios de obtenção de prova[47]. Tal como refere o Autor *supra* referido, os meios de obtenção de prova são instrumentos de que as AJ's dispõem para que possam investigar e recolher meios de prova[48]. Ainda na linha deste Autor, existe uma segunda perspectiva de diferenciamento entre meios de prova e de obtenção de prova (técnico-operativa), que caracteriza os segundos pelo modo e momento da sua aquisição no processo – sobretudo no inquérito – como sendo "modos de investigação" para a obtenção dos meios de prova, sendo estes, novamente, entendidos como fontes de convencimento do julgador.[49]

No entanto, poderá existir uma certa convergência conceptual relativamente a estes dois termos tão ligados, nomeadamente no que se refere, por exemplo, às escutas telefónicas[50]. Atente-se que as escutas, *de per si*, encontram-se reguladas em capítulo próprio dentro do título referente aos *meios de obtenção de prova* do CPP. No entanto, se atendermos às gravações que se obtêm (que não deixam de ser "escutas"), já poderemos cair no feixe dos *meios de prova*. Impera, então, a delimitação de uma linha divisória (embora que ténue), entre aquilo que se subsume à actividade de recolha da prova, e aquilo que consubstancia o produto final daquilo que se obteve (por determinados *meios*).

Não aludiremos individualmente a cada um dos meios de obtenção de prova existentes, dado que tal sempre extravasaria os limites do presente estudo, e ainda porque trataremos posteriormente aqueles que mais relevam para o presente trabalho.

1.5 Meios de Obtenção de Prova implicados nas Comunicações Electrónicas – Análise geral

É assumida pela lei portuguesa[51] a possibilidade de utilizar, paralelamente a outras comunicações, as mensagens de correio electrónico como meio de prova em processo penal[52]. Todavia, parece algo nebulosa a "escolha" de regimes legais nos quais este tipo de

[47] Que se contêm no Título III, do Livro III da Parte Primeira do CPP, entre os artigos 171.º a 190.º. São eles: os exames, as revistas e buscas, a apreensão e as escutas telefónicas.
[48] Acrescenta o Autor que os meios de obtenção de prova "não são instrumentos de demonstração do *thema probandi*, são instrumentos para recolher no processo esses instrumentos". Cfr. Germano Marques da Silva, *op. cit.*, p. 233.
[49] *Idem*, p. 234.
[50] Exemplo escolhido devido à proximidade do regime das escutas com o do correio electrónico.
[51] Designadamente nos Artigos 125.º, 179.º n.º 1 e 189.º n.º1 do CPP.
[52] Pedro Verdelho (2004), "A obtenção de prova no ambiente digital" *in RMP*, Ano 25, n.º 99, Julho – Setembro, p. 122, acrescentando que o Estado reconhece que "as mensagens de correio electrónico podem revelar-se importantes fontes de material probatório (…) podendo ser usadas com essa finalidade".

prova se possa enquadrar. Neste sentido, faremos de seguida uma breve alusão aos regimes que poderão ser convergentes em matéria de recolha de prova digital.

1.5.1 O regime das buscas

A matéria das buscas – tema inscrito no Título III do Livro III do CPP como meio de obtenção de prova – consigna, *lato senso*, as diligências processuais que aludem à procura, em lugares reservados e não acessíveis ao público[53], de objectos ou indícios respeitantes a um determinado crime, e capazes de ajudarem a comprová-lo (conforme artigo 174.º do CPP). MANUEL GUEDES VALENTE define busca como sendo "a operação desenvolvida pela AJ ou por OPC (…) no intuito de obter indícios probatórios (…), para serem carreados para o processo de modo a que se possa prosseguir os fins da investigação: a realização da justiça (…)"[54].

A regra será, portanto, a da prévia autorização judicial para que se possam efectivar as buscas. O novo n.º 4 do artigo 174.º[55] surge com a pretensão de evitar a emissão de mandados de busca sem data definida, impedindo assim que viessem a ser cumpridos decorrido um qualquer hiato temporal após a sua emissão[56].

Todavia, as buscas podem também integrar o formato de medida cautelar e de polícia[57], não dependendo de prévia autorização da AJ competente, conforme legalmente previsto no artigo 251.º do CPP. Estes casos – em tudo semelhantes às excepções previstas no n.º 5 do 174.º – são em nosso entender tão importantes como os primeiros, embora se exclua a possibilidade de realizar buscas domiciliárias sem prévia autorização[58]. Aqui impera, obviamente, um importante requisito formal que consiste na *urgência* e

[53] Fernando Gonçalves e Manuel Alves definem *lugar reservado e não acessível ao público* como sendo "todo aquele que, embora possa revelar factos da vida privada do arguido ou de qualquer outra pessoa que deva ser detida, não seja considerado domicílio destes, nomeadamente, garagens, barracões ou outras dependências para guarda de materiais de construção, alfaias agrícolas, ferramentas ou outros utensílios domésticos, veículos automóveis, etc…". Cfr. *op. cit.*, p. 212.
[54] Manuel Monteiro Guedes Valente (2005), *Revistas e buscas*, Almedina, Coimbra, p. 45.
[55] Que advém da revisão imposta pela Lei n.º 48/2007, de 29 de Agosto e cuja redacção é: "O despacho previsto no número anterior tem um prazo de validade máxima de 30 dias, sob pena de nulidade".
[56] *Vide* Paulo Pinto de Albuquerque (2009), *Comentário do Código de Processo Penal à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem*, 3ª edição actualizada, Universidade Católica Portuguesa, Lisboa, p. 470 a 472.
[57] Nos ensinamentos de MANUEL GUEDES VALENTE, medidas cautelares e de polícia são todos os "actos cautelares, actos de natureza pré-processual e de competência própria que se mostrem não só necessários e urgentes como também adequados e menos onerosos para os direitos do cidadão e que se destinem assegurar os meios de prova". Cfr. Manuel M. Guedes Valente (2009), *Processo Penal – Tomo I*, Almedina, Coimbra, p. 293.
[58] Estas terão sempre de ser ordenadas ou autorizadas pelo juiz (art. 177.º do CPP).

necessidade em realizar a diligência[59]. Neste sentido, e porque o próprio espírito da lei assim impele, perder-se-ia a utilidade da busca se não fosse efectuada em momento imediato. Estes casos são, como refere MANUEL GONÇALVES, aqueles em que "os órgãos de polícia criminal podem ir além dos poderes já conferidos por outras disposições, realizando revistas e buscas não domiciliárias mesmo sem prévia autorização judiciária, desde que a demora na obtenção dessa autorização faça perder a utilidade da diligência ou a ponha em grave risco de perder-se"[60]. Neste mesmo sentido, se atendermos à al. c) do n.º 5 do artigo 174.º, facilmente estabelecemos um paralelismo de semelhança com o que se consagra no artigo 251.º. Porém, enquanto que na busca praticada como meio de obtenção de prova o *periculum in moram* apenas legitima o acto em caso de detenção em flagrante delito, na busca levada a cabo como medida cautelar e de polícia basta haver fuga iminente de um suspeito para que o OPC proceda à busca.[61]

Feita esta primeira triagem conceptual, podemos subdividir o tema das buscas em três grandes domínios: as buscas não domiciliárias, as buscas domiciliárias e as buscas em escritório de advogado, em consultório médico e em estabelecimento oficial de saúde. Em relação às buscas não domiciliárias, como já referido anteriormente, vigora uma dualidade de regimes, que tanto pode pender para a busca enquanto meio de obtenção de prova, como para a busca enquanto medida cautelar e de polícia.

No que concerne às buscas domiciliárias, o seu regime jurídico é algo complexo. Apesar da restrição ao direito fundamental de inviolabilidade do domicílio, com vista à aquisição de prova, não constituir obtenção de prova por meio proibido, existe vasta doutrina e jurisprudência a pronunciarem-se sobre o tema. De forma sumária, existem dois momentos de diferente valência temporal em que as buscas domiciliárias se podem realizar: durante o dia (entre as 7 e as 21 horas) e durante a noite (entre as 21 e as 7 horas). As primeiras, sendo a regra, só podem ser ordenadas ou autorizadas pelo juiz, salvo em casos de consentimento ou flagrante delito[62]. As segundas, sendo excepção, só podem ser realizadas quando se verificar uma situação grave que implique a necessidade urgente de

[59] Retira-se esta condição pela última parte da al. a) do n.º1 do artigo 251.º: "(…) e que de outra forma poderiam perder-se".
[60] Manuel Lopes Maia Gonçalves, *op. cit.*, p. 602.
[61] Para um esclarecimento mais apurado sobre o problema, *idem*, pp. 602 a 604.
[62] Esta regra resulta do disposto no artigo 177.º n.º1 do CPP, conjugado com o artigo 32.º n.º 4 da CRP ("Toda a instrução é da competência de um juiz, o qual pode, nos termos da lei, delegar noutras entidades a prática dos actos instrutórios que se não prendam directamente com os direitos fundamentais").

tal diligência, ou mediante flagrante delito por crime com pena de prisão de limite máximo superior a 3 anos, ou com consentimento do visado[63].

Numa outra análise, importa também referir que, segundo MANUEL GONÇALVES, as buscas domiciliárias não integram o espírito de acto processual em sentido estrito, sendo antes um acto de inquérito ou de instrução, mediante a fase em que sejam realizadas[64]. Assim, sem desprimor da desejável aceleração processual, deixa de existir o imperativo legal/temporal de cumprimento dos actos processuais – 10 dias – conforme se retira do artigo 105.º n.º 1 do CPP.

Algo que muito interesse tem para o nosso estudo, no domínio das buscas domiciliárias, é o que se refere ao acesso à informação contida em computador. Por poder ser considerada uma ingerência em informações de carácter pessoal, deve-se, logo em primeira instância, afirmar que a "exigência constitucional de a busca domiciliária ser autorizada ou ordenada por um juiz é já uma decorrência de o domicílio ser, por excelência, um espaço de privacidade e intimidade[65]. Por isso, o facto de um computador pessoal que nele se encontre poder conter 'informação de carácter pessoal' nada altera a natureza dos direitos lesados pela realização da busca domiciliária[66]. Só assim não será quanto ao correio electrónico que nele se encontre armazenado uma vez que, quanto a ele, subsiste a dúvida se lhe deve ser aplicado o regime estabelecido para a apreensão de correspondência – artigos 179º e 252º do CPP"[67].

Por assim se entender, e conforme explanaremos no ponto seguinte, esta equiparação do correio electrónico à correspondência tradicional poderá ser alvo de algumas incertezas.

Sobre as buscas em escritório de advogado ou em consultório médico, impera referir a sua especial particularidade, decorrente do imperativo legal de serem presididas pessoalmente pelo juiz, sob pena de nulidade, sendo que este notifica em momento anterior o responsável local da Ordem dos Advogados ou da Ordem dos Médicos – artigo 177.º n.º 5 e 268.º n.º 1 al. *c*) do CPP.

---

[63] Cfr. alíneas a), b) e c) do n.º 2 do artigo 177.º do CPP.
[64] Manuel Lopes Maia Gonçalves, *op. cit.*, p. 441.
[65] Não iremos problematizar as questões advenientes da exploração do conceito de *domicílio,* porquanto esse não ser propósito essencial ao nosso estudo.
[66] No seguimento da mesma fonte: "(…) Daí que a autorização conferida para a realização desta diligência e para a apreensão do que se encontrar dentro do local em que ela se realiza compreenda a possibilidade de o OPC tomar conhecimento do conteúdo do disco rígido de um computador que aí se encontre."
[67] Ainda citando a mesma fonte, "diga-se apenas que se se tratasse efectivamente de correio electrónico o regime jurídico aplicável não seria (…) o que o Código de Processo Penal reserva para a intercepção das comunicações, uma vez que este se destina apenas à intercepção de conversas ou comunicações em curso". Cfr. ACR do Tribunal da Relação de Lisboa n.º 5150/2005-3, de 13-10-2004. Consultável em: http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/2e8989f0e7de2437802570ab00575823?OpenDocument&Highlight=0,apreens%C3%A3o,correio,electr%C3%B3nico.

Em estabelecimento oficial de saúde bastará a presença do presidente do conselho directivo ou de gestão do estabelecimento – artigo 177.º n.º 6 do CPP.

Outra questão que se coloca relativamente às apreensões no âmbito de buscas é a de saber se podem ser apreendidos todos os objectos que tenham significado probatório potencial, ou se existem objectos insusceptíveis de serem apreendidos. Assim, a lei proíbe a apreensão de determinados objectos, por exemplo, os documentos abrangidos por segredo profissional salvo se eles mesmos constituírem objecto ou elemento de um crime (art. 180º, nº 2 CPP e 182º, nº 1 CPP).

1.5.2 O regime da apreensão de correspondência

A apreensão de correspondência é um meio de obtenção de prova consagrado no artigo 179.º do CPP, sendo uma das formas especiais de apreensão[68] que contém mais regras e exigências. E assim o é, desde logo porque previsto na Lei Fundamental que a correspondência, como direito, liberdade e garantia, é inviolável[69], cominando-se a nulidade das provas obtidas mediante abusiva intromissão na correspondência (artigo 32.º n.º8 da CRP – também concretizado no artigo 126.º n.º 3 do CPP).

É por toda esta conjuntura legal que a apreensão de correspondência depende de prévia autorização judicial[70], e só pode ter lugar quando a correspondência em causa tiver sido expedida pelo suspeito ou a ele dirigida, mesmo que sob nome diverso ou através de pessoa diversa. É também requisito que a diligência se revele de grande interesse para a descoberta da verdade ou para a prova, sendo apenas possível de realizar quando estiver em causa crime punível com pena de prisão superior a 3 anos[71]. Por este motivo, e à semelhança das escutas telefónicas, verifica-se uma restrição na admissibilidade de utilização dos conhecimentos fortuitos, que só podem ser validados[72] se referentes a crime constante deste catálogo.

---

[68] Como formas especiais de apreensão o CPP também prevê a apreensão em escritório de advogado ou consultório médico (artigo 180.º do CPP) e a apreensão em estabelecimento bancário (artigo 181.º do CPP).
[69] *Vide* artigo 34.º n.º4 da CRP.
[70] Cfr. artigo 179.º n.º 1 e artigo 269.º n.º 1 al. *d*) do CPP.
[71] Cfr. artigo 179.º n.º 1 do CPP.
[72] No que se refere à **exigência de despacho de validação das apreensões** (nº 3 do art. 178º CPP), coloca-se a questão de saber se o mesmo tem que ser expresso ou se, pelo contrário, é permitida uma validação tácita. O Tribunal Constitucional já se pronunciou sobre esta questão decidindo que " (…) é, do ponto de vista das garantias de defesa, irrelevante que a mesma tenha tradução numa declaração expressa ou que apenas se revele implicitamente." Acrescenta que " (…) a garantia para o arguido é a exigência de que uma apreensão feita por um OPC seja validada, num prazo curto, por uma autoridade judiciária". *Vide* ACR do Tribunal Constitucional n.º 410/2001 de 02/09/2001, in http://www.tribunalconstitucional.pt/. Cfr., no mesmo sentido, ACR do Tribunal da Relação de Coimbra n.º 607/06 de 29/03/2006.

É neste contexto de admissibilidade da apreensão de correspondência derivante de conhecimentos fortuitos obtidos no âmbito de buscas e revistas[73], que MANUEL DA COSTA ANDRADE considera estes casos como sendo "razões de economia processual – evitando-se a repetição de formas e diligências – que ditam a apreensão directa ou valoração probatória dos objectos que corporizam os conhecimentos fortuitos[74]. Ora, as apreensões têm uma natureza meramente preventiva[75], direccionada para o acautelamento da eficácia das revistas e buscas, permitindo conservar as provas e os bens susceptíveis de servirem de prova.

Outra possibilidade se retira do artigo 252.º n.º 2 do CPP que, em casos de perigo na demora, prevê a hipótese de o juiz autorizar o OPC a proceder à abertura imediata de encomendas ou valores fechados, bem como a ordenar o retardamento na remessa da correspondência tendo em vista obter a autorização atempada do juiz, como disposto no art. 252º, nº3 CPP. Todos os casos que extravasem os contornos desta excepção, tornam nula a prova obtida mediante intromissão dos OPC no conteúdo da correspondência[76].

A questão última que levantamos nesta sede prende-se com a definição de *correspondência* e com a possibilidade de esta abarcar o conceito de correio electrónico. O artigo 179.º n.º 1 do CPP define correspondência como as cartas, encomendas, valores, telegramas ou qualquer outra correspondência. Será que na expressão "qualquer outra correspondência" se inclui o correio electrónico? E que regime aplicar, tendo em conta as disposições constitucionais de proibição de ingerências nas comunicações e correspondência[77], já que não existe um regime específico para apreensão de correio electrónico no CPP?

Estas questões serão dissecadas adiante neste trabalho, seguindo com o apoio que BENJAMIM SILVA RODRIGUES nos dá sobre este assunto: "continua controversa a questão de saber se o denominado 'correio electrónico' (*«e-mail»*) deve ser sujeito ao regime das

[73] Pois, como é sabido, compete aos OPC, nos termos do artigo 55.º n.º 2 do CPP, 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, e no âmbito das medidas cautelares proceder à apreensão no decurso das revistas e buscas (artigo 249.º n.º2 al. *c*), do CPP).
[74] Manuel da Costa Andrade, *op. cit.*, pág. 278
[75] Manuel Simas Santos e Manuel Leal-Henriques (2003), *Código de Processo Penal Anotado*, Vol. I, Editora Rei dos Livros, Lisboa, p. 902.
[76] "É nula toda a prova obtida por agentes policiais mediante a apreensão e abertura, ou exposição a raios-X, de encomendas postais depositadas em estações dos CTT, sem prévia ordem ou autorização judicial." Cfr. ACR do Tribunal da Relação de Lisboa n.º CJ 2004-III-149 de 23/06/2004.
[77] Artigos 32.º n.º 8 e 34.º n.º 4 da CRP.

comunicações escritas (…) ou, se, pelo contrário, deve ficar sujeito ao regime das comunicações telefónicas"[78].

1.5.3 O regime das escutas telefónicas[79; 80]

O que nos leva a abordar o tema das escutas telefónicas é, desde logo e em primeira instância, a cláusula de extensão presente no artigo 189.º do CPP, que prevê a aplicação deste regime "às comunicações transmitidas por qualquer meio técnico diferente do telefone, designadamente correio electrónico" [81] . Embora manifestemos já um entendimento discordante face a este normativo, cumpre por ora esclarecer as regras sobre as quais assenta o instituto das escutas telefónicas. E sobre elas começam FERNANDO GONÇALVES e MANUEL ALVES por referir que "são, sem dúvida, o meio de obtenção de prova mais devassador dos direitos e liberdades fundamentais das pessoas"[82]. Sendo-o, o legislador viu-se obrigado a considerar atentamente os pressupostos legais de admissibilidade das escutas para a descoberta da verdade, que, no pós-reforma de 2007[83], se baseiam em critérios de indispensabilidade e impossibilidade de comprovar por outra forma, a prática dos factos criminais ("a diligência seja indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter.") – artigo 187.º n.º 1 do CPP. Este primeiro pressuposto de admissibilidade permite evidenciar a necessidade de um despacho de fundamentação do juiz altamente cuidado[84], de acordo com os princípios da subsidiariedade e proporcionalidade que regem a necessidade da escuta telefónica, colocando-lhe uma dupla condição de legalidade: não será legítimo o

[78] Benjamim Silva Rodrigues (2009), *Das Escutas Telefónicas à Obtenção da Prova [em ambiente]* Digital, Tomo II, Coimbra Editora, Coimbra, p. 56.
[79] Não abordaremos, por desnecessidade de contexto, as questões relativas às formalidades das operações previstas no artigo 188.º do CPP.
[80] Para uma referência mais aprofundada, veja-se o estudo do Professor Manuel da Costa Andrade, de título "Sobre o Regime Processual Penal das Escutas Telefónicas", *in Revista Portuguesa de Ciência Criminal, I*.
[81] Desde 2007 que se sujeitam as comunicações electrónicas ao regime do artigo 189.º, "mesmo que se encontrem guardadas em suporte digital" incluindo, por maioria de interpretação, também o correio electrónico já recebido ou mesmo aberto e tratado pelo destinatário.
[82] Fernando Gonçalves e Manuel João Alves, *op. cit.*, p. 231.
[83] Das alterações influídas pela Lei n.º 48/2007 retira-se, também, que as intercepções só são possíveis na fase de inquérito (afastando-se a possibilidade de intercepções telefónicas com fins de prevenção criminal).
[84] A este propósito, algo que parece óbvio, mas que não pode deixar de ser referido, é que apenas o JIC pode autorizar a intercepção e gravação de conversações nos termos dos artigo. 187.º a 190.º do CPP), sendo que apenas será possível proceder à intercepção de comunicações electrónicas (não telefónicas), nas mesmas condições em que é permitida a realização de intercepções telefónicas. MANUEL GONÇALVES acrescenta que "A intercepção e gravação de conversações telefónicas ou transmitidas por qualquer meio técnico diferente do telefone, sem ordem ou autorização judicial, é cominada com nulidade insanável, (…), sem prejuízo de outras eventuais sanções. A inobservância de quaisquer outros requisitos constitui nulidade relativa ou sanável – arts. 189.º, 120.º e 121.º do CPP". Cfr. Manuel Lopes Maia Gonçalves, *op. cit.*, p. 460.

recurso às escutas nos casos em que os resultados probatórios desejados sejam, sem dificuldade, alcançados por meio menos invasivo dos direitos fundamentais; é ainda necessário que a escuta telefónica se apresente como um meio ajustado para obter aquele resultado[85].

Quanto ao catálogo de crimes que admitem o recurso às escutas telefónicas, encontra-se uma lista que é, obviamente, restrita[86], em função da profunda interferência que provoca na esfera pessoal e jurídica dos escutados[87]. Em referência aos alvos das escutas (artigo 187.º n.º 4 do CPP), a revisão de 2007 delimitou o campo subjectivo do universo dos escutados a um elenco igualmente reservado, assim obstando à determinação de escutas em processos contra incertos[88].

No que se refere à equiparação feita pelo nosso CPP entre as escutas telefónicas e o correio electrónico, esta surge como algo incongruente, desde logo pelos diferentes modos de comunicação utilizados por cada um dos meios – chamada telefónica e *e-mail*. Enquanto que na primeira a informação é passada por meio da palavra falada, no segundo faz-se – em tese – por escrito[89]. A mesma Autora citada em rodapé, acrescenta com pertinência que o rol de crimes criado para ser abrangido pela *"ultima ratio"* dos meios de obtenção de prova (escutas telefónicas), também se mostra algo disforme em relação àqueles que poderiam caber no catálogo que devia guiar a intercepção e/ou registo das comunicações electrónicas escritas (vulgo correio electrónico, *sms*, *chat*, etc.)[90]. Em

[85] A reforma de 2007 pretendeu, pois, disciplinar que a escuta telefónica não seja determinada como primeiro meio de obtenção de prova, logo na abertura do inquérito, nem com base em mera denúncia anónima, mesmo que desta se possam retirar indícios da prática de crime. A determinação da escuta telefónica, tanto num caso como no outro, constituirá uma interferência proibida, desproporcional e desnecessária de investigação.

[86] Limitando a possibilidade aos crimes puníveis com pena de prisão superior, no seu máximo, a três anos, aos relativos ao tráfico de estupefacientes, aos de detenção de arma proibida e de tráfico de armas, aos de contrabando, de injúrias, ameaça, coacção, devassa da vida privada e perturbação da paz e sossego (quando cometidos através do telefone), aos de ameaça com prática de crime ou de abuso e simulação de sinais de perigo; ou aos de evasão, quando o arguido haja sido condenado por algum dos crimes anteriores. Cfr. artigo 187.º n.º 1 do CPP.

[87] Mais uma vez se trás à colação o texto constitucional, designadamente o artigo 34.º n.os 1 e 4.

[88] As escutas só podem ser efectuadas contra o suspeito ou arguido, pessoas que sirvam de intermediário ou vítimas do crime. A propósito do "intermediário" presente no artigo 187.º n.º 4 al. *b*), não deverá ser confundido com o suspeito da prática do crime, pois a lei não lhe exige dolo nem sequer a sua má fé.

[89] Na mesma linha se pronuncia RITA CASTANHEIRA NEVES, ao referir que "não é tanto o instrumento técnico através do qual é levada a cabo a comunicação susceptível de ingerência, é sim a própria comunicação que serve de critério distintivo e, eventualmente, gradativo da protecção a conferir. (…). Numa conversação telefónica, a palavra é dirigida para se extinguir naquele mesmo tempo e propósito. Não é suposto haver qualquer tipo de perpetuação do que vai dito. Ao contrário, quando se escreve, sabe-se que se eterniza uma mensagem, seja privada ou não. Há, nesta última hipótese, uma ponderação que vai implicada na mensagem que se transmite e que se põe ao dispor de quem a recebe". Cfr. Rita Castanheira Neves (2009), *A ingerência nas comunicações electrónicas em processo penal – uma análise guiada pela natureza e respectivo regime jurídico do correio electrónico enquanto meio de obtenção de prova*, Dissertação de Mestrado em Ciências Jurídico – Criminais, Faculdade de Direito da Universidade de Coimbra, Coimbra, p. 146.

[90] *Vide*, *idem*, *ibidem*, pp. 146 a 148.

contínuo desabono do artigo de extensão das escutas, joga a colocação do conceito "intercepção", que, apesar de estar perfeitamente subsumido às chamadas telefónicas, não se nos afigura como virtualmente acessível em termos de investigação criminal para as mensagens de correio electrónico, como analisaremos posteriormente.

1.6 Conclusão Capitular

Com este primeiro capítulo, essencialmente teórico e conceptual, foi nosso objectivo, numa primeira perspectiva, delimitar as fronteiras dentro das quais balanceiam as questões advenientes do instituto da prova em geral, e, noutra segunda, apresentar os regimes legais que poderão ser invocados pela relação existente entre correio electrónico e processo penal. Esta, como já é possível compreender, não se apresenta inteiramente clara em termos legais. É certo que o correio electrónico pode (e deve), ser utilizado como meio de prova, ou até como modo de a obter, funcionando como um instrumento de que se servem as AJ e/ou os OPC para atingirem as finalidades do processo.

A verdade é que, consoante o contexto em que surgem ou o carácter que possam tomar, os *e-mails* não têm ainda no nosso ordenamento jurídico um estatuto bem definido, funcionando um pouco mediante uma inconstância de regime, que tanto pode cair nas **buscas** (se se tiver a percepção de que o conteúdo dos *e-mails* só é alcançável através das buscas e apreensões, excluindo-se a possibilidade de captação no acto de transmissão da mensagem, ou se se considerar a procura em sistema informático como sendo uma busca), ou da **apreensão de correspondência** (desde logo por constar expressa no artigo 179.º do CPP a sua aplicação a "qualquer outra correspondência" e ao que acresce a referência expressa na LC, como veremos), ou ao das **intercepções telefónicas** (que é absolutamente flagrante quando refere no seu artigo de extensão o "correio electrónico").

Capítulo 2 – Do Correio Electrónico e seu Enquadramento Jurídico em geral

"O mundo virtual foi 'apropriado' pelos criminosos que vêem nele 'novas oportunidades' até aí desconhecidas. A rapidez de execução das instruções realizadas com a velocidade electrónica, a confidencialidade assegurada pelo encriptamento dos dados numéricos e a imaterialidade das transacções que protegem o anonimato, tudo isto surge como um incentivo ao crime..."[91].

2.1 Introdução Capitular

No seguimento do referido no Capítulo I, cumpre agora esclarecer nesta sede, por necessidade de tratamento, a definição de correio electrónico e os subconceitos que integram a sua composição, comparando, embora de forma breve, a realidade do *e-mail* com outras que, *a simili*, lhe sejam próximas.

Algo que também importará compreender, por estarem ligados à própria noção de correio electrónico, são os momentos capazes de alterar a qualificação jurídica do *e-mail*, podendo passar do conceito de comunicação electrónica para o de correspondência tradicional, em função da interpretação daquilo que consubstancia o acto de transmissão[92], ou, em diferente análise, do que faz perdurar no tempo o teor comunicacional do *e-mail*.

Noutra perspectiva, igualmente essencial para o reconhecimento da potencialidade do correio electrónico como fonte de auxílio à investigação criminal, impõe-se estudar o seu valor e validade, no contexto do actual ordenamento jurídico português, e bem assim atingir o alcance e implicações da sua recolha e utilização como meio de (obtenção de) prova.

[91] Benjamim Silva Rodrigues (2009), *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*, Tomo I, Coimbra Editora, Coimbra, p. 745.

[92] Esta terminologia sugere, *per si*, que a forma de recolher prova de dados ou informação em transmissão, será através da sua *intercepção*. Este conceito, expressamente utilizado no artigo 189.º do CPP, será alvo de análise própria neste trabalho.

2.2 Correio Electrónico – Especificação Conceitual

2.2.1 Noção

Para que possamos valorizar e apreender os regimes em que balanceia o instituto da prova em matéria de correio electrónico, importa, numa primeira análise, conhecer efectivamente aquilo que é o tão vulgar *e-mail*, apesar da lei penal e processual penal não reconhecerem de forma clara e taxativa a natureza deste tipo de mensagens. De forma simplista, "o correio electrónico (*e-mail*) é um serviço da Internet que permite compor, enviar e receber mensagens através de sistemas electrónicos de comunicação"[93]. Noutra definição, retira-se da *Revista Técnica del Cuerpo Nacional de Policía*, que o "Correo electrónico es todo mensaje de texto, voz, sonido o imagen enviado a través de una red de comunicaciones pública que pueda almacenarse en la red o en el equipo terminal del receptor hasta que éste acceda al mismo"[94]. Assim, esta forma de comunicar, além de possibilitar uma ligação rápida, fácil, económica e capaz de enviar/receber dados informáticos, quebra todas as barreiras geográficas existentes entre o emissor e o(s) receptor(es), sem que para tal tenha havido qualquer tipo de deslocação ou prejuízo pessoal[95]. Daqui se retira também que a definição de correio electrónico abrange qualquer tipo de mensagens transmitidas por forma electrónica, na certeza porém de que não é necessária a participação simultânea do remetente e do destinatário.

Contudo, não se esgota nestas definições a abrangência do conceito, na medida em que o percurso tomado pelo correio electrónico, para além de ser tecnicamente complexo, é extremamente vulnerável. E é-o, como referem GARCIA MARQUES e LOURENÇO MARTINS, por circular na rede "efectuando 'saltos' de servidor em servidor", abrindo possibilidades de "efectiva espionagem dos endereços"[96] electrónicos IP[97] (*Internet Protocol*). Esta característica marcadamente digital, além de abrir portas a um sem número de crimes

[93] Fonte: Universidade do Algarve. Consultável em: http://www.ualg.pt/index.php?option=com_content&task=view&id=26363&Itemid=1793&lang=pt.
[94] "Intervención y/o interceptación de correo electrónico", *in* Revista *Ciencia policial – Revista Técnica del Cuerpo Nacional de Policía*, n.º 96, OCT 2009, pp. 50 e 51.
[95] O correio electrónico foi inventado por Ray Tomlinson, em 1971. Ray era um funcionário da *Bolt Beranek and Newman* (BBN), empresa contratada pelo Departamento de Defesa dos Estados Unidos da América em 1968 para implementar um sistema de correio electrónico na *Advanced Research Projects Agency Network* (ARPANet). Fonte: http://pt.wikipedia.org/wiki/Ray_Tomlinson.
[96] Garcia Marques e Lourenço Martins (2006), *Direito da Informática*, 2.ª edição refundida e actualizada, Almedina, Coimbra, p. 434.
[97] Relativamente ao endereço IP, veja-se a seguinte definição: "O endereço IP (…) é um número de 32 bits escrito com quatro octetos representados no formato decimal (exemplo: 128.6.4.7). A primeira parte do endereço identifica uma rede específica na inter-rede, a segunda parte identifica um host dentro dessa rede. Devemos notar que um endereço IP não identifica uma máquina individual, mas uma conexão à inter-rede". Fonte: http://pt.wikipedia.org/wiki/Endere%C3%A7o_IP.

praticados na Internet ou com recurso a ela (cibercrimes)[98], também nos impele a questionar qual a verdadeira natureza do correio electrónico.

Só uma resposta parece poder dar-se à questão anterior: o correio electrónico singulariza uma concreta forma de comunicação electrónica. Não soe isto absurdo ou até repetitivo, pois este carácter electrónico dos *e-mails*, refira-se, em muito particulariza a sua definição. Torna-se assim, como facilmente se infere, incontornável a remissão para o conceito de *comunicação electrónica*. Este, por sua vez, encontra uma boa explicação conceptual na alínea *a)* do n.º 1 do artigo 2.º da Lei n.º 41/2004, de 18 de Agosto[99], a qual estatui que, comunicação electrónica é "qualquer informação trocada ou enviada entre um número finito de partes mediante a utilização de um serviço de comunicações electrónicas acessível ao público"[100].

Assim sendo, e porque existe uma base comum às várias formas de comunicação aqui implícitas, importa trazer à colação aquilo que são os três pilares fundamentais em que assenta qualquer telecomunicação e, em particular, as comunicações electrónicas[101;102]. São eles: *i*) dados de base; *ii*) dados de tráfego; e *iii*) dados de conteúdo.

Os dados de base, lato senso, são aqueles que se referem à identificação do titular do contrato de acesso à Internet, acrescentando CRISTINA MÁXIMO DOS SANTOS que são dados

[98] Esclareça-se que os cibercrimes não integram, de todo, o âmbito do presente trabalho. No entanto, não poderemos deixar de lhes fazer referência ao longo do estudo.

[99] Esta lei transpõe para a ordem jurídica nacional a Directiva n.º 2002/58/CE, do Parlamento Europeu e do Conselho, de 12 de Julho, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas.

[100] Estranhamente àquilo que seria de esperar, a Lei n.º 5/2004 de 10 de Fevereiro – Lei das Comunicações Electrónicas (LCE) – não define o conceito de comunicação electrónica, nem sobre ele se pronuncia. Apenas refere o que se entende por serviço de comunicações electrónicas: "o serviço oferecido em geral mediante remuneração, que consiste total ou principalmente no envio de sinais através de redes de comunicações electrónicas, incluindo os serviços de telecomunicações e os serviços de transmissão em redes utilizadas para a rádio difusão". Ficamos assim com a noção de que este é um diploma com um cariz de regulação do sector empresarial, de prestação de serviços públicos de diversos âmbitos, desde a utilização de frequências de radiocomunicação ao regime aplicável às redes de televisão digital. Citando o *website* do diário da república electrónico, esta lei "estabelece o regime jurídico aplicável às redes e serviços de comunicações electrónicas e aos recursos e serviços conexos e define as competências da autoridade reguladora nacional neste domínio – Instituto de Comunicações de Portugal – Autoridade Nacional de Comunicações (ICP – ANACOM) " – consultável em: http://digestoconvidados.dre.pt/digesto/%28S%28azil3wzb10daqcycebxa1c55%29%29/Paginas/DiplomaDetalhado.aspx?claint=20040378@s1.

[101] Nesta senda, seguiremos de perto CRISTINA MÁXIMO DOS SANTOS, e a sua publicação "As novas tecnologias da informação e o sigilo das telecomunicações" *in RMP, Ano 25.º, N.º 99, Julho/Setembro de 2004*.

[102] Há também quem reconheça outros tipos de dados, nomeadamente os de localização, referindo o Projecto de Lei n.º 240/X que estes são "quaisquer dados tratados numa rede de comunicações electrónicas que indiquem a posição geográfica do equipamento terminal de um utilizador de um serviço de comunicações electrónicas publicamente disponível".

de comunicação meramente "instrumentais, (…) tais como o posto e o número de acesso, a identificação do utilizador ou da sua morada"[103].

Os dados de tráfego funcionam como uma espécie de descrição do percurso de uma comunicação nas redes, desde o ponto de partida até ao seu destino. Nas palavras da Autora, são "aqueles que permitem a identificação da comunicação e respeitam à direcção, percurso, destinatário, hora, duração e intensidade/frequência, (…), necessários ao estabelecimento de uma comunicação e os dados gerados pela utilização da rede de telecomunicações"[104].

A informação que consubstancia os dados de conteúdo, conforme se deduz, reflecte "o próprio conteúdo da comunicação e os dados gerados pela utilização da rede de telecomunicações"[105], ou seja, o teor ou essência do acto comunicacional.

Relativamente ao sigilo ou protecção conferida a estes tipos de dados, existe um alargado consenso na doutrina em relação ao resguardo que os dados de tráfego e de conteúdo devem ter. Todavia, apesar de o legislador prever a "obtenção e junção aos autos de dados (…) de conversações ou comunicações"[106], não se apresenta claro a que tipo de dados se refere. O Projecto de Lei n.º 240/X[107], apesar de não ter tido assento legislativo definitivo, ajuda-nos a compreender uma possível dinâmica de acesso aos dados, designadamente quando prevê, no artigo 3.º que, "para efeitos de prevenção e investigação criminal, os operadores de comunicações devem facultar às autoridades de polícia criminal ou às autoridades judiciárias os dados de tráfego e os dados de localização, sempre que estes lhes sejam por elas solicitados", acrescentando um leque de crimes relativamente aos quais tal cedência seria admissível. Quanto aos dados de base, o mesmo diploma determina que se lhes devem ser aplicadas as mesmas regras, exceptuando-se as listagens de movimentos de comunicação ou os dados que se encontrem em regime de confidencialidade[108]. Nestas duas situações, apenas a AJ titular da direcção do processo poderá formular o pedido através de despacho devidamente fundamentado[109].

---

[103] Cristina Máximo dos Santos, *op. cit.*, p. 95.
[104] *Idem, ibidem*.
[105] *Idem, ibidem*.
[106] Cfr. n.º 2 do artigo 189.º do CPP.
[107] Consultável e disponível para *download* em: http://app.parlamento.pt/webutils/docs/doc.pdf?path=6148523063446f764c3246795a5868774d546f334e7a67774c325276593342734c576c75615668305a586776634770734d6a51774c5667755a47396a&fich=pjl240-X.doc&Inline=true.
[108] Segundo o n.º 2 do artigo 4.º do Projecto de Lei n.º 240/X, consideram-se sujeitos ao regime de confidencialidade "os dados relativamente aos quais o utilizador tenha expressamente manifestado o desejo de não serem publicitados, nos termos dos artigos 6.º e 13.º da Lei n.º 41/2004, de 18 de Agosto.
[109] Cfr. n.º 3 do artigo 4.º do Projecto de Lei n.º 240/X.

Por último, e talvez mais importante no âmbito do presente estudo, surge o acesso aos dados de conteúdo, prevendo-se, nestes casos, a aplicação do regime das escutas telefónicas, com as necessárias adaptações[110]. Ora, são justamente estas "necessárias adaptações" que podem desvirtuar a actividade probatória, na medida em que a intercepção de uma chamada telefónica, na prática, pouco ou nada tem a ver com a intercepção de um *e-mail* em fase de transmissão, como veremos *infra.*

O registo de comunicações mencionado no artigo 189.º n.º 2 do CPP, por não vir correctamente esclarecido na lei, abre também espaço para perplexidades relativas à recolha deste tipo de prova.

Porém, e apesar de subsistirem dúvidas relativamente à forma de utilizar o correio electrónico como prova penal, parece facilmente possível perspectivar utilidade no acesso a estes dados por parte dos OPC no âmbito de uma qualquer investigação criminal. Quem não utiliza o *e-mail* nos dias de hoje? Esta é uma realidade cada vez mais "aproveitada" para a prática[111] de crimes tão diversos como simples ameaças, injúrias, subornos, chantagens, ou mesmo outros crimes mais graves como o tráfico de armas e de droga, o terrorismo organizado, a exploração sexual de menores, entre outros.

Por outro lado, "o *e-mail* constitui (…) um veículo perfeito para a transmissão de programas de *software*"[112], podendo-se aqui fazer a ponte para a multiplicidade de anexos que se podem enviar numa mensagem de correio electrónico, caindo neste leque todo o tipo de ficheiros digitais.

2.2.2 Delimitação face a realidades próximas

O propósito que nos impeliu a pronunciar sobre algumas realidades próximas à do correio electrónico, em matéria de prova penal, foi unicamente o de problematizar e trazer à colação um eventual vazio ou falta de abrangência legal, tendo em conta determinadas potencialidades tecnológicas e sociais, tanto modernas e sofisticadas quanto livremente acessíveis[113]. Atentemos novamente à redacção do n.º 1 artigo 189.º do CPP: "O disposto nos artigos 187.º e 188.º é correspondentemente aplicável às conversações transmitidas por

[110] Cfr. artigo 6.º do Projecto de Lei n.º 240/X.
[111] Salvaguarde-se, novamente, que o que está em causa neste trabalho não são os cibercrimes – *stricto senso* – mas antes todos os actos preparatórios ou comunicações utilizadas para planear ou perpetrar determinados crimes.
[112] *Idem*, p. 61.
[113] Aqui, siga-se também a indicação constante da Lei n.º 38/2009, de 20 de Julho, que define os Objectivos, Prioridades e Orientações de Política Criminal para o biénio de 2009-2011 (LOPOPC), no seu artigo 3.º n.º 2, al. *b)*: São considerados de prevenção prioritária os crimes executados "com elevado grau de mobilidade, elevada especialidade técnica…".

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". Cumpre pois efectuar um esclarecimento conceptual, desta vez relativo ao conceito de "telemática". Segundo o dicionário da língua portuguesa[114], telemática é o termo utilizado para referir um "conjunto de técnicas e serviços que associam as redes de telecomunicação e a informática".

Perante isto, será legítimo admitir que cabem neste leque, a título de exemplo, os *e-mails*, as *sms*'s (*Short Message Service)*, as *mms*'s (*Multimedia Messaging Service)*, as conversações *chat* através de programas do tipo *instant messaging (MSN)*, as conversações de voz sobre IP (*VoIP)* como é exemplo a aplicação *Skype*, os sites que disponibilizam *chat on-line* (caso da maior rede social da actualidade: o *facebook*), *IRC* (*Internet Relay Chat*), entre outros, na consciente certeza, porém, de que a rede de telecomunicação utilizada por estas últimas é sempre a Internet.

Todavia, dada a diferente natureza destes tipos de comunicação, não seria conveniente orientar os mecanismos legais para um enfoque mais directo quanto a cada um deles? Atente-se, por exemplo, ser totalmente díspar o mecanismo de intercepção de uma *sms* em relação a uma conversa de um *chat* ou de um *e-mail*.

O caso das *sms's*, talvez por ser o mais paradigmático, encontra-se discutido em diversa jurisprudência, sendo de realçar o entendimento do ACR n.º 3453/2008-5 do Tribunal da Relação de Lisboa[115], do qual comungamos. O seu espírito é o de que, sempre que é enviada uma *sms*, a mesma fica guardada no telemóvel do receptor, sendo de presumir que, atendendo à natureza e finalidade do aparelho (telemóvel), está implícita a sua leitura e consentimento de gravação. Assim, será de presumir o mesmo regime conferido às cartas em papel que tenham sido recebidas, abertas e guardadas em arquivo pessoal, a uma *sms* mantida em suporte digital depois de recebida e lida.

Também o Tribunal da Relação do Porto considerou que a informação relativa a *sms's* enviadas ou recebidas, mesmo que não lidas pelo seu detentor, não estão sob a tutela das telecomunicações, funcionando, em termos legais, como um normal escrito fechado, perfeitamente susceptível de poder ser apreendido[116].

---

[114] Dicionário "O Português Essencial", Selecções do Reader's Digest, Porto Editora.
[115] ACR de 15-07-2008. Disponível para consulta em: http://www.dgsi.pt/Jtrl.nsf/0/9182245992c7c5d18025749000503b8c?OpenDocument.
[116] Cfr. ACR da Relação do Porto n.º 1978/09.4JAPRT-B.P1 de 07-07-2010, consultável em: http://www.dgsi.pt/jtrp.nsf/c3fb530030ea1c61802568d9005cd5bb/d81b24cfc47ba41e802577c1004d383c?OpenDocument.

O que nos impele a partilhar desta opinião, no caso dos *e-mails*, e tal como clarificaremos mais à frente, é a possibilidade de dissimular uma mensagem já aberta e lida, atribuindo-lhe novamente o aspecto de não ter sido sequer aberta, parecendo justo optar-se por uma modalidade mais garantística que a dos simples documentos, gozando-se aqui da tutela da correspondência.

No domínio das actividades de investigação, e porque sobreleva aludir-lhes, são inúmeros os meios e métodos de prova disponíveis para a descoberta da verdade material. Contudo, a sistematização intelectual e o atavismo do legislador, parecem faltar à chamada destes desafios, deixando às polícias, muitas vezes, a ideia de "oportunidade perdida". Uma realidade que se afigura exponencial, relativamente aos actuais equipamentos de suporte digital, é a banal posse de *smartphones* ou meios análogos, que possibilitam uma utilização em tudo à igual à efectuada num computador (com ou sem acesso à Internet). Embora esta certeza se apresente como um indicador de clara evolução social positiva, também não é menos verdade que potencia algumas indesejáveis faculdades criminais, principalmente no plano das formas de comunicação por via telemática.

2.2.3 Momentos de diferente valência axiológico-material

Um dos aspectos que mais perplexidade levanta à qualificação legal do correio electrónico prende-se, em particular, com a sua "aparente imaterialidade" ou "invisibilidade"[117].

No que respeita às comunicações electrónicas em geral, para que seja possível estabelecer a sua origem e o seu destino final, exige-se, normalmente, a recolha e monitorização dos dados da rede de comunicações, principalmente considerando os já referidos dados de tráfego. E assim é, porque, tal como defende RODRÍGUEZ LAINZ, as redes de telecomunicações ou comunicações electrónicas públicas são o "instrumento para o cometimento do crime", sendo que nestes casos a simples localização da origem e destino das comunicações, no durante ou pós acto de transmissão, permitirá a definição do círculo de pessoas às quais se poderá imputar a infracção criminal.

[117] Expressões utilizadas por BENJAMIM SILVA RODRIGUES para se referir à prova "electrónico-digital" em geral. Em causa está, nas palavras do autor, "uma (…) dificuldade do investigador forense (…) que implica o uso de determinadas técnicas e conhecimentos científicos que, ao não estarem presentes, não só não permitirão captar tal tipo de prova, como levarão à sua perda ou alteração, visto que o investigador pensa que a mesma não está presente e, muitas vezes, introduz-lhe alterações significativas e invalidantes da sua força probatória em juízo", cfr. Benjamim Silva Rodrigues (2009), *Das Escutas Telefónicas à Obtenção da Prova [em ambiente]* Digital, Tomo II, Coimbra Editora, Coimbra, p. 576.

Neste justo sentido, como em qualquer outra forma de comunicação, também as comunicações electrónicas perduram durante um certo lapso temporal, que se inicia quando entram na rede e termina quando atingem o seu destino. Contrariamente ao que se possa pensar, a esta tão evidente dinâmica, subjaz uma divisão axiológico-material, também decorrente do facto dos *e-mails* serem algo de incorpóreo, que se traduz na separação entre o momento do envio e o momento que se inicia com o recebimento da mensagem. Conforme referido no citado ACR da Relação de Lisboa[118], só existe intercepção (por analogia aos preceitos das escutas telefónicas) no lapso de tempo que vai desde a entrada da comunicação na rede até à sua saída. Toda a ingerência posterior ao momento do recebimento, não terá, então, qualquer laço de similitude com a ideia de intercepção, uma vez que as mensagens depois de recebidas e gravadas na plataforma receptora, deixam de ter a natureza de comunicação em transmissão.

É defendido pela doutrina e pela jurisprudência em geral que as comunicações já recebidas deverão ter o mesmo tratamento da tradicional correspondência escrita (artigos 179.º e ss. do CPP). Conquanto assim se entenda, parece-nos manifestamente insuficiente efectuar esta directa equiparação. Para além dos diferentes juízos de prognose que o emissor faz entre as potenciais consequências de uma comunicação electrónica ou postal física, todo o processo comunicacional é notoriamente diferente.

É aqui que importa clarificar os dois momentos já admitidos, uma vez que uma mensagem de correio electrónico, depois de recebida, não mais poderá ser "interceptada", isto é, o seu conhecimento terá obrigatoriamente de decorrer de um acesso, seja ele físico – no sentido de apreensão de um computador ou de *e-mails* impressos –, digital *in loco* – no sentido de se transferir algo do computador para outro suporte digital –, ou até mesmo de um acesso pelo ciberespaço – em relação a entradas remotas.

Também na revista espanhola *Ciencia Policial* se defende que, "la doctrina científica más cualificada suele distinguir entre diferentes momentos en cuanto al correo electrónico, y así se habla de correo electrónico ya enviado pero no leído, y de otro; el correo electrónico escrito pero no enviado al destinatario. Por otro lado se distinguen aquellos que se encuentran en el PC de aquellos que se encuentran en la fase de transferencia"[119].

Nesta linha de pensamento, e por o correio electrónico ter tanto de material quanto de virtual, importa fazer a destrinça entre o respeito legal que abrange as mensagens em fase

[118] ACR da Relação de Lisboa, n.º 3453/2008-5 de 15-07-2008. Consultável em: http://www.dgsi.pt/Jtrl.nsf/0/9182245992c7c5d18025749000503b8c?OpenDocument.
[119] "Intervención y/o interceptación de correo electrónico", *in* Revista *Ciencia policial – Revista Técnica del Cuerpo Nacional de Policía*, n.º 96, OCT 2009, pp. 50.

de transmissão – direito ao segredo das comunicações – e as mensagens já recebidas e armazenadas – direito à intimidade privada. É fundamentalmente a partir desta premissa que a citada fonte apresenta a maior dificuldade em relação ao uso dos *e-mails* como prova penal: "el problema que plantea el correo electrónico a la policia, y a la Justicia en general, es cual será el concepto de secreto de las comunicaciones que aplicarán, si el relativo a las intervenciones telefónicas o el correspondiente a las comunicaciones postales o telegráficas"[120].

2.3 Breve Comentário às Alterações Introduzidas na Reforma do Código de Processo Penal de 2007

Iniciamos este ponto compartilhando a convicção já amplamente defendida pela mais autorizada doutrina, segundo a qual em Portugal legisla-se demais. Em matéria criminal abstracta, podemos contar, desde 1852 até 1982, 28 "reformas" do Código Penal (CP). Muitas vezes, principalmente a nível nacional, existe um espírito que apesar de estar consciente da não resolução das perplexidades criminais da actualidade, decide lançar leis sobre esses problemas, de forma sistemática, sem efectivamente os resolver. A reforma de 2007 do Código de Processo Penal[121] foi, em matéria de prova electrónica, praticamente inútil, revelando um grande atavismo por parte do legislador. As alterações que se fizeram sentir, além de deverem ser pensadas com vista a garantir o equilíbrio entre os direitos fundamentais dos arguidos, os direitos das vítimas e os interesses da investigação criminal, também deveriam prever um salto qualitativo em matéria dos "novos meios de (obtenção de) prova". Só uma visão harmoniosa, e necessariamente realista, destes quatro aspectos, pode garantir que uma revisão legislativa resulte em mais direitos para os cidadãos, mas também, e necessariamente, em maior eficácia no combate ao crime (que é cada vez mais sofisticado). BENJAMIM SILVA RODRIGUES expressa o seu desalento, por nós partilhado, referindo que "o actual processo penal português não se encontra preparado para a investigação em 'ambiente digital', pois bastará atentar nas diversas normas do regime das perícias, das buscas e apreensões, bem como das 'escutas telefónicas', para constatarmos que tudo foi pensado para o ambiente analógico ou físico"[122].

[120] *Idem, ibidem*.
[121] Introduzida através da Lei n.º 48/2007, de 29 de Agosto
[122] Benjamim Silva Rodrigues (2009), *Das Escutas Telefónicas à Obtenção da Prova [em ambiente]* Digital, Tomo II, Coimbra Editora, Coimbra, p.581.

Como referido por PAULO DÁ MESQUITA, citando Michael Madison, "a desmaterialização através do digital, para além das componentes relativas à prova penal, (…), gera desafios para o direito que ultrapassam as 'fronteiras das disciplinas e envolvem perspectivas teóricas múltiplas', num quadro em que as 'coisas reais e as coisas jurídicas estão cada vez mais misturadas"[123]. Esta realidade digital implica, segundo o Autor, que se façam, por parte de quem legisla, escolhas que têm implicações na legitimidade e autoridade da própria lei.

Neste sentido, à parte da incisão legislativa sobre os sujeitos processuais, o regime do segredo de justiça ou as medidas de coacção, a Lei 48/2007, de 29 de Agosto revela, em matéria de prova electrónica, alguns nódulos problemáticos, como sendo a já referida redacção dos artigos 179.º e 189.º do CPP. Parece ser o espírito do legislador, ao efectuar esta dupla referência, o de se poder linearmente aplicar o regime das escutas telefónicas à intercepção de um *e-mail* que está, no momento, a ser enviado, da mesma forma que se pode aplicar o regime da apreensão de correspondência ao acesso ao *e-mail* no momento posterior à comunicação.

Acresce a este raciocínio crítico, que a anterior redacção do artigo 189.º apenas diferia da actual pela ausência da expressão "mesmo que se encontrem guardadas em suporte digital". Significa isto que a nova redacção apenas veio complicar mais aquilo que já não tinha uma solução cabal, ou seja: se antes se podia aceitar a insuficiente concordância entre o artigo 179.º e o 189.º[124], agora é de todo impossível compreender, afinal, que regime aplicar às mensagens de correio electrónico já recebidas e guardadas na plataforma informática receptora[125].

Importa voltar a referir, tal como em 2.2.1 e 2.2.3, a duvidosa hipótese de um *e-mail* recebido e arquivado no computador destinatário, ainda ser considerado como verdadeira "comunicação". Interpretando a lei, existe então, no correio electrónico, um vínculo que

[123] Michael J. Madison (2005), *Law as Design: Objects, Concepts, and Digital Thinks*, Case Western Reserve L. Rev., v. 56, pp. 382 a 384, *apud* Paulo Dá Mesquita (2010), *Processo Penal, Prova e Sistema Judiciário*, Coimbra Editora, Coimbra, p. 87.

[124] Porque, ao se interpretarem as duas normas, existem nós de intercepção aparentemente não resolvidos pelo legislador. Senão atente-se a redacção do artigo 179.º do CPP, segundo a qual é possível apreender, "mesmo nas estações de correios e de telecomunicações, cartas, (…), ou qualquer outra correspondência".

[125] Devemos também referir-nos, neste encadeamento, ao aditamento criado pela Lei n.º 48/2007, de 27 de Agosto, ao n.º 2 do artigo 189.º do CPP, passando este a dispor 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". Ora, adianta-se esclarecer que é esta a regra a aplicar aos registos da realização de comunicações ou conversações, isto é, aos dados de tráfego que já foram anteriormente analisados.

decorre da aplicação do procedimento[126] previsto para as escutas, em função de se considerar que a comunicação, apesar de já ter sido enviada, não perdeu o direito de protecção legal que assiste às escutas telefónicas. Este entendimento, do qual não partilham PEDRO VERDELHO[127] e PINTO DE ALBUQUERQUE[128], também nos parece extremamente redutor e pouco ousado por parte do legislador.

Ainda relativamente a este acrescento que o artigo de extensão das escutas recebeu em 2007, torna-se impossível não citar novamente DÁ MESQUITA, quando refere que esta foi uma "inovação que, além de teleologicamente infundada, se apresenta imprecisa, por carência de explicação de um critério delimitador entre o âmbito de protecção das comunicações teleologicamente cobertas pelo manto da norma (…), essencial para identificar a autonomia de dados *guardados* em suporte digital que tenham sido transmitidos no passado"[129].

Em tom crítico e de desencanto, sobreleva ainda referir uma necessidade basilar que FARIA COSTA menciona a propósito desta revisão processual, que, ao que parece, também não foi cumprida. É ela a exigência de, "pelo menos à preparação das leis de maior complexidade, um labor e um rigor científicos que, visivelmente, não precederam a proposta em análise"[130]. Ou seja, ao tentar resolver um problema, logo criou o legislador outro.

A realidade, hoje, é que as novas formas de comunicação implicam uma adaptação legislativa ao mundo telemático. E esta é, como aliás refere RITA CASTANHEIRA NEVES, a verdadeira questão que deve ser colocada: será que "a remissão das novas realidades que surgiram com a era digital para os clássicos institutos do direito processual penal" é adequada[131]? Existem autores cuja escrita serve de resposta a esta pergunta. É o caso de LOURENÇO MARTINS, segundo o qual, "uma das questões mais debatidas no âmbito da telemática relativa à disciplina jurídica desejável para a Internet consiste em saber se será adequado recorrer, com as inevitáveis adaptações, ao esquema jurídico próprio do 'mundo

[126] GERMANO MARQUES DA SILVA chama à atenção que o conceito de *procedimento* pode corresponder "(…) à actividade efectiva, isto é, à sequência dos actos processuais correspondentes ao processo (modelo) que se inicia com a *notitia criminis*", cfr. Germano Marques da Silva (2000), *Curso de Processo Penal* I, 4.ª edição, Editorial Verbo, Lisboa, p. 19.
[127] Pedro Verdelho (2008), "Técnica no novo C.P.P.: Exames, perícias e prova digital", *in Revista do CEJ*, n.º 9, pp. 164 a 166.
[128] Paulo Pinto de Albuquerque (2007), *Comentário do Código de Processo Penal*, Universidade Católica Editora, Lisboa, p. 518.
[129] Paulo Dá Mesquita, *op. cit.*, p. 90.
[130] José de Faria Costa (2009), "Os códigos e a mesmidade: O Código de Processo Penal de 1987", *in Que futuro para o direito processual penal? – Simpósio de homenagem a Jorge de Figueiredo Dias por ocasião dos 20 anos do Código de Processo Penal português*, Coimbra Editora, Coimbra, p. 458.
[131] Cfr. Rita Castanheira Neves (2009), *op. cit.*, p. 122.

tradicional' e aos princípios jurídicos nele amadurecidos ou se, pelo contrário, convirá repensar integralmente um estatuto jurídico para o 'mundo virtual', caracterizando-o com os seus princípios e institutos específicos"[132].

É nesta senda que a Lei n.º 48/2007, de 29 de Agosto, nas alterações aos artigos 189.º e 190.º do CPP, reflecte, à primeira vista, a modesta intenção que o legislador teve em olhar o regime das escutas telefónicas como um abrigo ajustado para acolher também o correio electrónico, enquanto meio de obtenção de prova. O que importa de facto indagar é se faz realmente sentido estabelecer esta aparente e harmoniosa equiparação que, como já *supra* transparece, causa alguma perplexidade.

É certo que a alteração do CPP de 2007 foi algo tímida em matéria de prova digital. Acresce que, também a Lei n.º 109/2009, de 15 de Setembro[133], não pode passar sem lhe fazermos referência. Consta no artigo 1.º que o seu objecto é estabelecer "as disposições penais materiais e processuais (…), relativas ao domínio do cibercrime e da recolha de prova em suporte electrónico…". Para o que aqui se pretende interessam as disposições processuais, sendo o artigo 11.º o primeiro destas: "1 – (…) as disposições processuais previstas no presente capítulo aplicam-se a processos relativos a crimes: (…) *c)* Em relação aos quais seja necessário proceder à recolha de prova em suporte electrónico". Sucede porém que, apenas o artigo 17.º versa directamente sobre o correio electrónico: "Quando, no decurso de uma pesquisa informática ou outro acesso legítimo a um sistema informático, forem encontradas, (…), mensagens de correio electrónico ou registos de comunicações de natureza semelhante, o juiz pode autorizar ou ordenar, por despacho, a apreensão (…), aplicando-se correspondentemente o regime da apreensão de correspondência previsto no Código de Processo Penal".

Ora, atendendo ao grau de especificidade de um normativo como este, com uma inequívoca pretensão de harmonização da "manta de retalhos"[134] do processo legislativo de 2007, não seria de trazer algo de novo à "tão exigente" utilização do correio electrónico como prova penal? Teremos ainda a oportunidade de analisar outros aspectos proeminentes da Lei do Cibercrime (LC).

---

[132] Garcia Marques e Lourenço Martins (2006), *op. cit.*, p. 425.

[133] Que aprova a Lei do Cibercrime, transpondo 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 adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa.

[134] Expressão utilizada por PAULO DÁ MESQUITA para caracterizar a revisão do CPP de 2007 e também a Lei do Cibercrime (2009), *in op. cit.*, p. 111.

2.4 Valor e Validade da Prova Electrónico-Digital

No presente estudo interessa conceber, mesmo que num plano mais teórico, uma análise que permita observar e mensurar a utilidade e validade do acesso ao conteúdo do correio electrónico, como forma de prova electrónica ou digital. Assim sendo, e fazendo *jus* aos ensinamentos de BENJAMIM SILVA RODRIGUES, retiramos que "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 de comunicações electrónicas, privadas ou publicamente acessíveis], sob a forma binária ou digital"[135].

Enquadrando-se o correio electrónico na abrangência polissémica desta definição, exige-se em primeiro lugar, que se definam as duas dimensões em que este tipo de prova pode ser utilizado no combate ao crime. A primeira, que consideramos mais invasiva da esfera particular daqueles que são o objecto da medida[136], caindo quase na frecha da desproporcionalidade, situa-se no hiato criminal preventivo – como assim lhe chamamos. A segunda, como não podia deixar de ser, refere-se às necessárias medidas judiciárias e policiais que são despoletadas por um crime já praticado e não totalmente esclarecido – entenda-se esta como sendo a actividade de investigação criminal por excelência.

Analisaremos com maior enfoque a segunda das dimensões, o que não significa que seja esta totalmente desprovida da componente preventiva, identificada na primeira dimensão, como veremos *infra*. Sabendo que o objectivo da investigação criminal é descobrir se um determinado crime foi ou não praticado, reunindo para tal todos os indícios que o possam ajudar a concluir, reveste-se de colossal importância toda a prova que permita desmistificar e responder às seis questões fundamentais de qualquer investigação: Quem? O quê? Onde? Quando? Como? Porquê?[137] Assim, tendo em conta o objectivo principal que subjaz às ingerências autorizadas nas comunicações electrónicas, "o dado recolhido, seja mediante a intervenção judicial nos elementos externos das

[135] Benjamim Silva Rodrigues (2009), *Das Escutas Telefónicas à Obtenção da Prova [em ambiente]* Digital, Tomo II, Coimbra Editora, Coimbra, p. 573.

[136] Assim entendemos, porquanto se puderem traçar linhas preventivas que podem fracassar e viciar-se numa teoria incorrecta, mas que ainda assim não deixam de ferir os direitos fundamentais do cidadão. Já na actividade de investigação pós crime, existem fundamentos de admissibilidade melhor justificados, que acabam por tornar a actividade de investigação necessária e adequada, na estrita medida legal, mesmo que se conclua pela incorrecção da suspeita.

[137] Para além destas questões, a actividade de investigação criminal deve também recolher, nas palavras de PEDRO VERDELHO, "elementos de prova quanto a factos que determinem a punibilidade ou não e, bem assim, quanto a factos que levem à determinação concreta da medida da pena" – Cfr. Pedro Verdelho (2004), "A obtenção de prova no ambiente digital" *in RMP*, Ano 25, n.º 99, Julho – Setembro, p. 118. Também aqui, em grande medida, consideramos que existe um enorme potencial na prova digital.

comunicações, seja mediante o acesso aos dados de tráfego recolhidos, tratados e armazenados em ficheiros automatizados por ordem ou autorização judicial, visa fazer face à necessidade de identificar o presumível autor da infracção, a descoberta do *modus operandi*, a identificação das conexões ou grau de envolvimento de terceiros no âmbito de uma investigação criminal em curso"[138].

Nesta linha, apesar de não ser extrapolável a todas as realidades criminais, a prova electrónica (digital) adquire, a passos largos, uma maior credibilidade e utilidade na investigação de variados modelos criminais. Este tipo de material probatório, pelas características que apresenta, pela utilidade processual que dele se pode extrair e pela respeitabilidade que deve merecer, não pode caminhar para o silêncio ou para a descrença no seio dos novos métodos de investigação. Isto porque, se um estado criminógeno convida à delinquência, uma investigação insuficiente convida à sua aceitação. Na grande maioria das situações, o acesso aos dados de uma determinada comunicação electrónica pode consubstanciar, para os OPC, o concretizar de determinadas "linhas de investigação" capazes de fundar hipóteses que imputem um crime a determinadas pessoas[139].

Também PAULO DÁ MESQUITA, comparando a prova documental (em papel) e a prova electrónica, entende que "existe uma maior fiabilidade no acesso ao suporte digital para avaliar a respectiva fidedignidade" do que em relação a registos guardados em suporte de papel. Isto porque, explica o Autor, a informação contida em suporte digital será o "original" ou, se corresponder a uma cópia ou renomeação, ainda poderá ter o "lastro informático" do original, não detectável em papel[140]. Daqui se retira facilmente a conclusão de que a prova electrónica em tudo difere da que é produzida em formato de papel, em razão de suas características de intangibilidade, forma, e volume[141].

Por conseguinte, arquivos ou registos de mensagens de *e-mail*, tal como outros suportes digitais de informação, podem ser imprescindíveis à demonstração da existência e verificação de um facto jurídico relevante, qualquer que seja a sua natureza. Casos em que se consiga verificar, por exemplo, um juízo de previsibilidade "positivo" na conduta ou

---

[138] Benjamim Silva Rodrigues (2009), *A Monitorização dos Fluxos Informacionais e Comunicacionais (Contributo para a Superação do "Paradigma da Ponderação Constitucional e Legalmente Codificado" em Matéria de Escutas Telefónicas)*, Volume II, Coimbra Editora, Coimbra, p.224.

[139] Rodríguez Lainz (2003), "Intervención judicial en los dados de tráfico de las comunicaciones, La injerencia judicial en los listados de llamadas y otros elementos externos de las telecomunicaciones y comunicaciones electrónicas", Editorial BOSH, S.A., Barcelona, p. 326.

[140] Paulo Dá Mesquita, *op. cit*, p. 93.

[141] Actualmente, a capacidade de armazenamento de qualquer base de dados digital é normalmente medida em *terabytes*, unidade que isoladamente representa o equivalente a cerca de 500 milhões de páginas de texto escrito.

mensagem enviada pelo emissor, poderão revelar que o comportamento daí adveniente é causa adequada à produção de determinado resultado lesivo ao receptor[142].

Nesta senda, e cientes de que as comunicações electrónicas poderão ser uma importante ferramenta de investigação criminal, interessa salientar, citando o *Rapport explicatif de la Convention sur la cybercriminalité*, que "a capacidade de recolher dados de tráfego respeitantes às comunicações informáticas é (…) importante, senão importantíssima, comparativamente às telecomunicações clássicas. Esta técnica de investigação permite aceder à hora, data, fonte e destino das comunicações do suspeito (…), bem como identificar outras vítimas ou estabelecer ligações com eventuais cúmplices"[143].

Mas, esta possibilidade é também assumida pela lei portuguesa, como refere PEDRO VERDELHO, podendo encontrar-se nas mensagens de correio electrónico um elevado potencial probatório. Acrescenta o Autor que "os hábitos actuais conferem-lhe grande importância, não só quanto aos crimes especificamente cometidos no ambiente digital, mas também no que respeita à criminalidade em geral"[144].

Relativamente ao estatuto processual que lhes deve ser atribuído, as mensagens de correio electrónico são, quer em formato digital quer em papel, equivalentes a documentos, funcionando sob a égide do capítulo do CPP referente à prova documental (artigos 164.º e seguintes) [145]. Sucede que, apesar de alguma doutrina assim entender, outra há que apenas admite o correio electrónico capaz de ser submetido a valoração do JIC, verificados que estejam alguns aspectos, como sendo a "fonte do suporte de armazenamento (*hardware*) e as garantias que ao tratamento da informação oferece o programa informático empregue para o seu processamento (*software*)"[146]. Ou seja, denota-se ainda alguma relutância e incerteza em relação à qualidade a atribuir a este tipo de prova – digital/documental.

Em termos práticos, consideramos que o decisivo é efectuar uma clara distinção entre o acesso ao conteúdo de um *e-mail* através da sua intercepção, ou, noutra hipótese,

---

[142] Tal conclusão deriva do chamado "juízo de prognose póstuma". Este tipo de raciocínio marcadamente jurídico, caracteriza-se por fazer uma previsão posterior (póstuma) à ocorrência do resultado, isto é, pretende-se efectivamente comprovar se a conduta ora praticada é conducente à produção do resultado já conhecido.

[143] Traduzido do ponto 218 do *Rapport explicatif de la Convention sur la cybercriminalité* (STE n.º 185), disponível para consulta em: http://conventions.coe.int/Treaty/fr/Reports/Html/185.htm (acedido em 28-02-2011).

[144] Pedro Verdelho (2004), "A obtenção de prova no ambiente digital" *in RMP*, Ano 25, n.º 99, Julho – Setembro, p. 122.

[145] *Idem, ibidem*.

[146] Eduardo de Urbano Castrillo, "El documento electrónico: aspectos procesales", s/d, p. 590, *apud* Benjamim Silva Rodrigues (2009), *A Monitorização dos Fluxos Informacionais e Comunicacionais (Contributo para a Superação do "Paradigma da Ponderação Constitucional e Legalmente Codificado" em Matéria de Escutas Telefónicas)*, Volume II, Coimbra Editora, Coimbra, p.231.

através do seu acesso *a posteriori*. Esta questão, como já se focou, acaba por se subsumir à disjunção dos dois momentos de diferente valência axiológico material, esclarecendo PEDRO VERDELHO que, "se é verdade que, sendo interceptadas em tempo real, as mensagens de correio electrónico são *comunicações electrónicas*, após o seu recebimento devem ser antes encaradas como correspondência"[147]. Pensamos que, apesar de na sua essência um *e-mail* já recebido ser idêntico a uma carta remetida pelo correio tradicional, nunca deixou de ser uma forma de correspondência mesmo no exacto momento do seu envio. Esta perspectiva, algo turbulenta para alguma doutrina e jurisprudência, vem trazer uma série de outras perplexidades aos regimes legais que abrangem a obtenção e utilização das mensagens de correio electrónico como prova penal.

Também é importante que se clarifiquem as principais formas de obtenção deste tipo de mensagens, referindo-nos apenas ao hiato temporal posterior ao envio. Como refere PEDRO VERDELHO, existe um "molde clássico" de obtenção de prova que resulta de buscas e das respectivas apreensões. Em matéria de correio electrónico, vislumbra-se, à primeira vista, a hipótese de "confisco de bens" através da apreensão de máquinas, tendo em vista obter a informação nelas registada. No entanto, e em harmonia com a opinião do Autor, esta modalidade torna-se algo coerciva e até "gravosa para os visados". É neste pressuposto que se dá o salto para as novas formas de apreensão, que, além de poderem englobar a "clássica apreensão de informação no respectivo suporte", passam também pela realização de uma cópia dos dados em causa, e bem assim pela possibilidade de os tornar inacessíveis[148]. Todavia, todo o processo não é ainda muito bem conhecido pela lei portuguesa.

2.5 Conclusão Capitular

O assento conceptual em que se enquadrou o presente capítulo, para além de pretender abrir caminho a problematizações práticas adiante exploradas, quis primar pela construção dos suficientes alicerces teóricos imprescindíveis à discussão deste tipo de matérias, tanto específicas quanto ainda "ocultas". Assim sendo, e talvez ainda de forma prematura, entendemos que a equiparação de regimes entre a recolha de prova em forma de correio electrónico e escutas telefónicas ou a apreensão de correspondência tradicional, afigura-se desadequada, na medida em que as diligências em causa envolvem mecanismos

[147] Pedro Verdelho (2004), "A obtenção de prova no ambiente digital" *in RMP*, Ano 25, n.º 99, Julho – Setembro, p. 123.
[148] *Idem*, p. 130.

completamente díspares[149]. É reconhecido que os *e-mails* podem, inclusivamente, ser editados já no destino, como forma de ludibriar os OPC's e bem assim os restantes mecanismos judiciais/criminais. Embora esta particularidade possa evidenciar uma fragilidade deste tipo de prova, também será verdade que é possível falsificar uma carta do normal correio físico ou simular conversações telefónicas na convicção de que se está a ser escutado. Apesar destas vicissitudes sempre presentes em qualquer tipo de prova, acredita-se que o acesso ao conteúdo dos *e-mails*, por singularizar um meio de prova ou meio de obtenção de prova único, jamais poderá ser regulado por analogia legal a outro tipo de regime, por daí resultarem diversas lacunas e *nuances* prático-processuais dificilmente sanáveis.

[149] Tal como refere BENAJMIM SILVA RODRIGUES, "a investigação criminal, 'em ambiente electrónico-digital', impõe novas exigências ao processo penal português, já que se afigura imprescindível tomar em linha de conta as específicas características da chamada prova digital", cfr. Benjamim Silva Rodrigues (2009), *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*, Tomo I, Coimbra Editora, Coimbra, p. 509.

Capítulo 3 – Regimes Aplicáveis ao Correio Electrónico e Relevância da Actuação dos OPC's

"Omnipresente está um contexto em que (…) se revela uma democracia por realizar na ausência de discursos de justificação transparentes no estabelecimento de regras centrais do processo penal como 'jogo argumentativo especificamente programado' e no desconhecimento generalizado, mesmo entre as elites, das normas estabelecidas, muitas das quais com níveis de ambiguidade que levam a que mesmo quando sejam objecto de discussão na esfera pública subsistam opacas nos múltiplos desencontros de explicações sobre o dever ser da aplicação"[150].

3.1 Introdução Capitular

Atento o que se expôs já, reveste agora especial importância começar por construir uma clarificação relativamente à interpretação dos artigos 179.º e 189.º do CPP, mormente através da análise conceptual de algumas expressões aí empregues pelo legislador.

Seguidamente, e porque releva projectar a solução que, no actual cenário legislativo, melhor parece responder ao problema de fundo que o presente trabalho levanta, empreender-se-á uma análise primordialmente jurídica quanto aos diferentes panoramas concernentes à apreensão de correio electrónico (em momento posterior ao do seu envio). Nesta discussão, obrigar-nos-emos a fazer referência à Lei 109/2009, de 15 de Setembro, considerando-a como um dos caminhos que melhor responde às confusas regras do CPP que, em matéria de recolha de prova digital, assumem particular melindre.

Por último, e talvez sendo a parte mais subjectiva e característica deste estudo, pretende-se agitar a questão da actuação dos OPC's em cenários onde surge a necessidade, ou até apenas a oportunidade, de proceder à recolha de prova digital. O objectivo é o de que, conscientes da enormíssima volatilidade deste tipo de material probatório, se ajustem os procedimentos inerentes à necessidade da sua preservação, principalmente em sede de uma actuação primária dos OPC's. Neste sentido, aludiremos à importante interoperabilidade existente entre as polícias e as autoridades judiciárias competentes, bem como aos limites (em particular os penais) e capacidades práticas dentro das quais a Polícia

[150] Paulo Dá Mesquita (7 de Abril de 2010) *in* Nota Prévia à sua obra *Processo Penal, Prova e Sistema Judiciário*.

de Segurança Pública (PSP) se pode articular neste tipo de investigações, que, porventura, se podem denominar "mais sensíveis".

3.2 A Expressão "qualquer outra correspondência" no Artigo 179.º do CPP – sua relevância

A eficiência da prossecução penal e processual penal deriva, em larga medida, da correcta e específica redacção dos seus Códigos, não omitindo referências imprescindíveis à boa interpretação da lei. A redacção do artigo 179.º do CPP, além de abrir margem a amplas interpretações, congrega alguns elementos que poderão estar, em certa medida, em contradição com outras disposições legais. Referimo-nos, em tais termos, à bivalência legal que existe, para o correio electrónico, entre o instituto das escutas e o da apreensão de correspondência[151]. No entanto, parece óbvio que o legislador baralhou de tal forma a sua redacção, ao ponto de incluir uma chamada a todo o tipo de correspondência no artigo da apreensão de correspondência, mas também de se referir às comunicações guardadas em suporte digital no artigo das escutas. É certo que o *jus non scriptum* revela-se a favor da superação de determinadas brechas existentes na lei escrita. No entanto, nem sempre é linear encontrar uma solução dentro de tão nebuloso cenário legal.

Considerando a letra do artigo 179.º do CPP[152], e quando se levanta a interrogação relativamente à natureza jurídica de um *e-mail*, já não restam dúvidas em defini-lo como um tipo de correspondência decorrente de uma comunicação electrónica. Isto porque, à partida, correspondência será toda a mensagem reduzida a um instrumento de comunicação, na forma escrita.

---

[151] Exemplo de um factor não concordante de ambos, é, por exemplo, o catálogo de crimes que permite cada uma das medidas. Aqui, apesar deste comentário, estamos conscientes da diferente natureza que o correio electrónico pode apresentar para que se lhe aplique um ou outro regime.

[152] Nos termos do qual, "***1***. *Sob pena de nulidade, o juiz pode autorizar ou ordenar, por despacho, 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 nome 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.*

2. *É proibida, sob pena de nulidade, a apreensão e qualquer outra forma de controlo da correspondência entre o arguido e o seu defensor, salvo se o juiz tiver fundadas razões para crer que aquela constitui objecto ou elemento de um crime.*

3. *O juiz que tiver autorizado ou ordenado a diligência é a primeira pessoa a tomar conhecimento do conteúdo da correspondência apreendida. Se a considerar relevante para a prova, fá-la juntar ao processo; caso contrário, restitui-a a quem de direito, não podendo ela ser utilizada como meio de prova, e fica ligado por dever de segredo relativamente àquilo de que tiver tomado conhecimento e não tiver interesse para a prova."*

Assim, torna-se de certa forma inócua, no contexto deste artigo, a discussão sobre uma eventual intercepção de correio electrónico. O que está aqui em causa, no espírito do legislador, é regular o acesso à correspondência electrónica que se encontra impressa em formato de papel. Isto se, obviamente, a expressão "qualquer outra correspondência" abranger tal forma de comunicação, como *infra* se analisará. No entanto, embora que de forma menos óbvia, parece também levantar-se a hipótese de este artigo abranger a apreensão de mensagens de correio electrónico recebidas mas não impressas[153]. Até porque, como veremos, a apreensão de correio electrónico terá mais potencial probatório (ou de utilidade processual), quando a recolha for feita de um suporte digital – tendo em conta que, regra geral, poucas são as probabilidades de se encontrarem *e-mails* impressos com valia criminal.

Relativamente à expressão mote deste apontamento, importa, antes de mais, retornar à definição base. Assim, segundo o dicionário da língua portuguesa, correspondência significa "acto de corresponder; troca de cartas, telegramas, etc.; o conjunto de cartas, telegramas, etc., que se recebam; relação mútua; simetria; carta a um jornal; comunicação entre países, localidades ou pessoas"[154]. Ora, importa também verificar se a definição de correio – por completar o conceito de *e-mail* – se subsume à de correspondência. Do mesmo dicionário extraímos que correio é o "serviço de transporte e distribuição de correspondência; pessoa que transporta ou distribui a correspondência; estação postal; correspondência; indivíduo expedido com um despacho, notícia, recado, etc.; anunciador; precursor; pessoa linguaruda, indiscreta"[155].

É então possível afirmar que correspondência e correio podem ser uma e a mesma coisa. No entanto, ainda não abandonámos a dimensão física dos escritos. Nota-se, claramente, que o tipo de prova ínsito na letra do artigo 179.º do CPP se enquadra nos artigos 164.º[156] e seguintes do mesmo Código – da prova documental.

---

[153] Adiante neste trabalho analisaremos as diversas hipóteses ou formas em que se poderá encontrar o correio electrónico já enviado.
[154] Dicionário "O Português Essencial", Selecções do Reader's Digest, Porto Editora.
[155] *Idem, ibidem*.
[156] Este artigo consagra que "é admissível prova por documento, entendendo-se por tal a declaração, sinal ou notação corporizada em escrito ou qualquer outro meio técnico, nos termos da lei penal". O CP, por sua vez, define documento no seu artigo 255.º, alínea *a)*, como sendo "a declaração corporizada em escrito , ou registada em disco, fita gravada ou qualquer outro meio técnico, inteligível para a generalidade das pessoas ou para um certo círculo de pessoas, que, permitindo reconhecer o eminente, é idónea para provar facto juridicamente relevante, quer tal destino lhe seja dado no momento da sua emissão quer posteriormente; e bem assim o sinal materialmente feito, dado ou posto numa coisa para provar facto juridicamente relevante e que permite reconhecer à generalidade das pessoas ou a um certo círculo de pessoas o seu destino e a prova que dele resulta".

Neste sentido, ainda que seja algo envergonhado, por parte do legislador, regular por analogia os procedimentos a ter em conta quando se trata de correio electrónico impresso, compreendemos, agora, que se lhe aplique o regime da apreensão de documentos – e não o da correspondência tradicional, como o referido artigo parece indicar. Senão veja-se: no decurso de uma busca domiciliária, ordenada ou autorizada no âmbito de uma qualquer investigação, o OPC depara-se com alguns *e-mails* impressos na secretária do suspeito, cujo teor é (ou poderá ser) de potencial interesse probatório se juntos ao processo. Neste caso, com que suporte legal poderá actuar a polícia senão com base na apreensão de documentos, visto se tratarem de "meras folhas impressas" e não "fechadas"? Aqui, a identificação dos *e-mails* como um simples documento afigura-se, de facto, como a melhor das alternativas.

Resta saber se, no decurso da mesma busca domiciliária, se apresentar diante do OPC um computador em funcionamento e com uma janela de correspondência electrónica (vulgo caixa de correio electrónico) aberta, com *e-mails* à vista de igual valor deíctico e penal, é de aplicar ainda o regime da apreensão de documentos. Questão a ser aludida *infra* naquela que se considera ser sistematicamente a sede própria.

3.3 O Artigo 189.º do CPP – Ponderação à sua Proficiência

Se ainda podiam subsistir dúvidas quanto ao facto de o artigo 179.º parece aludir às mensagens de correio electrónico, o artigo 189.º não deixa quaisquer incertezas quanto a essa referência. Como já se referiu *supra*, este artigo estabelece, no n.º 1, que o instituto das escutas telefónicas é também aplicável a todas as "conversações ou comunicações transmitidas por qualquer meio técnico diferente do telefone", fazendo a directa ponte para os *e-mails* através da expressão: "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"[157]. Para MANUEL GUEDES VALENTE as alterações legislativas ao regime das escutas telefónicas destinaram-se a restringir mais eficazmente o recurso a este meio de obtenção de prova, reforçando-se o seu carácter de excepcionalidade, através da rigorosa delimitação da sua

[157] Note-se que a actual redacção deste normativo é decorrente da revisão do CPP de 2007. Conforme referem FERNANDO GONÇALVES e MANUEL ALVES, "Esta previsão não tem nem podia ter correspondência no direito anterior ao CPP de 87, atento o quase alucinante avanço tecnológico registado de então para cá", cfr. Fernando Gonçalves e Manuel João Alves (2009), *op. cit.*, p. 243.

admissibilidade[158]. Com este mesmo sentido, MANUEL DA COSTA ANDRADE considera o catálogo de crimes previstos para as escutas telefónicas como sendo demasiado amplo, principalmente atendendo ao facto do regime das escutas funcionar em subsidiariedade[159] face aos restantes meios de obtenção de prova[160].

No entanto, com a redacção do artigo 189.º o legislador quis deixar claro que é de aplicar o regime das intercepções telefónicas também ao correio electrónico, quer se encontre em transmissão, quer já se encontre efectivamente recebido. É neste ponto que surge a crítica dúvida do presente estudo.

Quanto ao primeiro – correio electrónico em transmissão – e apesar de não vislumbrarmos grandes similitudes práticas entre o processo de transmissão do correio electrónico e o de transmissão telefónica, pode considerar-se minimamente equiparável o regime das escutas à intercepção de *e-mails*, uma vez que a tónica, em termos conceptuais, está colocada na questão da "intercepção".

Relativamente ao segundo, e atendendo à tamanha confusão que o legislador de 2007 trouxe com a nova redacção do n.º1 do artigo 189.º do CPP ("mesmo que se encontrem guardadas em suporte digital"), não é linearmente acessível à compreensão o que fazer a *e-mails* já enviados e guardados digitalmente, para os tornar num alvo "de escutas" acessível em termos legais. Aliás, a lei processual penal prevê, no fundo, resposta a esta dúvida, com algo que na nossa óptica é extremamente redutor da eficácia penal: em primeiro lugar o artigo 189.º do CPP determina que as mensagens de correio electrónico guardadas em suporte digital são ainda "comunicação" – o que vai contra o preceituado no artigo 179.º, que as encara como "correspondência"); e em segundo, sujeita-as ao apertado regime das escutas telefónicas – o que levanta outro novelo de problemas, não só a nível de operacionalização dos métodos, como também a nível dos requisitos formais que têm de estar preenchidos para se proceder a uma escuta telefónica[161]. A este propósito é

[158] Manuel Monteiro Guedes Valente (2008), *Escutas telefónicas: da excepcionalidade à vulgaridade*, Almedina, Coimbra, p. 87.
[159] Ou seja, só quando "há 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", cfr. n.º1 do artigo 187.º do CPP.
[160] Manuel da Costa Andrade *in* conferência dia 23 de Fevereiro de 2011, em Abrantes, subordinada ao tema: "Escutas telefónicas e conhecimentos fortuitos".
[161] Que já se explanaram no ponto 1.5.3. Também com este sentido se refere SARA RODRIGUES: "A actual redacção do n.º 1 do artigo 189.º (…) dá azo a interpretações divergentes do significado a atribuir à expressão 'mesmo que se encontrem guardadas em suporte digital'. Coloca-se (…) a questão de saber se é de aplicar o regime das escutas telefónicas às comunicações efectuadas por correio electrónico, tão só enquanto perdure tal comunicação, ou se, ao invés, tal regime acompanha as mensagens de correio electrónico, mesmo quando as mesmas já se encontrem guardadas, lidas ou não, em suporte digital", cfr. Sara Mafalda de Anjos Rodrigues (2009), *Da admissibilidade de apreensão de correio electrónico no âmbito das buscas efectuadas*

obrigatório citar o ACR da Relação de Coimbra de 29-03-2006, segundo o qual, "como em qualquer outra comunicação, também as comunicações por via electrónica ocorrem durante certo lapso de tempo; começam quando entram na rede e acabam quando saem da rede. 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"[162]. Aliás, para BENJAMIM SILVA RODRIGUES, a expressão "intercepção" só deve ser utilizada quando está em causa a interrupção do curso de algo, ou quando nos apoderamos de algo que está a ser dirigido a outrem, impedindo a sua chegada[163].

Pelo exposto, impera também questionar, na prática, como funcionará a intercepção de um *e-mail*. Acresce que, para tal, exige-se uma comparação com a intercepção de uma chamada telefónica. Enquanto que nesta existe uma interoperabilidade entre OPC's[164] e operadoras telefónicas[165] – que hoje em dia é simples e directa – para que haja a intercepção de um *e-mail* o processo já é algo diferente. A relação existente entre a Polícia e a entidade prestadora do serviço de internet (*ISP – Internet Service Provider*[166]), bem como os equipamentos tecnológicos necessários, ainda se apresentam como um aspecto muito limitativo da questão da "intercepção" de correio electrónico.

Numa outra análise, parece garantido que aquilo a que se pretende aceder através de uma qualquer intercepção, é ao conteúdo da comunicação. Ora, este conteúdo apresenta diferentes comportamentos quer se trate de uma conversação telefónica ou de uma mensagem de correio electrónico. O conteúdo de uma chamada telefónica apenas pode ser obtido no momento da comunicação. Fora deste lapso, apenas restam para investigação dados como a hora, data ou duração da telecomunicação. No correio electrónico já assim

---

pela autoridade da concorrência, Dissertação de Mestrado em Ciências Juridico-Forenses, Faculdade de Direito da Universidade de Lisboa, Lisboa, p. 101.

[162] ACR do Tribunal da Relação de Coimbra, processo n.º 607/06 de 29-03-2006, consultável em: http://www.dgsi.pt/jtrc.nsf/8fe0e606d8f56b22802576c0005637dc/553a95b9c55abec18025716800494c3d?OpenDocument.

[163] A este propósito o Autor refere que em matéria de comunicações telefónicas, "apesar de o legislador usar a expressão 'intercepção', do que se trata não é de uma verdadeira intercepção – proibida pelo texto constitucional – mas, sim, de uma fiscalização, observação, registo, escuta e gravação da comunicação que ocorre via telefónica ou outro meio equiparado, sem que se impeça a chegada/entrega, à esfera de disponibilidade empírica do destinatário, do respectivo fluxo informacional e comunicacional". Assim, considera que é mais gravosa a intervenção na correspondência escrita (onde está implícita a apreensão e consequente abertura do escrito) que nas comunicações telefónicas e electrónicas, cfr. Benjamim Silva Rodrigues (2009), *Das Escutas Telefónicas à Obtenção da Prova [em ambiente]* Digital, Tomo II, Coimbra Editora, Coimbra, p. 40.

[164] Em particular a Polícia Judiciária.

[165] Sem esquecer, obviamente, o prévio consentimento e autorização do juiz.

[166] Uma boa definição encontrada foi a seguinte: "Um *ISP* (*Internet Service Provider*) é um fornecedor de acessos à Internet, através de uma linha telefónica ou outro meio ligado ao computador do cliente, dando ao cliente um pacote de software, um *username*, uma *password* e um número de acesso telefónico" *in* http://www.cgd.pt/Seguranca/Glossario/Pages/Seguranca-Glossario.aspx.

não sucede: existe todo um rasto que se mantém registado na plataforma emissora ou na receptora (ou numa conta de *webmail* [167]), capaz de ser suficiente para decifrar e demonstrar todo o conteúdo[168] e substância do acto comunicacional.

Significa isto que a fórmula encontrada pelo legislador em considerar a possibilidade de intercepção de mensagens de correio electrónico, apesar de possível – e de constar inclusivamente fora do CPP[169] – parece-nos de certa forma desnecessária e até ineficaz, na medida em que, um pouco também à semelhança das escutas, seria necessário um esforço enormíssimo de investigação para se encontrar um detalhe valorável dentro de um gigantesco universo de "lixo comunicacional". Até porque, como já se viu, o conteúdo de uma mensagem de correio electrónico, devido à sua natureza, tende a ser mantida conservada em mais do que um local (em situações em que não é eliminada). Identicamente refere PEDRO VERDELHO que, pese embora também seja uma actividade de investigação trabalhosa e sensível, tem muito mais interesse probatório a apreensão de correio electrónico no momento posterior à comunicação, do que a sua própria intercepção durante o acto comunicacional[170].

3.4. Do Momento Posterior à Comunicação e não da Intercepção

A discussão sobre o momento posterior à comunicação existente no "mundo" do correio electrónico é fundamental e algo complexa. A questão de partida é, novamente, o saber qual o momento em que o correio electrónico deixa de ser comunicação para passar a ser ficheiro digital. Existem entendimentos que defendem que um *e-mail* apenas deixa de ser considerado uma comunicação quando o destinatário toma conhecimento da própria mensagem. É o caso de MANUEL DA COSTA ANDRADE que refere que, "a comunicação só existe (…) até ao momento em que ela é recebida e lida pelo destinatário". Acrescenta ainda que "não deve identificar-se o fim do processo dinâmico da transmissão com a sua chegada ao (último) aparelho (telefone, computador, etc.) do destinatário"[171].

---

[167] Isto porque "a comunicação electrónica, pressupondo a distância entre os interlocutores, faz com que a transmissão da mensagem comunicacional dependa de terceiros, os operadores dos serviços de comunicações electrónicas", cfr. Rita Castanheira Neves, *op. cit.*, p. 228.

[168] Tal como refere RITA CASTANHEIRA NEVES, "o conteúdo da mensagem jaz localmente num computador ou numa conta de *webmail*", *idem*, p. 229.

[169] Referimo-nos, em concreto, ao artigo 18.º da Lei n.º 109/2009, de 15 de Setembro.

[170] Conforme referido por PEDRO VERDELHO. Para mais informações cfr. Anexo 5.

[171] Neste sentido, Manuel da Costa Andrade (2009), *Bruscamente no Verão Passado, a reforma do Código de Processo Penal – Observações críticas sobre uma lei que podia e devia ter sido diferente*, Coimbra Editora, Coimbra, pp. 156 a 160. Segue a mesma orientação Rita Castanheira Neves (2009), *op. cit.*

No entanto este sentido, ao qual não negamos radicalmente validade, encontra também algumas opiniões divergentes. É o caso de ROGÉRIO BRAVO segundo o qual, "a comunicação acaba logo que chega ao terminal do destinatário"[172]. Aliás, é também este o entendimento da maioria da jurisprudência que se pronuncia sobre esta questão.

Neste sentido, tal como acontece na correspondência efectuada pelo correio tradicional, vários são os debates sobre a diferenciação de uma mensagem já recebida mas ainda não aberta da mensagem já recebida e aberta. No entanto, como teremos oportunidade de referir de seguida, não nos parece adequado que se assim se faça em relação ao correio electrónico.

3.4.1 *E-mails* simplesmente recebidos *VS e-mails* recebidos e abertos

Pese embora aquilo que se acaba de afirmar, entende-se ainda assim ser relevante, mesmo que de forma breve, estabelecer a discussão que gravita em torno destas duas realidades, matéria que importa analisar, antes de mais, à luz da Constituição. Como se sabe, a Lei Fundamental apenas prevê protecção aos escritos fechados, deixando sem prenúncio os escritos abertos. Conforme refere PEDRO VERDELHO, "a qualificação legal de uma carta aberta é a de um simples documento"[173]. Significa isto que, *a simili*, poder-se-ia considerar que no correio electrónico as regras seriam as mesmas. O entendimento de GERMANO MARQUES DA SILVA é justamente este: tratamento igual para coisas que são, na óptica do Autor, semelhantes[174]. Sustenta ainda que neste tipo de abordagens, exige-se uma actuação que tem de ser, acima de tudo, "garantística"[175]. Assim, o Autor opta por diferenciar essencialmente o correio (electrónico) antes de ser aberto e depois de ser aberto. Antes de ser aberto, considera-o "em tudo semelhante a uma escuta telefónica, porque há aqui todo um problema de intercepção (…). Depois de aberta e arquivada no computador ou em fotocópias, torna-se correspondência, portanto está sujeita às mesmas regras que outros tipos de correspondência normais"[176].

Defendendo outro entendimento, considerou o Supremo Tribunal de Justiça, irrelevante o facto de as mensagens (em particular as *sms* guardadas em telemóvel) estarem

[172] Rogério Bravo, "Da não equiparação do correio-electrónico ao conceito tradicional de correspondência por carta", *in Revista Polícia e Justiça*, III série, n.º 7, Janeiro – Junho, p. 209, *apud* Rita Castanheira Neves (2009), *op. cit.*, p. 231.
[173] Conforme referido por PEDRO VERDELHO. Para mais informações cfr. Anexo 5.
[174] Conforme referido por GERMANO MARQUES DA SILVA. Para mais informações cfr. Anexo 4.
[175] *Idem*.
[176] *Idem*.

abertas ou fechadas, face ao direito à inviolabilidade da vida privada, sendo sempre de aplicar o regime da apreensão de correspondência[177].

Assim também considera PEDRO VERDELHO[178] segundo o qual, nas comunicações electrónicas não faz sentido diferenciar aquelas que já foram abertas (e lidas) das que ainda não foram.

No nosso entender, dada a natureza deste tipo de comunicações, em tudo semelhantes às *sms* dos telemóveis[179], parece adequado seguir o critério de PEDRO VERDELHO, até porque a letra da LC é, em nossa interpretação, concertada com este raciocínio[180]. Também os magistrados de Coimbra já referiram que "as mensagens que depois de recebidas ficam gravadas no receptor deixam de ter a natureza da comunicação em transmissão; são comunicações recebidas pelo que deverão ter o mesmo tratamento da correspondência escrita já recebida e guardada pelo destinatário"[181].

Atente-se ainda no entendimento defendido por MANUEL DA COSTA ANDRADE, que propugna que o juízo a estar aqui em causa deve ter a sua essência no controlo que o utilizador tem sobre a própria mensagem[182]. Isto é, o Autor privilegia a distinção entre as comunicações que ainda estão (ou não) no domínio do destinatário, ao invés da distinção entre aberto e fechado. Anote-se que MANUEL DA COSTA ANDRADE refere, em concreto, que a distinção importante é entre o "ter ou não ter o domínio sobre a comunicação (…). Se a mensagem é recebida, lida, imprimida em papel, guardada no computador, num disco externo ou em qualquer outro suporte, adquire a natureza de documento simples. Quando, pelo contrário, a mensagem fica guardada no servidor, (…) ainda deve ter a tutela das telecomunicações, independentemente de ser lido ou não" [183].

---

[177] Cfr. ACR do Supremo Tribunal de Justiça, processo n.º 06P2321, de 20-09-2006. Consultável em: http://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/2e7cf04133dd20f78025723d005a62ab?OpenDocument&Highlight=0,06P2321.

[178] Conforme referido por PEDRO VERDELHO. Para mais informações cfr. Anexo 5.

[179] A este propósito *vide* ACR da Relação de Lisboa, processo n.º 3453/2008-5 de 15-07-2008: "a mensagem recebida em telemóvel, atenta a natureza e finalidade do aparelho, é de presumir que uma vez recebida foi lida pelo seu destinatário". Consultável em: http://www.dgsi.pt/Jtrl.nsf/0/9182245992c7c5d18025749000503b8c?OpenDocument.

[180] Como teremos oportunidade de analisar *infra.*

[181] ACR do Tribunal da Relação de Coimbra, processo n.º 607/06 de 29-03-2006, consultável em: http://www.dgsi.pt/jtrc.nsf/8fe0e606d8f56b22802576c0005637dc/553a95b9c55abec18025716800494c3d?OpenDocument.

[182] MANUEL DA COSTA ANDRADE suporta esta sua convicção no entendimento do Tribunal Constitucional Alemão, segundo o qual "o *e-mail* guardado no servidor, no *ISP*, ainda deve e ter a tutela das telecomunicações, independentemente de ser lido ou não", cfr. Anexo 3.

[183] *Idem, ibidem.*

Sem dúvida que esta é uma abordagem possível, até porque, como refere o Autor, a empresa de telecomunicações pode facilmente aceder às mensagens de correio electrónico que estão guardadas no servidor e devassá-las sem conhecimento da pessoa visada.

3.4.2 *E-mails* recebidos e impressos

Relativamente aos *e-mails* impressos já poucas dúvidas se mantêm. Por estarem materializados, não há como não aplicar o regime dos documentos em geral. A doutrina e jurisprudência não têm reservas em considerar as mensagens de correio electrónico impressas como escritos normais, iguais a qualquer outro tipo de documento que pode ser apreendido ao abrigo dos artigos 164.º e seguintes do CPP[184].

PAULA RAINHA e SÓNIA VAZ arriscam até a equiparar o *e-mail* impresso, "a guardar uma folha de papel, uma mensagem de *voice-mail* e uma discussão de negócios nos registos da empresa"[185]. A verdade é que nem é necessário emaranhar mais esta discussão. As mensagens de correio electrónico, tal como ajuizou o Tribunal da Relação de Lisboa em 2008, quando impressas, tratam-se de "meros documentos escritos, (…) não gozam de aplicação do regime de protecção e de reserva da correspondência e das comunicações"[186]. No mesmo sentido já tinha também decidido o supra referido ACR da Relação de Coimbra, de 29 de Março de 2006[187], bem como GERMANO MARQUES DA SILVA, MANUEL DA COSTA ANDRADE e PEDRO VERDELHO[188].

Parece ser também reconduzível a este regime (apreensão de documentos) o caso já exposto anteriormente, relativo aos *e-mails* que se apresentam à vista (num ecrã) no âmbito, por exemplo, de uma busca efectuada por OPC's.

[184] Também neste sentido, FILIPA QUELHAS: "Caso uma mensagem de correio electrónico esteja impressa, pode ser livremente apreendida e nada impede que se aceda ao seu teor", cfr. Filipa Marta de Figueiroa Quelhas (2008), *O meio de (obtenção de) prova digital electrónica – Sua admissibilidade e relevância, em especial, face à globalização e ao uso das novas tecnologias pelas organizações criminosas*, Curso de Especialização tendente a Mestrado em Ciências Jurídico–Criminais, Faculdade de Direito da Universidade de Lisboa, Lisboa, p. 65.

[185] Paula Raínha e Sónia Vaz (2001), *Guia Jurídico da Internet em Portugal*, Barrocas & Alves Pereira, Sociedade de Advogados, Edições Centro Atlântico, Lisboa, p. 60.

[186] Cfr. ACR do Tribunal da Relação de Lisboa, processo n.º 3453/2008-5, de 15/07/08. Consultável em: http://www.dgsi.pt/Jtrl.nsf/0/9182245992c7c5d18025749000503b8c?OpenDocument.

[187] Neste seguimento, reforçando o que se entende relativamente aos *e-mails* impressos, *vide* entrevistas a PEDRO VERDELHO, GERMANO MARQUES DA SILVA e MANUEL DA COSTA ANDRADE, disponíveis em anexo ao presente trabalho.

[188] Conforme entrevistas disponíveis em anexo.

3.5 As Soluções da Lei n.º 109/2009, de 15 de Setembro[189]

O surgimento da LC, no Verão de 2009, foi para alguns Autores uma espécie de esperança de resolução das vincadas lacunas que a lei ordinária apresentava em matéria de prova digital. PAULO DÁ MESQUITA salienta que a LC surgiu com a pretensão de "responder ao diagnóstico de uma carência do ordenamento jurídico nacional relativa à recolha de prova electrónica ressaltando, de acordo com a própria exposição de motivos da proposta de lei, os problemas suscitados pela 'recente revisão do Código de Processo Penal'"[190]. Sobre esta lei, o Autor começa mesmo por caracterizá-la como uma espécie de revisão "escondida" ou "envergonhada" do CPP[191].

Em abstracto, podemos admitir que tal diploma consistiu num bom esforço de sistematização. No entanto sobejam nesta lei alguns tendões de Aquiles que retratam uma falta de consonância entre leis, pois, como afirma MANUEL DA COSTA ANDRADE, "dá a impressão que foram feitas cada uma por seu legislador, separados no tempo, separados na história e separados por um grande abismo civilizacional"[192].

Relativamente ao âmbito de aplicação processual desta lei, certo é que ela compreende duas vertentes que PAULO DÁ MESQUITA caracteriza como "analiticamente autonomizáveis"[193]: a primeira refere-se a um amplo conjunto de regras processuais aplicáveis aos cibercrimes e aos crimes cometidos através de um sistema informático; a outra aos crime em que seja necessário proceder à recolha de prova em suporte electrónico – conforme se pode retirar do artigo 11.º (Âmbito de aplicação das disposições processuais). À presente exposição sobrelevam os casos contidos na segunda vertente.

Fazendo incidir o enfoque sobre as questões de conteúdo e menos sobre as de índole formal e/ou político, cumpre analisar as concretas ferramentas que a LC disponibilizou. Ora, são de considerar, *a priori*, dois instrumentos de investigação bastante importantes. O primeiro consiste na possibilidade de ordenar ao operador de comunicações (fornecedor de serviço) a preservação dos dados de tráfego, mesmo por parte do OPC[194]. Esta preservação,

[189] Esta lei "estabelece 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, transpondo 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 adaptando o direito interno à Convenção sobre Cibercrime do Conselho da Europa", cfr. o seu artigo 1.º.
[190] Paulo Dá Mesquita (2010), *op. cit.*, p. 97.
[191] *Idem*, p. 95.
[192] Nesta observação o Autor inclui também a Lei n.º 32/2008, de 17 de Julho, cfr. Anexo 3.
[193] Paulo Dá Mesquita (2010), *op. cit.*, p. 98.
[194] O n.º 2 do artigo 12.º da Lei 109/2009, de 15 de Setembro prevê expressamente que "A preservação pode também ser ordenada pelo órgão de polícia criminal mediante autorização da autoridade judiciária

embora não disponibilize no imediato as informações dos dados em causa[195], permite à AJ competente a sua posterior obtenção, com integridade, no prazo fixado na lei.

Em consonância com o exposto, e ainda sob a égide deste primeiro instrumento, importa também atentar na Lei n.º 32/2008, de 17 de Julho[196]. Esta, por sua vez, refere-se à obrigação de conservação e transmissão de dados (de tráfego e de localização[197]) por parte dos fornecedores de serviços de comunicações electrónicas, para que possam ser acedidos pelas autoridades competentes, exclusivamente para fins de investigação, detecção e repressão de crimes graves[198;199].

O segundo instrumento, na nossa óptica bastante mais útil e operativo em termos práticos, abarca a questão da apreensão de correio electrónico, prevista no artigo 17.º. A letra deste artigo, embora demasiado condensada num único período gramatical, é de extrema importância para este estudo, na medida em que pode consubstanciar uma resposta ou solução a alguns dos problemas levantados no início. Assim, "Quando, no decurso de uma pesquisa informática ou outro acesso legítimo a um sistema informático, forem encontrados, armazenados nesse sistema 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" [200].

---

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".

[195] Quanto ao tipo de dados a preservar, esclarece o n.º 3 do mesmo artigo que "A ordem de preservação discrimina, sob pena de nulidade: *a)* A natureza dos dados; *b)* A sua origem e destino, se forem conhecidos; e *c)* O período de tempo pelo qual deverão ser preservados, até um máximo de três meses".

[196] Esta lei procedeu à transposição para a ordem jurídica interna da 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", cfr. o n.º 1 do seu artigo 1.º.

[197] Estes dados, segundo o artigo 4.º da Lei 32/2008, de 17 de Julho, podem ser os necessários para: *a)* encontrar e identificar a fonte de uma comunicação; *b)* encontrar e identificar o destino de uma comunicação; *c)* identificar a data, a hora e a duração de uma comunicação; *d)* identificar o tipo de comunicação; *e)* identificar o equipamento de telecomunicações dos utilizadores; e para *f)* identificar a localização do equipamento de comunicação móvel.

[198] *Vide*, neste sentido, artigos 1.º (n.º 1 e 2) e 3.º da Lei n.º 32/2008, de 17 de Julho.

[199] Na sequência da Lei 32/2008, de 17 de Julho, *vide* também a Portaria 469/2009, de 6 de Maio – que vem concretizar as regras técnicas e de segurança relativas à transmissão electrónica de dados entre os fornecedores de serviços e as autoridades competentes – e a Portaria 915/2009, de 18 de Agosto – que veio criar um período experimental de cerca de três meses para se aprofundar e incrementar a funcionalidade e usabilidade da aplicação informática prevista na Portaria 469/2009, aditando-a com um artigo 6.º-A.

[200] Sobre estes casos considere-se também o artigo 252.º do CPP (Apreensão de correspondência), consignado pela lei processual penal no leque das medidas cautelares e de polícia. Este artigo, para além de

Reportando este artigo a uma tentativa de superação de lacunas legislativas em matéria de prova digital (ou electrónica), em particular no que se refere ao correio electrónico, PAULO DÁ MESQUITA defende estar aqui plasmado ou subentendido um "problema que ultrapassa a cibercriminalidade e os crimes cometidos por meio de sistema informático". Acrescenta, neste sentido, que, "existe um amplo universo de actividades criminosas em que as comunicações e registos electrónicos são, fundamentalmente, instrumentos da prática e ocultação do crime, além de meios essenciais para a reconstrução histórica do passado"[201;202].

Retornando à letra do artigo 17.º, aquele que mais relevância terá, verificamos que dissimula, em certa medida, o artigo 179.º do CPP (em matéria de correio electrónico), uma vez que apenas tem para ele uma remissão residual, nos casos em que aquele não se possa aplicar. Aqui, referimos ainda a eventualmente polémica interpretação de PEDRO VERDELHO, que entende não ser necessário um despacho inicial do juiz para se poder aceder ao conteúdo dos *e-mails* encontrados no âmbito de uma pesquisa informática ou outro acesso legítimo[203]. Isto porque o artigo, inicialmente, começa por determinar que "quando, no decurso de uma pesquisa (…) forem encontradas (…) mensagens de correio electrónico…". Ora, isto poderá pressupor a desnecessidade do despacho inicial imposto pelo regime da apreensão de correspondência do CPP, bem como do facto de o juiz ter de ser a primeira pessoa a tomar conhecimento da correspondência[204].

Na opinião de PEDRO VERDELHO, "o que é necessário é que, uma vez detectado o correio electrónico, este se leve ao juiz para que ele possa decidir sobre a sua validação ou não validação". O Autor acrescenta que esta sequência de procedimentos acaba por ser uma "exigência da vida prática. Não é possível para cada computador que se apreende o juiz dizer antecipadamente que se deve apreender o correio electrónico"[205].

---

nem ter grande razão de existir (à excepção talvez do seu n.º 3), soa-nos desde logo incongruente que preveja, no seu n.º1, uma prévia autorização ou ordem judicial, visto que as diligências previstas como medidas cautelares e de polícia pressupõem a ausência de autorização prévia.

[201] Para compreensão do contexto em que o Autor assim se pronuncia, *vide* nota de rodapé n.º 45 *in op. cit*, p. 106.

[202] Este entendimento, por nós corroborado, vai exactamente ao encontro do pensar de PEDRO VERDELHO e de DÁRIO PRATES, segundo os quais o espírito que está por detrás de um cibercrime é o que incorpora a ideia de "manipulação informática", deixando de fora do conceito todos aqueles em que a informática for usada como um recurso meramente instrumental – como é o caso do uso do correio electrónico para a prática de determinado tipo de crimes, cfr. Anexo 5 e 6. *Infra* iremos aprofundar esta questão com mais detalhe.

[203] Conforme referido por PEDRO VERDELHO. Para mais informações cfr. Anexo 5.

[204] Aliás, em bom rigor, acaba por estar aqui presente, como pano de fundo, a qualificação de documentos aos *e-mails* recebidos e guardados no computador, conforme referimos *supra* em 3.4.1.

[205] Conforme referido por PEDRO VERDELHO. Para mais informações cfr. Anexo 5.

3.6 O Papel dos OPC's na Actividade de Investigação Criminal[206]

3.6.1 A missão de coadjuvação com as Autoridades Judiciárias

Tal como ensina MANUEL GUEDES VALENTE, a actividade de investigação criminal "permite que a lei penal seja aplicada ao caso concreto, promovendo deste modo a sua 'cristalização definitiva'[207], saindo da sua redoma abstracta para uma aplicação material e concreta[208]. Mas, para que haja uma maior eficácia e celeridade em processos que envolvam a recolha de prova digital (quer por ingerência nas comunicações electrónicas em curso, quer pelo seu acesso posterior), importa a todo o tempo que exista um concertado relacionamento entre os diversos actores processuais implicados.

Como se sabe, o Ministério Público (MP) é a AJ competente para promover o processo penal, cumprindo-lhe colaborar com o Tribunal na descoberta da verdade e na realização do direito, obedecendo em todas as intervenções processuais a critérios de estrita objectividade[209]. Aos OPC's, por força do artigo 55.º do CPP, cabem funções de coadjuvação com as AJ's, igualmente com vista à realização das finalidades do processo, acrescendo o artigo 56.º que funcionam sob a sua direcção e dependência funcional. Neste sentido, embarcam no seu leque de competências: *a)* colher notícia dos crimes; *b)* impedir o quanto possível as suas consequências; *c)* descobrir os seus agentes; e *d)* levar a cabo os actos necessários e urgentes destinados a assegurar os meios de prova[210]. Daqui não podemos duvidar do patente assento investigatório presente na norma.

Acontece que, quando estão em causa determinados meios de obtenção de prova, surgem as necessárias intervenções judiciais para ordenar ou autorizar diligências, onde intervém, em regra, um juiz. BENJAMIM DA SILVA RODRIGUES escreve, sobre este desígnio, que, "a medida judicial que ordena ou autoriza a ingerência nos elementos externos e dados de tráfego das comunicações electrónicas deve ser submetida a um duplo controlo: *i)* a existência e suficiência da motivação – quer isto significar que o Juiz de Instrução Criminal (JIC) tem de tornar cognoscíveis os motivos (justificadores) que deram lugar à

[206] Comece-se com o esclarecimento constante na Lei n.º 53/2008, de 29 de Agosto – Lei de Segurança Interna (LSI), segundo a qual a PSP exerce funções de segurança interna, cfr. artigo 25.º, n.º 2, al. *b)*, e na Lei n.º 53/2007, de 31 de Agosto – Lei Orgânica da PSP (LOPSP), que refere que à PSP compete "desenvolver as acções de investigação criminal e contra-ordenacional que lhe sejam atribuídas por lei, delegadas pelas autoridades judiciárias ou solicitadas pelas autoridades administrativas", cfr. artigo 3.º, n.º 2, al *e)*.
[207] Jorge de Figueiredo Dias e Manuel da Costa Andrade (1992), *Criminologia – O Homem Delinquente e a Sociedade Criminógena*, Reimpressão, Coimbra Editora, Coimbra, p 67, *apud* Manuel Monteiro Guedes Valente (2009), *Teoria Geral do Direito Policial*, 2.ª edição, Almedina, Coimbra, p. 313.
[208] Manuel Monteiro Guedes Valente (2009), *ibidem.*
[209] Cfr. artigo 48.º e 53.º do CPP.
[210] Cfr. artigo 55.º n.º 2 do CPP.

autorização judicial da medida de acesso aos elementos externos ou dados de tráfego das comunicações electrónicas; *ii)* a 'plausibilidade' do seu discurso – submissão do raciocínio judicial exteriorizado ao juízo de proporcionalidade, sob três ópticas distintas: idoneidade e necessidade da medida e a prevalência do interesse público (investigatório) sobre o direito ao segredo nas comunicações da pessoa alvo da ingerência e titular das comunicações"[211].

O que está em causa no enunciado, no fundo, são critérios de subrogação do juiz às partes ausentes, através do princípio da reserva do juiz. MANUEL DA COSTA ANDRADE esclarece que, "o juiz deve ser particularmente exigente e ser ele, no seu próprio processo psicológico, a mobilizar os argumentos que a pessoa atingida diria. Ou seja, o juiz tem de subjectivizar, interiorizar as resistências que o outro faria, para que de alguma maneira, no seu próprio espírito, consiga fazer aquela contraposição de pontos de vista a que um juiz tem sempre de se subordinar"[212]. O Autor diz mesmo que o juiz é uma espécie de "sucedâneo do contraditório"[213].

No que concerne à ligação existente entre os OPC's e o JIC – em matéria de prova digital – sublinhe-se que, por força dos tempos que correm, pode ser altamente conveniente adoptar a interpretação que PEDRO VERDELHO confere ao artigo 17.º da LC, como aliás se chamou à colação *supra*. E não se tome este partido como sendo uma abusiva compressão dos Direitos Liberdades e Garantias dos visados pela medida, pois no nosso espírito de interpretação da norma está sempre patente que "os responsáveis pela aplicação das leis devem respeitar e proteger a dignidade humana e defender e proteger os direitos fundamentais de toda a pessoa"[214].

Significa isto que, não havendo necessidade do despacho inicial do juiz nem que seja ele o primeiro a tomar conhecimento do(s) *e-mail(s)*, existirá um dever de sigilo que vinculará o OPC enquanto promotor "quase autónomo"[215] da medida. É justamente neste sentido que ensina GERMANO MARQUES DA SILVA, no comentário ao artigo 4.º do Código de Conduta das Nações Unidas para os Responsáveis pela aplicação das Leis

[211] Benjamim Silva Rodrigues (2009), *A Monitorização dos Fluxos Informacionais e Comunicacionais (Contributo para a Superação do "Paradigma da Ponderação Constitucional e Legalmente Codificado" em Matéria de Escutas Telefónicas)*, Volume II, Coimbra Editora, Coimbra, p.191.
[212] Conforme referido por MANUEL DA COSTA ANDRADE. Para mais informações cfr. Anexo 3.
[213] *Idem, ibidem*.
[214] Cfr. artigo 2.º do CCNURAL.
[215] Dizemos "quase autónomo" na medida em que terá sempre de existir uma prévia autorização judicial de busca ou de perícia técnica.

(CCNURAL)[216]: "Através das suas funções, os responsáveis pela aplicação das leis recolhem informações que podem estar relacionadas com a vida privada de outras pessoas ou serem susceptíveis de prejudicar os interesses e, particularmente, a reputação dessas pessoas. Deve-se dar o maior cuidado à preservação e utilização dessas informações, que não devem ser divulgadas, a não ser para necessidades de serviço e dentro do interesse da justiça. Toda a divulgação feita para outros fins é totalmente abusiva". Reutilizando as palavras do Autor, "o polícia deve (…) possuir grande capacidade de julgamento e fazer prova de profissionalismo na acção"[217].

Caso não se proceda segundo esta linha e se actue segundo um modelo mais cauteloso, (regime integral do 179.º do CPP), e atendendo ao amplo leque de barreiras electrónicas existentes no mundo digital, "se cada vez que se apreendesse correio electrónico no *microsoft outlook*, ou outra aplicação de *e-mail* com regras específicas, se levasse esse ficheiro que contém todas as mensagens, de por exemplo 5 *gigabytes*, a um juiz, não seria possível avançar, porque as mensagens seriam tantas que a diligência acabaria por não ser viável"[218], e daí poder ser importante a triagem dos OPC's, *in loco*.

O importante é que, visto o *e-mail* ser uma forma de comunicação inscrita no quadro da *correspondência privada*[219], o seu acesso por parto dos OPC's nunca seja ilegítimo, sob pena de se cometer o crime tipificado no artigo 194.º do CP ("Violação de correspondência ou telecomunicações")[220]. Tal como refere RITA CASTANHEIRA NEVES, a questão que sempre se terá de colocar em sede da actuação das polícias de investigação, está "nos limites a essa investigação, que não pode tudo. A investigação criminal tem de respeitar parâmetros que permitam ao Estado lutar com uma superioridade ética que não tolere a sua conversão em criminoso"[221]. Entendemos que, para não abrir fácil caminho à violação de uma norma penal pelas polícias, é necessário que sejam tidos em conta princípios de transparência e simplificação burocrática nos seus relacionamentos com as AJ's.

---

[216] Nos termos do artigo: "As informações de carácter confidencial que estão na posse dos responsáveis pela aplicação das leis devem ser mantidas em sigilo a não ser que o cumprimento das suas funções ou as necessidades da justiça exijam absolutamente o contrário".
[217] Germano Marques da Silva (2001), *Ética Policial e Sociedade Democrática*, Instituto Superior de Ciências Policiais e Segurança Interna, Lisboa, p. 21.
[218] Conforme referido por PEDRO VERDELHO. Para mais informações cfr. Anexo 5.
[219] Cfr. Garcia Marques e Lourenço Martins (2006), *op. cit.*, p. 433
[220] Esta referência impõe-se, igualmente, devido ao próprio inciso constitucional do artigo 34.º da lei fundamental, que é o primeiro dos escudos da privacidade e intimidade de quem comunica. Ora, é esta também uma cláusula limitadora da acção do poder público do Estado, permitindo antever toda a amplitude que é possível à sua actuação, eliminando-se os excessos e abusos de autoridade.
[221] Cfr. Rita Castanheira Neves (2009), *op. cit.*, p. 228.

3.6.2 A PSP enquanto promotora de diligências fundamentais na preservação e recolha de prova digital – análise à luz das suas capacidades operacionais

A recolha de informação em ambiente digital, capaz de se tornar em prova, não se harmoniza com o que sucede com as apreensões tradicionais. A este propósito PEDRO VERDELHO esclarece que, "ao contrário do que acontecerá numa busca num ambiente físico, em que a entidade que realiza a busca identifica eventuais documentos a apreender e procede à sua apreensão, no ambiente digital pode ser muito difícil identificar e localizar a informação que importa apreender, no vasto acervo de informação eventualmente disponível nos registos de um computador ou sistema informático"[222].

Ora, uma das questões que se pode (e deve) levantar acerca da recolha de prova digital, consiste no carácter volátil e fugaz que a caracteriza, o que impele o Estado a usufruir do factor "oportunidade" na sua actuação. Ora, a ideia de prossecução criminal (fortemente dependente da actuação dos OPC's), antes de qualquer outra referência, tem que ver com o grande equilíbrio de direitos e interesses com que se regula o processo penal. Aliás, a ideia de proporcionalidade do próprio Direito Penal advém directamente da nossa Constituição, quando prevê no artigo 18.º que, "a lei só pode restringir os direitos, liberdades e garantias nos casos previstos na Constituição, devendo as restrições limitar-se ao necessário para salvaguardar outros direitos ou interesses constitucionalmente protegidos. É também sobre esta égide que GERMANO MARQUES DA SILVA conduz a sua opinião em matéria de recolha de prova digital[223]. Neste sentido, o princípio da oportunidade tem implicâncias que desaguam em relações de prioridade, prevalência ou urgência no acautelamento da prova.

Do que se explana, e numa abordagem eminentemente prática, a recolha de prova digital (ou em particular a apreensão de correio electrónico), implicará, em regra, "uma 'busca informática' e uma verdadeira 'perícia informático-digital'"[224]. Importa então considerar a actividade de recolha de prova digital segundo determinadas necessidades e circunstancialismos específicos para cada caso. DÁRIO PRATES classifica esta actividade seguindo dois critérios fundamentais: o critério da apreensão de equipamento que possa

[222] Cfr. Pedro Verdelho (2004), "A obtenção de prova no ambiente digital" *in RMP*, Ano 25, n.º 99, Julho – Setembro, p. 131.
[223] Conforme referido por GERMANO MARQUES DA SILVA. Para mais informações cfr. Anexo 4.
[224] Cfr., neste sentido, Benjamim Silva Rodrigues (2009), *Das Escutas Telefónicas à Obtenção da Prova [em ambiente]* Digital, Tomo II, Coimbra Editora, Coimbra, p. 582.

conter prova digital, por um lado, e o critério da "fotografia ao interior" do equipamento[225] – a chamada cópia de imagem – por outro[226].

Relativamente ao primeiro dos momentos – o da apreensão do equipamento – vários são os cuidados que relevam considerar, desde um registo fotográfico do aspecto exterior do equipamento, a uma eficaz selagem e/ou bloqueamento das portas de comunicação informática, à etiquetagem de cabos e/ou outros dispositivos móveis, a especiais cuidados de transporte, entre outros.

Noutro plano está, naturalmente, presente a intencionalidade de se assegurar uma proporcionada e garantística recolha do material probatório. Esta, que tanto pode ser no local do crime como noutro (consequência de uma prévia apreensão), que obviamente assumirá o carácter de uma cópia, pretende-se absolutamente fiel ao original. PEDRO VERDELHO denomina esta cópia recorrendo a uma expressão de origem americana, "cadeia de custódia"[227], referindo-se à manutenção da integridade dos dados a serem copiados[228].

Em bom rigor, deverá estimular-se o recurso a um perito informático[229] para credibilizar a diligência de recolha de prova digital. PEDRO VERDELHO prevê também a possibilidade de manter a "cadeia de custódia" através do recurso a assinatura digital, no uso da autorização conferida pela LC ou, nessa impossibilidade, juntar-se um auto ao processo a certificar a autenticidade da cópia como sendo fiel ao original[230].

Outra das circunstâncias em que a Polícia pode ser chamada a lidar com prova digital – em particular com o correio electrónico – é no âmbito das suas "normais" funções de atendimento ao público, nas diversas subunidades territoriais. Nesse momento, o importante é que se consiga ter capacidade para analisar os cabeçalhos dos *e-mails* apresentados (presumivelmente utilizados para a prática do crime). Nestas situações, DÁRIO PRATES refere que a PSP tem actualmente as ferramentas necessárias para "conseguir salvaguardar e acautelar logo os meios de prova existentes (…) independentemente da competência de investigação do crime"[231].

---

[225] Conforme referido por DÁRIO PRATES. Para mais informações cfr. Anexo 6.
[226] Exactamente no mesmo sentido, PEDRO VERDELHO refere: "As capacidades operacionais para a recolha de prova digital cingem-se, no fundo, a duas questões: chegar ao local e apreender o computador ou fazer uma cópia". Para melhores desenvolvimentos, *vide* Anexo 5.
[227] Conforme referido por PEDRO VERDELHO. Para mais informações cfr. Anexo 5.
[228] O que está em causa é a necessidade da técnica permitir preservar na prova a sua autoria e integridade, de modo a que seja auditável e periciável, mantendo a segurança da informação, para que ela, quando for precisa, tenha força jurídica e faça fé pública.
[229] Tal como para exames médicos directos se recorre a um perito de saúde ou para exames balísticos se recorre a um técnico especialista da área.
[230] Conforme referido por PEDRO VERDELHO. Para mais informações cfr. Anexo 5.
[231] Conforme referido por DÁRIO PRATES. Para mais informações cfr. Anexo 6.

Em todo o caso, DÁRIO PRATES está ciente de que, "para concretizar um bom trabalho nesta área, há ainda necessidade de percorrer mais algum caminho"[232], sendo certo que é garantidamente uma área na qual os OPC's de proximidade em geral e a PSP em particular têm um papel indispensável, principalmente em sede de diligências fundamentais na preservação e recolha de prova digital[233].

3.6.3 A LOIC e o seu cunho de normativo orientador

Já deixámos patente anteriormente que, embora possam existir alguns pontos de intercepção (que nem sempre são claros), não se devem confundir os cibercrimes com os crimes em que se recorre à informática como mero instrumento utilizado para a sua consumação. Deste desentendimento, com implicâncias meramente organizacionais, podem surgir conflitos de competência ou dúvidas práticas que são perfeitamente supríveis.

Numa primeira abordagem, da análise do artigo 249.º do CPP retira-se que compete aos OPC's praticarem os actos cautelares e urgentes para assegurar os meios de prova, nomeadamente através de exames de vestígios ou de apreensões no decurso de revistas ou buscas. Sobressai aqui, novamente, a ideia subjacente ao princípio da oportunidade da actuação policial.

Numa segunda análise, especificamente direccionada para o problema deste apontamento, refira-se a alínea *l)* do n.º 3 do artigo 7.º da Lei de Organização da Investigação Criminal (LOIC): A Polícia Judiciária (PJ) tem competência reservada para a investigação de crimes "informáticos e praticados com recurso a tecnologia informática". Esta norma, marcadamente restritiva das competências de investigação da PSP[234] em matéria de prova digital, é, no entendimento de PEDRO VERDELHO, um exagero impraticável, pois, se fosse cumprida à letra, "a PJ ficava inundada de crimes que não fazem parte do perfil típico de crimes que a PJ investiga"[235]. O Autor acrescenta que "há prova digital de crimes que não têm nada a ver com o mundo "*ciber*", com o informático,

[232] *Idem*.
[233] DÁRIO PRATES elucida para a existência, na PSP, de um manual de boas práticas para a recolha de prova digital (disponível no anexo 7), realizado em conjunto com o Departamento de Investigação e Acção Penal de Lisboa. Este Departamento criou também um guião para recolha de cabeçalhos técnicos (disponível no anexo 8), que, nas palavras de DÁRIO PRATES, "é um documento de extrema importância para a recolha da prova digital quando o crime é praticado através de correio electrónico", cfr. anexo 6.
[234] Desenvolver as acções de investigação criminal e contra-ordenacional que lhe sejam atribuídas por lei, delegadas pelas autoridades judiciárias ou solicitadas pelas autoridades administrativas
[235] Conforme referido por PEDRO VERDELHO. Para mais informações cfr. Anexo 5.

com o acesso ilegítimo. Muitas vezes o que está em causa é um crime clássico cometido por uma via diferente"[236].

DÁRIO PRATES esclarece que "um crime informático é um núcleo bastante mais restrito do que todos os crimes que possam recorrer à tecnologia informática"[237]. E é-o desde logo pelo facto de hoje em dia ser banal comunicar à distância. A forma de comunicação que recorre a uma aplicação *skype* ou de correio electrónico, por exemplo, é uma conduta demasiadamente vulgar para poder vir a cair na alçada dos crimes informáticos.

Mais uma vez comprovamos que a letra da LOIC (que prima pelo seu carácter orientador e não obrigatório – *stricto sensu*), ao mencionar crimes "informáticos e praticados com recurso a tecnologia informática", tem no seu espírito os crimes em que exista uso manipulado da tecnologia, isto é, aqueles em que o criminoso faça tratamento e uso de dados digitais, acessos ilegítimos a bases de dados (vulgos *hackers*), entre outros. Nos restantes casos, a informática "traduz-se numa mera plataforma não essencial como atributo da conduta criminosa (…), sendo que sem ela o crime poder-se-ia dar de outra forma"[238].

Acresce que, ainda segundo DÁRIO PRATES[239], o Departamento de Investigação e Acção Penal de Lisboa entendeu juntamente com os OPC's de investigação, que apenas os crimes que tenham como atributo o ataque à tecnologia informática – através da sua manipulação – devem ser delegados à PJ, ao abrigo da alínea *l)* do n.º3 do artigo 7.º da LOIC.

Ou seja, a LOIC, além das grandes e necessárias orientações estratégicas que define e das regras que consagra para o crime particular e seu dever de investigação, padece de vícios de redacção que emaranham o funcionamento da máquina de investigação, enquanto um todo dependente do desempenho das suas partes. É, em nosso entender, o caso da alínea *l)* do n.º 2 do seu artigo 7.º, a qual não deve ser tida como um entrave à recolha de prova digital, em particular o correio electrónico, por parte da PSP – e Guarda Nacional Republicana (GNR) – enquanto OPC's com reconhecidas competências e capacidades de investigação, e bem assim enquanto entidades com privilegiados "conhecimentos de rua", atenta a sua natureza de OPC's de proximidade[240].

[236] *Idem*.
[237] Conforme referido por DÁRIO PRATES. Para mais informações cfr. Anexo 6.
[238] Dário Prates, *idem*.
[239] *Idem, ibidem*.
[240] *Idem, ibidem*.

3.7 Conclusão Capitular

Este terceiro e último capítulo, de abordagens tanto jurídicas quanto eminentemente práticas, permite concluir que o correio electrónico, que é a forma de comunicação que nos serve de referência, pode ser, sem dúvida, um possível meio de obtenção de (obtenção de) prova utilizável num variadíssimo leque de crimes. Sucede que, dadas as retorcidas normas legais e as constantes alterações que se têm vindo a processar, não se vislumbra um normativo absolutamente esclarecedor e capaz de ser aplicado integral e descomplexadamente ao correio electrónico. A este propósito, e atendendo à maior importância que damos à apreensão de *e-mails* no momento posterior ao seu envio, conclui-se que a LC soluciona as dúvidas até então existentes, autonomizando um regime processual extra CPP para a apreensão de correio electrónico (aplicando-lhe o regime da apreensão de correspondência), não revogando tácita nem expressamente nenhuma norma do Código, o que, só por si, se nos afigura como um vício legal desnecessário.

Considerámos também, nas páginas anteriores, que atendendo à exacerbada liberdade de acesso aos recursos comunicacionais, existe a necessidade de descentralização da investigação de crimes que recorrem à informática como mero instrumento para a sua consumação. Conforme se verificou, pode afirmar-se que a PSP tem e deve fazer uso das prerrogativas de OPC de proximidade e de investigação, mormente nos crimes em que o correio electrónico seja usado como mero instrumento de comunicação. Neste âmbito, existem documentos internos orientadores – como é o caso dos disponíveis em anexo – que demonstram o *know how* que a PSP detém para a actividade de recolha de prova digital. Assim, apesar da LOIC parecer à primeira vista um obstáculo a esta delegação de competência na PSP, percebe-se não ser esse o seu espírito.

Conclusão

Cada vez mais a investigação criminal exige, por força dos novos tempos, o recurso a elementos de prova em suporte digital. Tal como referido na Introdução, comprova-se ser necessário esclarecer e dotar as autoridades de novos métodos de investigação, desde que enquadrados pelo acervo constitucional e legal dos direitos à reserva da vida privada, ao sigilo das comunicações e à protecção de dados pessoais, revelando-se, assim, essenciais as ideias de proporcionalidade e de ponderação relativa dos interesses em causa.

Neste sentido, apesar de a Constituição ser sempre o principal parâmetro interpretativo da lei penal e processual penal, conclui-se que o potencial probatório que se pode extrair do conteúdo dos *e-mails*, embora não comparável com o das outras realidades previstas no Título III do CPP, diferencia-se do destas, na medida em que se caracteriza por particularidades singulares de um tipo de prova digital capaz de ser alcançado por diversas formas. E de tal modo assim é, que seria inteiramente benéfico que se procedesse a uma autonomização do seu regime, afastando o actual carácter vago de algumas soluções legais – apesar da já existente LC, a qual consideramos como sendo dos poucos instrumentos de investigação dirigido ao ambiente digital.

A título de análise aos objectivos inicialmente fixados, e apesar das dificuldades encontradas em razão da pouca e complexa literatura disponível sobre correio electrónico, acredita-se terem os mesmos sido plenamente atingidos, desde logo por se ter esclarecido que o correio electrónico detém, no ordenamento jurídico português, um lugar (ainda) pouco reconhecido e mal definido[241]. De qualquer forma, conclui-se sem margem para dúvidas, que o correio electrónico é, dependendo da situação concreta, um meio de obtenção de prova ou meio de prova em si mesmo, apesar de não consagrado una e formalmente no CPP[242].

A sua utilização traduz-se num conjunto de diligências que podem cingir-se a três modalidades completamente distintas: *a) intercepção* em tempo real – aqui, para que haja acesso aos dados de conteúdo por parte do OPC, verifica-se a necessidade de preenchimento dos requisitos formais das escutas, pois, na verdade, trata-se da situação em que a invasão da reserva da vida privada e do sigilo das comunicações é mais contundente,

[241] Desde logo por não haver uma constante designação: ora se fala em correio electrónico, ora em correspondência electrónica, ora em comunicações electrónicas (referindo-se ao seu sentido mais estrito – *e-mails*).
[242] De acordo com a exploração inicial deste trabalho, verifica-se que o actual conceito de *prova* não contempla no seu espírito, de forma aberta, o conceito de prova digital, apesar de o podermos lá incluir.

estando em causa precisamente o conhecimento do teor das comunicações dos sujeitos em tempo real, pelo que se impõe nestes casos um maior rigor; *b)* possibilidade de *acesso* aos dados de localização e de tráfego – consoante uma bifurcação entre aqueles que possam ou não estar sujeitos ao regime de confidencialidade: aos que não estejam, bastará a formalização de um pedido por uma Autoridade de Polícia Criminal (APC) endereçado ao operador/fornecedor de serviço *Internet*[243], aos que estejam, um despacho de autorização da AJ competente (pois, face aos interesses envolvidos, importa ponderar se se justifica que no caso em apreço seja dada prevalência à investigação criminal em curso); *c) apreensão* de correio electrónico – referimo-nos, obviamente, à recolha, "*in loco*", dos *e-mails*, quer seja em formato físico, quer seja em formato digital.

Esta terceira modalidade, que melhor explorámos no terceiro capítulo, já não levanta incertezas quando se tratar de apreensão em formato físico – pois aí aferimos que se tratam de vulgares documentos. No que concerne à apreensão em formato digital, levanta-se todo um processo técnico relativo à preservação do correio electrónico, bem como à sua recolha com integridade. Assim sendo, verificou-se "em jeito de 'sinopse operacional'", que, apesar da LC resolver a ausência normativa sobre este tipo de apreensão em concreto, não esclarece na prática como devem actuar os OPC's. Então, conclui-se pela competência da PSP[244] (e não apenas da PJ – como a LOIC induz) em proceder ao acautelamento de meios de prova digitais, recorrendo a peritos informáticos para fiabilizar a recolha da prova necessária do suporte informático. Para tal, demonstrou-se a fragilidade de alguns aspectos do correio electrónico, no que se refere ao tempo e espaço da sua criação, autoria, cópias, autenticidade, integridade e conteúdo.

Por fim, conclui-se que a fórmula encontrada para responder às hipóteses que inicialmente se colocaram, consiste na refutação parcial da primeira e da segunda (pois, como se viu, não é sempre de aplicar o regime das escutas nem o da apreensão de correspondência), na afirmação parcial da terceira (devido à previsão constante no artigo 17.º da LC) e na afirmação integral da quarta (adopção de um regime tripartido – escutas *vs* apreensão de correspondência *vs* apreensão de documentos[245]). Para o efeito referimo-nos

[243] Visto que estes operadores/fornecedores estão particularmente bem posicionados para auxiliarem os OPC's na realização da justiça, considerando-se que o ónus imposto a estas entidades não é desproporcional face à necessidade e características do actual modelo de investigação criminal. Sobreleva ainda o facto de serem os próprios operadores a terem interesse em que os seus serviços não funcionem como verdadeiros "instrumentos do crime".

[244] Falamos da PSP em concreto, por ser a realidade que mais nos interessa comentar.

[245] Pese embora continuemos a sustentar que o regime previsto para as escutas telefónicas se restringe (ou assim devia) às formas de comunicação oral, obtendo a sua razão na captação da palavra falada – opinião também defendida por MANUEL DA COSTA ANDRADE.

aos *e-mails* que estejam em trânsito, aos já recebidos e aos que se encontrem na forma impressa (ou guardados num suporte digital directamente dependente do utilizador receptor). Esta é a solução que nos parece, de facto, mais equilibrada e praticável.

Saliente-se que, embora esclareçamos – com base na LC – que é de aplicar subsidiariamente o regime da apreensão de correspondência para o momento posterior à transmissão, deixamos uma questão de fundo capaz de ser futuramente explorada: atenta a natureza do correio electrónico (que comparamos à das *sms's*), não seria de seguir a linha que defende que a partir do momento em que atingem a esfera do destinatário são de se presumir como abertos e lidos, ao que podem perder o direito ao sigilo da correspondência, funcionando como meros documentos (digitais), ficando sujeitos ao regime do artigo 178.º do CPP[246]?

Deixamos a achega de VERDELHO quando refere que "a qualificação legal de uma carta aberta é a de um simples documento"[247] e a de RITA CASTANHEIRA NEVES quando nos diz que, "para além de tudo o mais, sempre se diga desprovida de qualquer lógica aplicar o regime da correspondência a correio electrónico já aberto e lido, quando nem sequer as próprias cartas gozam desta exacerbada protecção: estas, depois de abertas e lidas, passam automaticamente a ser consideradas normais escritos e não mais correspondência / comunicação"[248].

Por tudo, não nos soa absurdo propor, para um futuro trabalho, um aprofundado estudo capaz de prever um maior leque de situações práticas, bem como o seu concreto assento legal – através da criação de um regime uno, específico e autónomo para o correio electrónico e restantes formas de comunicação análogas.

Realizado por:

_____

André Francisco Dias Antunes
Aspirante a Oficial de Polícia

[246] Ou, caso se opte por considerá-los documentos que contém dados pessoais – com o faz BENJAMIM SILVA RODRIGUES – porque não aplicar-lhes o artigo 178.º do CPP, ficando igualmente sujeitos aos limites da Lei n.º 41/2004, de 18 de Agosto (privacidade no sector das comunicações electrónicas) e da Lei n.º 67/98, de 26 de Outubro (protecção de dados pessoais)?
[247] Conforme referido por PEDRO VERDELHO. Para mais informações cfr. Anexo 5.
[248] Cfr. Rita Castanheira Neves (2009), *op. cit*, p. 130 e 131.

Bibliografia

Albuquerque, Paulo Pinto de (2007), *Comentário do Código de Processo Penal*, Universidade Católica Editora, Lisboa.

Albuquerque, Paulo Pinto de (2009), *Comentário do Código de Processo Penal à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem*, 3ª edição actualizada, Universidade Católica Portuguesa, Lisboa.

Andrade, José Carlos Vieira de (2009), *Os Direitos Fundamentais na Constituição Portuguesa de 1976*, 4.ª Edição, Almedina, Coimbra.

Andrade, Manuel da Costa (1992), *Sobre as Proibições de Prova em Processo Penal*, Coimbra Editora, Coimbra.

Andrade, Manuel da Costa (s/d), "Sobre o Regime Processual Penal das Escutas Telefónicas", *in Revista Portuguesa de Ciência Criminal,* I.

Andrade, Manuel da Costa (2009), *Bruscamente no Verão Passado, a reforma do Código de Processo Penal – Observações críticas sobre uma lei que podia e devia ter sido diferente*, Coimbra Editora, Coimbra.

Bravo, Rogério, "Da não equiparação do correio-electrónico ao conceito tradicional de correspondência por carta", *in Revista Polícia e Justiça*, III série, n.º 7, Janeiro – Junho.

Canotilho, J.J. Gomes; Vital Moreira (2007), *Constituição da República Portuguesa Anotada*, Vol. I, 4.ª Edição Revista, Coimbra Editora, Coimbra.

Clemente, Pedro (2009), "Polícia – O Caminho…", *in Estudos Comemorativos dos 25 Anos do Instituto Superior de Ciências Policiais e Segurança Interna em Homenagem ao Superintendente-Chefe Afonso de Almeida*, Novembro de 2009, Almedina, Coimbra.

Costa, José de Faria (2009), "Os códigos e a mesmidade: O Código de Processo Penal de 1987", *in Que futuro para o direito processual penal? – Simpósio de homenagem a Jorge de Figueiredo Dias por ocasião dos 20 anos do Código de Processo Penal português*, Coimbra Editora, Coimbra.

Eco, Umberto (2005), *Como se Faz uma Tese em Ciências Humanas*, 12.ª Edição, Editorial Presença, Lisboa.

Faria, Miguel José (2001), *Direitos Fundamentais e Direitos do Homem*, volume I, 3.ª Edição Revista e Ampliada, Instituto Superior de Ciências Policiais e Segurança Interna, Lisboa.

Gonçalves, Fernando; Manuel João Alves (2009), *A Prova do Crime – Meios Legais para a sua Obtenção*, Almedina, Coimbra.

Gonçalves, Manuel Lopes Maia (2009), *Código de Processo Penal Anotado*, 17.ª edição, Almedina, Coimbra.

Guiddens, Anthony (2006), *O mundo na era da globalização*, 6.ª edição, Editorial Presença, Lisboa.

Lainz, Rodríguez (2003), "Intervención judicial en los dados de tráfico de las comunicaciones, La injerencia judicial en los listados de llamadas y otros elementos externos de las telecomunicaciones y comunicaciones electrónicas", Editorial BOSH, S.A., Barcelona.

Marques, Garcia; Lourenço Martins (2006), *Direito da Informática*, 2.ª edição refundida e actualizada, Almedina, Coimbra.

Mesquita, Paulo Dá (2010), *Processo Penal, Prova e Sistema Judiciário*, Coimbra Editora, Coimbra.

Miranda, Jorge (2008), *Manual de Direito Constitucional.* Tomo IV, 4.ª Edição, Revista e Actualizada, Coimbra Editora, Coimbra.

Monteiro, Fernando Pinto (2009), *in* prefácio à obra *A Prova do Crime* de Fernando Gonçalves e Manuel João Alves.

Neves, Rita Castanheira (2009), *A ingerência nas comunicações electrónicas em processo penal – uma análise guiada pela natureza e respectivo regime jurídico do correio electrónico enquanto meio de obtenção de prova*, Dissertação de Mestrado em Ciências Jurídico – Criminais, Faculdade de Direito da Universidade de Coimbra, Coimbra.

Pereira, Alexandre; Carlos Poupa (2008), *Como Escrever uma Tese – monografia ou livro científico – usando o Word*, 4.ª Edição Revista, Edições Sílabo, Lisboa.

Queirós, Virgílio; Sofia Miranda (2009), *Breviário Latim-Português*, 2.ª edição (revista e aumentada), Quid Juris, Lisboa.

Quelhas, Filipa Marta de Figueiroa (2008), *O meio de (obtenção de) prova digital electrónica – Sua admissibilidade e relevância, em especial, face à globalização e ao uso das novas tecnologias pelas organizações criminosas*, Curso de Especialização tendente a Mestrado em Ciências Jurídico–Criminais, Faculdade de Direito da Universidade de Lisboa, Lisboa.

Quivy, Raymond; Luc Van Campenhoudt (1998), *Manual de Investigação em Ciências Sociais*, Gravida, Lisboa

Raínha, Paula; Sónia Vaz (2001), *Guia Jurídico da Internet em Portugal*, Barrocas & Alves Pereira, Sociedade de Advogados, Edições Centro Atlântico, Lisboa.

Raposo, João (2006), *Direito Policial I*, Tomo I, Almedina, Coimbra.

Rodrigues, Benjamim Silva (2008), *Das Escutas Telefónicas – A Monitorização dos Fluxos Informacionais e Comunicacionais*, Tomo I, Coimbra Editora, Coimbra.

Rodrigues, Benjamim Silva (2009), *Das Escutas Telefónicas à Obtenção da Prova [em ambiente]* Digital, Tomo II, Coimbra Editora, Coimbra.

Rodrigues, Benjamim Silva (2009), *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*, Tomo I, Coimbra Editora, Coimbra.

Rodrigues, Benjamim Silva (2009), *A Monitorização dos Fluxos Informacionais e Comunicacionais (Contributo para a Superação do "Paradigma da Ponderação Constitucional e Legalmente Codificado" em Matéria de Escutas Telefónicas)*, Volume II, Coimbra Editora, Coimbra.

Rodrigues, Sara Mafalda de Anjos (2009), *Da admissibilidade de apreensão de correio electrónico no âmbito das buscas efectuadas pela autoridade da concorrência*, Dissertação de Mestrado em Ciências Juridico-Forenses, Faculdade de Direito da Universidade de Lisboa, Lisboa.

Silva, Germano Marques da (2000), *Curso de Processo Penal* I, 4.ª edição, Editorial Verbo, Lisboa.

Silva, Germano Marques da (2001), *Ética Policial e Sociedade Democrática*, Instituto Superior de Ciências Policiais e Segurança Interna, Lisboa.

Silva, Germano Marques da (2008), *Curso de Processo Penal* II, 4.ª edição, Editorial Verbo, Lisboa.

Santos, Cristina Máximo dos (2004), "As novas tecnologias da informação e o sigilo das telecomunicações" *in RMP*, Ano 25, n.º 99, Julho – Setembro.

Santos, Manuel Simas; Manuel Leal-Henriques (2003), *Código de Processo Penal Anotado*, Vol. I, Editora Rei dos Livros, Lisboa.

Valente, Manuel Monteiro Guedes (2005), *Revistas e buscas*, Almedina, Coimbra.

Valente, Manuel Monteiro Guedes (2008), *Escutas telefónicas: da excepcionalidade à vulgaridade*, Almedina, Coimbra.

Valente, Manuel Monteiro Guedes (2009), *Processo Penal – Tomo I*, Almedina, Coimbra.

Valente, Manuel Monteiro Guedes (2009), *Teoria Geral do Direito Policial*, 2.ª edição, Almedina, Coimbra.

Varela, Antunes; J. Miguel Bezerra; Sampaio e Nora (2009), "Manual de Processo Civil", citado em Magistrados do Ministério Público do Distrito Judicial do Porto, *Código de Processo Penal – Comentários e Notas Práticas*, Coimbra Editora, Coimbra.

Verdelho, Pedro (2004), "A obtenção de prova no ambiente digital" *in RMP*, Ano 25, n.º 99, Julho – Setembro.

Verdelho, Pedro (2004), "Apreensão de correio electrónico em Processo Penal" *in RMP*, Ano 25, n.º 100, Outubro – Dezembro.

Verdelho, Pedro (2008), "Técnica no novo C.P.P.: Exames, perícias e prova digital", *in Revista do CEJ*, n.º 9.

Legislação:

Constituição da República Portuguesa

Código de Processo Penal

Código Penal

Código Civil

Lei n.º 5/2004 de 10 de Fevereiro – Lei das Comunicações Electrónicas

Lei n.º 41/2004 de 18 de Agosto – Tratamento de dados pessoais e protecção da privacidade no sector das comunicações electrónicas;

Lei n.º 48/2007, de 29 de Agosto – 15.ª alteração ao Código de Processo Penal;

Lei n.º 53/2007, de 31 de Agosto – Lei Orgânica da Polícia de Segurança Pública;

Lei 32/2008, de 17 de Julho – Conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações;

Lei n.º 53/2008, de 29 de Agosto – Lei de Segurança Interna;

Lei n.º 38/2009, de 20 de Julho, que define os Objectivos, Prioridades e Orientações de Política Criminal para o biénio de 2009-2011;

Lei n.º 109/2009, de 15 de Setembro – Lei do Cibercrime;

Portaria 469/2009, de 6 de Maio

Portaria 915/2009, de 18 de Agosto

Jurisprudência:

ACR do Tribunal Constitucional n.º 410/2001, de 02/09/2001 *in* http://www.tribunalconstitucional.pt

ACR do Supremo Tribunal de Justiça n.º 06P2321, de 20-09-2006 *in* http://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/2e7cf04133dd20f78025723d005a62ab?OpenDocument&Highlight=0,06P2321.

ACR do Tribunal da Relação de Coimbra n.º 607/06, de 29-03-2006 *in* http://www.dgsi.pt/jtrc.nsf/8fe0e606d8f56b22802576c0005637dc/553a95b9c55abec18025716800494c3d?OpenDocument.

ACR do Tribunal da Relação de Coimbra n.º 1265/06, de 17-05-2006 *in* http://www.dgsi.pt/jtrc.nsf/0/2a93252854f5d54c8025717d00377214?OpenDocument

Cfr. ACR do Tribunal da Relação de Lisboa n.º 5150/2005-3, de 13-10-2004 *in* http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/2e8989f0e7de2437802570ab00575823?OpenDocument&Highlight=0,apreens%C3%A3o,correio,electr%C3%B3nico.

ACR da Relação de Lisboa n.º 3453/2008-5, de 15-07-2008 *in* http://www.dgsi.pt/Jtrl.nsf/0/9182245992c7c5d18025749000503b8c?OpenDocument.

ACR do Tribunal da Relação do Porto, n.º 0844093 (JTRP00041933), de 10-12-2008 *in* http://www.dgsi.pt/jtrp.nsf/0/673fcb5dc0168da6802575220056a553?OpenDocument.

ACR do Tribunal da Relação do Porto n.º 0715930, de 26-03-2008 *in* http://www.dgsi.pt/jtrp.nsf/c3fb530030ea1c61802568d9005cd5bb/24cd01e84ff51ff88025741e0034cc7e?OpenDocument&Highlight=0,imagens,v%C3%ADdeo,prova.

ACR do Tribunal da Relação do Porto n.º 0514155, de 15-02-2006 *in* http://www.dgsi.pt/jtrp.nsf/d1d5ce625d24df5380257583004ee7d7/f0bc5863ddd1c7618025711b004fae50?OpenDocument.

ACR da Relação do Porto n.º 1978/09.4JAPRT-B.P1, de 07-07-2010 *in* http://www.dgsi.pt/jtrp.nsf/c3fb530030ea1c61802568d9005cd5bb/d81b24cfc47ba41e802577c1004d383c?OpenDocument.

Outros documentos e referências:

Andrade, Manuel da Costa (2011), "Escutas telefónicas e conhecimentos fortuitos" *in* conferência dia 23-02-2011, Abrantes.

Best Practives For Seizing Electronic Evidence v.3, *A Pocket Guide for First Responders* - U.S. Department of Homeland Security, United States Secret Service.

Código de Conduta das Nações Unidas para os Responsáveis pela Aplicação das Leis;

Declaração Universal dos Direitos do Homem;

Dicionário "O Português Essencial", Selecções do Reader's Digest, Porto Editora;

Guia para recolha e interpretação dos cabeçalhos técnicos dos *e-mails* – DIAP;

"Intervención y/o interceptación de correo electrónico", *in* Revista *Ciencia policial – Revista Técnica del Cuerpo Nacional de Policía*, n.º 96, OCT 2009;

Manual de boas práticas para a recolha e apreensão de prova digital – PSP;

Projecto de Lei n.º 240/X – Regime de Obtenção da Prova Digital Electrónica;

Rapport explicatif de la Convention sur la cybercriminalité (STE n.º 185), disponível para consulta em: http://conventions.coe.int/Treaty/fr/Reports/Html/185.htm (acedido em 28-02-2011);

ANEXOS

ANEXO 1 – Guião de entrevista a aplicar aos entrevistados civis

1) Tendo como principal objecto de estudo o correio electrónico, e atendendo à modernização das formas de comunicação e à crescente facilidade no seu acesso, considera útil o acreditar dos meios de (obtenção de) prova de qualidades direccionadas para a recolha de prova digital?

2) O artigo 189.º do CPP estende o regime aplicável às intercepções telefónicas ao correio electrónico. No entanto, também o artigo 179.º se refere à apreensão de qualquer tipo de correspondência, que não apenas a tradicional. Sob que tipo de regime considera que o correio electrónico e os respectivos anexos se devem reger, tendo actualmente também a Lei 109/2009 (Lei do Cibercrime) um prenúncio sobre este tipo de matéria?

a. E o que tem a dizer em relação a uma total autonomização de regime?

3) O processo de envio de um *e-mail* pode, no essencial, dividir-se em dois momentos de diferente valência axiológico-material: o momento de transmissão e o momento de arquivo na plataforma receptora (momento posterior à comunicação). Até que ponto um *e-mail* recebido e aberto deve ter tratamento jurídico diferente de um não aberto, tendo em conta a possibilidade de se marcarem como não lidos os *e-mails* já abertos?

a. E qual o tratamento legal a dar aos e-mails impressos?

4) Em matéria de validações, regimes e prazos, até que ponto pode o princípio da subrogação do JIC às partes ausentes, interferir na recolha de prova digital, em particular no correio electrónico?

5) Aludindo ao tipo criminal previsto no artigo 194.º do CP e às relações de dependência entre as Autoridades Judiciárias e os OPC's, em que circunstâncias poderá a Polícia pisar o limiar da prática do crime de violação de correspondência ou de telecomunicações, em matéria de recolha de prova digital (em particular os e-mails)?

ANEXO 2 – Guião de entrevista a aplicar ao entrevistado polícia

1) Tendo como principal objecto de estudo o correio electrónico, e atendendo à modernização das formas de comunicação e à crescente facilidade no seu acesso, considera útil o acreditar dos meios de (obtenção de) prova de qualidades direccionadas para a recolha de prova digital?

2) Considera as Forças de Segurança – com competência de OPC – dotadas de suficientes capacidades operacionais para recolha de prova digital, em particular de correio electrónico?

3) Atendendo ao princípio da oportunidade da actividade policial, como pode a PSP ser promotora de diligências fundamentais na preservação e recolha de prova digital?

4) Até que ponto considera a alínea *l)* do n.º 3 do artigo 7.º da LOIC (competência reservada da PJ para a investigação de crimes "informáticos e praticados com recurso a tecnologia informática"), como um entrave à recolha de prova digital, em particular o correio electrónico, por parte da PSP?

ANEXO 3 – Entrevista ao Professor Doutor Manuel da Costa Andrade (18/03/2011)

1) Tendo como principal objecto de estudo o correio electrónico, e atendendo à modernização das formas de comunicação e à crescente facilidade no seu acesso, considera útil o acreditar dos meios de (obtenção de) prova de qualidades direccionadas para a recolha de prova digital?

Bom, é evidente que a prova digital tem uma eficácia probatória irrecusável, até porque, além do mais, surpreende as pessoas na sua inocência de comunicação, não sabem que aquilo que comunicam vai ser amanhã objecto de prova utilizado contra eles, e, portanto, as pessoas são surpreendidas na sua autenticidade. Nalguns casos, a prova digital tem quase a força probatória de uma confissão. De todo o modo, como em geral acontece aqui, vigora o chamado o princípio da livre convicção do tribunal, não o princípio da prova formal. Isto é, um *e-mail* não é por si só a prova definitiva, tem de ser integrado no contexto probatório, passando tudo naturalmente pela livre convicção do juiz. Mas, obviamente pela natureza das coisas, a prova digital terá seguramente uma grande força de convicção, por isso é que também o seu uso deve ser moderado atendendo à sua "deslealdade", porque todos os chamados meios ocultos de prova, e este é um deles, são desleais, isto é, apanham as pessoas sem saberem que estão a ser interrogadas e, no fundo, há aqui uma certa violação da privacidade das pessoas tal como violam as relações de amizade e de afecto, até os segredos dos profissionais.

Por isso é que, do meu ponto de vista, as sociedades modernas não podem renunciar a estes meios na luta contra o crime mais grave e sobretudo contra aquele crime mais perverso – que às vezes não tem a ver com a gravidade – por exemplo, um homicídio é um crime particularmente grave, mas é fácil de provar sem recurso a isto. Agora, há aqueles crimes que provocam uma grande solidariedade entre os seus intervenientes e não há a tendência de nenhum deles para procurarem por exemplo a ajuda da polícia ou das autoridades. Portanto, há aqui crimes que têm tendência para se tornar num santuário de solidariedades intrínsecas. Normalmente são aqueles crimes que se analisam não numa relação de conflitualidade entre as partes (o A mata B, ou o A rouba B), mas numa relação de fornecedor e cliente, como a corrupção, os tráficos de armas, de droga, toda a

criminalidade económica e, portanto, para estes casos, deve ser utilizado. No entanto devemos sempre subordinarmo-nos a princípios de proporcionalidade. Há meios informáticos mais gravosos e outros menos gravosos, por isso os mais gravosos devem ser restritos às formas mais graves de criminalidade e às formas onde eles sejam mais necessários. Por isso, dizia eu que há exigências de proporcionalidade mas também de subsidiariedade.

2) O artigo 189.º do CPP estende o regime aplicável às intercepções telefónicas ao correio electrónico. No entanto, também o artigo 179.º se refere à apreensão de qualquer tipo de correspondência, que não apenas a tradicional. Sob que tipo de regime considera que o correio electrónico e os respectivos anexos se devem reger, tendo actualmente também a Lei 109/2009 (Lei do Cibercrime) um prenúncio sobre este tipo de matéria?

Aqui estamos perante matérias relativamente novas. A matéria das comunicações electrónicas e resposta do direito e do processo penal estão em constante mudança. Como dizia Heraclito: "não nos lavamos duas vezes na mesma água" porque quando voltamos a falar da mesma matéria as coisas já mudaram, já estamos a falar de coisas novas.

Portanto, esta novidade não permite que haja já ideias relativamente estabilizadas e definitivas, por isso as coisas vão-se clarificando. Eu penso que hoje as coisas tendem a clarificar-se neste sentido: uma coisa são as comunicações em relação às quais as partes têm um domínio total e podem controlar integralmente, outra coisa são as comunicações na parte em que o domínio não lhes pertence a eles mas sim à entidade fornecedora dos serviços, às empresas de telecomunicações. No primeiro caso, quando as pessoas têm o domínio sobre a comunicação, tanto sobre o conteúdo, como sobre os dados, elas não devem gozar da tutela das telecomunicações, mas devem gozar de um benefício mais restritivo e, portanto, menos aberto. Refiro-me ao regime da apreensão da correspondência. Explicando melhor as coisas: por exemplo, no que toca ao correio electrónico, há fases que ele é verdadeiramente uma telecomunicação, isto é, os seus destinatários não têm domínios sobre a comunicação. Sem eles saberem, a empresa pode aceder a tudo, dar a conhecer tudo ao Estado, isto é, à Polícia e ao MP. Aqui deve-se reportar o regime das escutas telefónicas. Coisa diferente é em relação aos *e-mails* que já foram recebidos e lidos, e que o destinatário guarda no seu próprio computador. Aqui eu penso que se tratam de um documento igual a qualquer outro. Do meu ponto de vista nem sequer deve ter a tutela da

correspondência, porque como é sabido há três regimes aqui implicados: o da apreensão de documentos, o da apreensão de correspondência e da intromissão nas telecomunicações (vulgo escutas), cada um destes mais exigente que o anterior, tanto no catálogo de crimes a que se destinam, como na entidade que pode autorizar ou aplicar a medida, (nuns casos pode a Polícia, noutros já é preciso o MP, noutros tem que ser mesmo um juiz).

Portanto, eu penso que os *e-mails* que a pessoa abriu, leu e guardou no seu computador são documentos, nem sequer são correspondência. Quando o *e-mail* está na fase de transmissão, é uma telecomunicação.

Há um caso especial que hoje a doutrina começa a chegar a acordo que é o caso dos *e-mails* lidos, recebidos, no entanto não guardados no computador mas sim no *Internet Service Provider*, ou seja, aqueles que voltam ao sistema informático do servidor. Hoje entende-se que estes também devem ter a tutela das telecomunicações. Isto porque não estão no domínio da pessoa, isto é, a empresa das telecomunicações pode lá aceder e devassá-los sem passar pela pessoa. Aqueles que o destinatário, recebeu, leu e guardou, tem em relação a eles possibilidades de auto tutela, pois pode fazer com eles o que quiser. Se os guarda, não pode estar a espera que o direito processual lhe dê a tutela máxima.

Relativamente à questão despoletada pelo artigo 189.º do CPP, quando refere a extensão da sua aplicação também às comunicações mantidas ou guardadas em suporte digital, eu julgo que essa é uma das partes mais infelizes da reforma de 2007, da qual fui muito crítico no livro que escrevi (“Bruscamente no Verão Passado”). Esta questão está completamente errada porque quando ficam guardadas em suporte digital passam a ser documentos, não tem nada a ver com telecomunicações. De resto, hoje a LC já muda isto, no artigo 17.º diz que isto está sujeito às apreensões de correspondência.

Portanto, do meu ponto de vista, (e eu como jurista em principio estou contra os agentes da repressão), penso que esta solução não é a solução mais justa. Quando guardados em suporte digital nem deviam ser tutela de correspondência, deviam ser a tutela dos documentos, mas de facto a LC já apresenta um passo em relação ao CPP, porque, segundo o artigo 189.º do CPP, tinha de se verificar todo o apertado regime das escutas. Agora este já é um quadro completamente diferente, o catálogo de crimes já é o da apreensão de correspondência, que é muito mais generoso que o outro para a Polícia.

a. E o que tem a dizer em relação a uma total autonomização de regime?

Esta é uma questão mais de sistematização do que de substância. Não há nenhuma desvantagem em agrupar as coisas se elas forem semelhantes. É evidente que a comunicação telefónica é uma coisa, a comunicação por telegrama é outra, a por telecópia é outra, por *e-mail* é outra, a comunicação de voz através da internet é outra… Mas penso que colocam na relação entre os cidadãos e as instâncias de controlo, problemas sensivelmente semelhantes e do ponto de vista da simplicidade tudo se ganha, na medida do possível, se os regimes forem unitários.

Agora isto é um problema de sistematização, se nós quiséssemos desenvolver muito os regimes, então poríamos um capitulo para cada um. Eu sou de uma escola, que é a Escola de Direito de Coimbra, que procura fazer as coisas por teoria geral, isto é, o que nós pudermos dizer através de uma fórmula geral, não dizemos em particular. E nós devemos confiar nos princípios gerais, porque eles só por si são uma grande aquisição.

Neste assunto em particular, a LC veio tentar encurtar o âmbito geral da lei, mas eu acho está muito mal feita, também tem muitas contradições entre ela e, sobretudo, o que não se fez quando se criou esta LC foi dizer que na parte em que ela não é compatível com o CPP, fica revogado o CPP no artigo "tal e tal", por exemplo, o artigo 17.º da LC revogou aquele bocadinho do artigo 189.º do CPP. Quando a LC foi feita, o legislador disse que o CPP fica inteiramente em vigor, porque não quis dar a mão à palmatória. Isto é o que se chama "uma revisão envergonhada do Código". Até porque na LC não há desde logo uma uniformidade da linguagem. Aqui fala-se em prova digital, ali fala-se em prova electrónica, é a mesma coisa? Eu penso que sim! Mas então para quê dois conceitos? Só se devem usar dois nomes quando há duas coisas diferentes.

Portanto, ainda não temos em Portugal uma linguagem com uma categorização e um sistema devidamente estruturado. Porque todas estas leis – revisão do CPP de 2007, a LC, e Lei n.º 32/2008, de 17 de Julho – dá a impressão que foram feitas cada uma por seu legislador, separados no tempo, separados na história e separados por um grande abismo civilizacional. Ora, a verdade é que foi o mesmo legislador, a mesma Assembleia da República (AR) em Portugal, mas só que na AR, hoje, há um défice muito grande de competência técnica. E é por isto é que sai isto que causa bastante engulho às polícias, ao MP, às universidades… E quem é que ganha com isto? Os criminosos. A melhor coisa que pode haver para os criminosos são leis confusas ou então mudanças permanentes de lei, que originam situações de *in dubio pro reo* ou *in dubio pro libertate*, porque entre a lei

nova e a lei velha vão sempre "escapando umas enguias" que nós não conseguimos agarrar.

3) O processo de envio de um *e-mail* pode, no essencial, dividir-se em dois momentos de diferente valência axiológico-material: o momento de transmissão e o momento de arquivo na plataforma receptora (momento posterior à comunicação). Até que ponto um *e-mail* recebido e aberto deve ter tratamento jurídico diferente de um não aberto, tendo em conta a possibilidade de se marcarem como não lidos os *e-mails* já abertos?

É evidente que há aqui dois momentos com duas fases e regimes completamente diferentes, e faz todo o sentido como está aqui estabelecida a distinção na questão. Mas numa perspectiva analítica há quem diga: bom, existe desde logo a fase em que o autor escreve o *e-mail* e ainda não o enviou (em que é um documento), depois há o envio para o servidor do próprio remetente, esse envia para o servidor do destinatário e depois o destinatário é que o chama ao seu conhecimento. Depois lê-o e ele guarda-o, mas este guardar pode ser uma de duas coisas: ou guarda no seu próprio sistema (no seu computador, ou num disco à parte), ou devolve-o para o servidor, ou até imprime, mas mantém no servidor. Portanto, podem ser aqui vistas muitas fases.

O que cada pessoa devia fazer, por razões de cautela, era ler, apagar e imprimir o *e-mail*, pois aí estava sempre sobre o seu controlo.

De facto a distinção dos dois momentos que faz na questão faz toda a diferença. No entanto, talvez mais importante que isso seja o ter ou não ter o domínio sobre a comunicação, sobre a mensagem. Se a mensagem é recebida, lida, imprimida em papel, guardada no computador, num disco externo ou em qualquer outro suporte, adquire a natureza de documento simples. Quando, pelo contrário, a mensagem fica guardada no servidor, a tendência agora, pelo menos no Tribunal Constitucional Alemão, é dizer que o *e-mail* guardado no servidor, no *ISP*, ainda deve ter a tutela das telecomunicações, independentemente de ser lido ou não.

a. E qual o tratamento legal a dar aos e-mails impressos?

São documentos escritos como quaisquer outros.

4) Em matéria de validações, regimes e prazos, até que ponto pode o princípio da subrogação do JIC às partes ausentes, interferir na recolha de prova digital, em particular no correio electrónico?

Esta pergunta coloca-nos directamente com uma questão que é a reserva de juiz e qual o papel que o juiz deve ter neste contexto do correio electrónico. O juiz em princípio só profere decisões depois de ouvir as duas partes. Há um princípio de direito que diz que a Administração decide na linha dos seus interesses. O juiz, no acto jurisdicional, obedece sempre ao princípio de ouvir ambas as partes. Ora, aqui (quando se trata de escutas) não se pode ouvir ambas as partes, porque está tudo oculto, sob pena de se perder a eficácia.

Portanto, entende-se hoje em dia que o juiz deve ser particularmente exigente e ser ele, no seu próprio processo psicológico, a mobilizar os argumentos que a pessoa atingida diria (será que há o crime do catálogo? Será que há o grau de suspeita? Será que há a necessidade?). Ou seja, o juiz tem de subjectivizar, interiorizar as resistências que o outro faria, para que de alguma maneira, no seu próprio espírito, consiga fazer aquela contraposição de pontos de vista a que um juiz tem sempre de se subordinar.

Como já referi, um juiz decide sempre na base de duas opiniões, nunca pode seguir na base de uma só. Mas aqui ele decide só na base de uma, que é do MP, mas é justamente aí que o juiz tem de contrapor alguma coisa, subrogando-se às partes ausentes através do princípio da reserva do juiz.

O juiz é uma espécie de sucedâneo do contraditório, interiormente ele faz uma pura simulação intelectual das implicações das suas decisões. Tudo isto para evitar o que acontece muitas vezes, que é um bocado chocante, que é a proporcionalidade que há entre pedidos de escutas e de outros meios, e as respectivas respostas positivas.

Eu tenho dito que os juízes em Portugal são bastante ciosos, por exemplo na pena de prisão preventiva, mas muito desleixados aqui. Isto às vezes para as pessoas tem consequências muito piores do que a prisão preventiva. Uma escuta telefónica pode ser desastrosa para uma pessoa e a prisão preventiva pode não ser assim tão pejorativa. Isto não é um discurso 100% simpático para a polícia como instituição, mas é um discurso onde temos de equilibrar todos os interesses, sobretudo quando está em causa uma diferença muito grande entre a chamada criminalidade comum (que é a criminalidade de pessoas que vivem na sociedade e respeitam os valores da sociedade) e a criminalidade que representa por si só um desafio aos alicerces da sociedade. Aí a lógica deve ser completamente outra: em relação àquelas pessoas que são contra o nosso modelo de civilização, ao nosso modelo

de Estado de Direito (o terrorismo, negócios de armas e droga, etc.). A lógica deve ser a de privilegiar esses domínios com grandes meios de devassa intromissão, mas não permitir que eles depois escorram para a criminalidade comum se não for necessário. Eu costumo usar a seguinte expressão: "o processo penal comum não deve ser colonizado por um processo criminal de luta", por exemplo, contra o terrorismo. Eu não quero dizer com isto que admito dois processos penais. Mas que defendo um processo muito musculado na luta contra o terrorismo e esta criminalidade mais danosa, não tenho dúvida nenhuma.

5) Aludindo ao tipo criminal previsto no artigo 194.º do CP e às relações de dependência entre as Autoridades Judiciárias e os OPC's, em que circunstâncias poderá a Polícia pisar o limiar da prática do crime de violação de correspondência ou de telecomunicações, em matéria de recolha de prova digital (em particular os e-mails)?

Em tese, quando a lei reúne os pressupostos, por exemplo das escutas telefónicas e da intromissão de correio electrónico (que são sensivelmente idênticas), já fez a ponderação toda e diz até onde admite a compressão da liberdade e da privacidade, o que significa que nem a Polícia nem o MP e nem mesmo o Juiz, podem substituir-se ao legislador. Portanto sempre que se ultrapassam aqueles limites legais, em princípio entra-se no campo da ilicitude, o que não quer dizer necessariamente que o polícia seja punido, até porque pode não ter culpa. Isto só quer dizer que não está justificado. Imaginemos que o polícia actua não só para perseguir um criminoso, mas também para salvar uma vítima, aqui o quadro já é outro. Depois imagine-se que não estava lá vitima nenhuma, mas ele pelo menos acreditou, portanto, aqui já é um problema de culpa.

Agora, no que toca à ilicitude, ela não existe enquanto se actua dentro dos pressupostos legais. Agora, dá-se o caso por exemplo de a policia estar a fazer uma escuta ou um acesso a correio electrónico que ultrapassa os pressupostos legais. Aqui, se foi autorizado pelo MP, o polícia em principio age sem culpa, porque ele não é propriamente o jurista. Há aqui um erro sobre a ilicitude que é perfeitamente não censurável. Ele actua ilicitamente mas sem culpa e, portanto, não pode ser punido.

Questão 4 do 2.º guião) **Até que ponto considera a alínea *l)* do n.º 3 do artigo 7.º da LOIC (competência reservada da PJ para a investigação de crimes "informáticos e praticados com recurso a tecnologia informática"), como um entrave à recolha de prova digital, em particular o correio electrónico, por parte da PSP?**

Vistas as coisas do nosso ponto de vista, que é o da reflexão universitária e dos grandes princípios sobre o direito, nós reportamos este assunto para a chamada polícia criminal. Agora, saber em concreto qual o OPC adequado, já é um problema de repartição de funções e de organização. Para mim a melhor opção é aquela que for mais eficaz na luta contra o crime. Mas isto só pode ser respondido por quem tem a experiência de "investigação" que eu não tenho.

Já do ponto de vista do direito eu não posso dizer que o melhor é o mais eficaz… A mais eficaz, por exemplo, era cortar as mãos aos ladrões. Na actividade de investigação criminal já existe os critérios de eficácia e de adequação. Mas quem os pode dizer é quem anda no terreno, ou pelo menos quem dirige as pessoas que andam no terreno. Portanto, para mim, como jurista e cultor do direito, qualquer solução serve. Este é um problema de intendência de repartição, não de direito, não de justiça.

ANEXO 4 – Entrevista ao Professor Doutor Germano Marques da Silva (17/03/2011)

1) Tendo como principal objecto de estudo o correio electrónico, e atendendo à modernização das formas de comunicação e à crescente facilidade no seu acesso, considera útil o acreditar dos meios de (obtenção de) prova de qualidades direccionadas para a recolha de prova digital?

Útil enquanto regulamentar pode ser, mas não é necessário, porque toda esta matéria é considerada correspondência e a regulamentação sobre correspondência já é exaustiva no Código do Processo Penal. O que acontece é que a legislação moderna é tudo regulamentado, que é um dos males do nosso tempo, pega num código português e compara com um código americano, ou até mesmo num inglês e vê a diferença. Em Portugal legisla-se demais porque se quer dizer tudo de todas as coisas, e aquilo que o legislador deve estabelecer são os princípios, não são os regulamentos. Portanto, nesta matéria, regulada a correspondência, está regulado o correio electrónico que é uma forma de correspondência.

No entanto temos de fazer a destrinça entre duas coisas. Uma coisa é a correspondência enquanto não está aberta, que é um problema de intercepção (tal como as escutas), outra coisa é a correspondência depois de aberta, que é um problema de apreensão de um documento – ou um tipo de correspondência aberta.

2) O artigo 189.º do CPP estende o regime aplicável às intercepções telefónicas ao correio electrónico. No entanto, também o artigo 179.º se refere à apreensão de qualquer tipo de correspondência, que não apenas a tradicional. Sob que tipo de regime considera que o correio electrónico e os respectivos anexos se devem reger, tendo actualmente também a Lei 109/2009 (Lei do Cibercrime) um prenúncio sobre este tipo de matéria?

Aqui no correio electrónico há duas realidades: o correio antes de ser aberto e o correio depois de ser aberto. Antes de ser aberto é em tudo semelhante a uma escuta telefónica, porque há aqui todo um problema de intercepção, podendo-se admitir que os

mecanismos de escuta ou de intercepção electrónica acedem ao meio, isto é, ao conteúdo, o que não acontece com a correspondência escrita, pois é preciso abri-la. Se eu criar um mecanismo de controlo ou de intercepção dos *e-mails* através do servidor eu posso ver qual é o conteúdo, dai que ela tenha que ser colocada aqui junto à correspondência. O CPP estabelece uma determinada tramitação, tem um determinado elenco de crimes para os quais é possivel a intersecção telefónica. O que surge com a LC é um alargamento do âmbito dos crimes, ou seja, temos aqui uma forma de facilitação.

Depois de aberta a mensagem de correio electrónico e de arquivada no computador ou em fotocópias, torna-se correspondência, portanto está sujeita às mesmas regras que outros tipos de correspondência normais, um telegrama ou outra coisa qualquer**.**

a. E o que tem a dizer em relação a uma total autonomização de regime?

Esta questão, apesar de não ser propriamente necessária, pode ser útil porque hoje como há muita gente a intervir em tudo isto, pode não haver uma unidade de orientação, portanto, isso pode ter a vantagem de clarificar: é o drama do nosso tempo,a chamada regulamentação, porque precisamente há muitas dúvidas, então o melhor é esclarecer. Pode ser útil, não tenho dúvida. E eu sou um dos que defendo que sempre que se suscita uma dúvida não vale a pena estarmos a espera que os tribunais se decidam, porque às vezes só ao fim de 10 ou 15 anos é que eles se decidem, e pelo caminho há muitas contradições. Portanto, se há uma situação que está a suscitar alguma dúvida na aplicação da lei, o melhor é resolvê-la rapidamente. O problema das intersecções das comunicações informáticas levanta muitas dúvidas, nomeadamente o saber se isto é mesmo equiparado às escutas telefónicas, um email antes de abrir, etc... Todas estas dúvidas se levantaram e ainda continua de alguma forma a doutrina a discutir. Neste sentido, pode ser útil para clarificar tudo isso, pois se há dúvidas ainda, e nós sabemos que há, sobretudo na apreensão.

Antigamente não se pensava assim. Havia a letra da lei e depois esperava-se que a jurisprudência a clarificasse, isto porque o legislador tem sempre dificuldade em prever todas as hipoteses. Isto era feito para evitar estar sempre a alterar os códigos. Mas hoje é melhor alterares os códigos porque estão todos informatizados, já não é preciso ter códigos em papel, dai ser fácil alterar e, se ajudar a clarificar e a evitar contradições e violações dos principios, deve fazer-se, é útil, é conveniente.

3) O processo de envio de um *e-mail* pode, no essencial, dividir-se em dois momentos de diferente valência axiológico-material: o momento de transmissão e o momento de arquivo na plataforma receptora (momento posterior à comunicação). Até que ponto um *e-mail* recebido e aberto deve ter tratamento jurídico diferente de um não aberto, tendo em conta a possibilidade de se marcarem como não lidos os *e-mails* já abertos?

Pois, eu penso que, neste momento a solução deve ser a da correspondência tradicional, pode ser aberta ou não aberta. Se ainda não está aberto deve ser tratado como correspondência fechada. Na dúvida se foi ou não foi aberto, devo ser garantístico. Tenho é que ter o juiz a intervir, autorizar a abertura. Fazendo a analogia com as cartas em papel, não precisamos de ter garantia que a carta não foi aberta, mesmo que ela tenha sido aberta não tem importância nenhuma, eu quero é aceder ao conteúdo. Então há duas hipóteses: ou o conteúdo está aberto, ou se estiver fechado eu presumo que não foi aberto. A correspondência sempre teve um problema por tradição liberal – que já vem da revolução francesa – que é a reserva de intimidade da vida privada. Portanto na dúvida se foi aberto ou não foi aberto, vou tratá-lo como não tendo sido. É todo um problema quase de tradição. Aquilo que mexe com a intimidade deve passar primeiro pelas mãos do juiz para este ponderar a sua importância ou não importância.

a. E qual o tratamento legal a dar aos e-mails impressos?

Considerou já ter respondido.

4) Em matéria de <u>validações</u>, <u>regimes</u> e <u>prazos</u>, até que ponto pode o princípio da subrogação do JIC às partes ausentes, interferir na recolha de prova digital, em particular no correio electrónico?

O legislador diz que só quer autorizar determinados meios de investigação relativamente a determinados crimes. Aos outros considera-se que esses meios são excessivos. A ideia de que se deve procurar a verdade por todos os meios é errada em democracia. A CRP no artigo 18.º diz que os direitos, liberdades e garantias devem ser limitados proporcionalmente. A questão da proporcionalidade quer dizer que por coisas sem importância não se deve usar certos meios extraodinariamente gravosos. Portanto, há

aqui uma escala de importância e um conflito de interesses, entre a justiça e a privacidade, sendo que a lei não hierarquiza dizendo que a justiça é superior, embora isto já tenha acontecido no passado. Tem de haver aqui uma certa proporção. Se é um crime que se pode investigar por outros meios, não se deve recorrer aos meios mais gravosos. É daqui que advem a ideia do catálogo de crimes, que tem vindo a ser alargado, mas com muita oposição…

Essa ponderação de interesses é das coisas mais dificeis do direito. E acaba muitas vezes por ser uma ponderação politica. Nunca é uma ponderação juridica. O que é importante é que se faça politicamente em razão de um determinado ambiente cultural. Portanto, a questão de haver mais ou menos crimes de investigação, é uma decisão que deve vir beber ao artigo 18.º da Constituição, que vem dizer precisamente que as leis restritivas de direitos, liberdades e garantias têm de revestir um carácter geral e abstracto e não podem ter efeito retroactivo nem diminuir a extensão e o alcance do conteúdo essencial dos preceitos constitucionais.

5) Aludindo ao tipo criminal previsto no artigo 194.º do CP e às relações de dependência entre as Autoridades Judiciárias e os OPC's, em que circunstâncias poderá a Polícia pisar o limiar da prática do crime de violação de correspondência ou de telecomunicações, em matéria de recolha de prova digital (em particular os e-mails)?

A Constituição sobre a correspondência diz no artigo 34.º que "o domicílio e o sigilo da correspondência e dos outros meios de comunicação privada são invioláveis". Diz-nos ainda no n.º 4 que "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". Portanto, a Constituição faz alguma restrição, diz que não é possível aceder à correspondência por mais nada a não ser para processo criminal. Nos termos do processo criminal deixa ao legislador ordinário conformar as condições em que pode ser feito o acesso, tendo sempre presente o artigo 18 – a ponderação de direitos. Nunca a Constituição fala em emails. O que acontece é que esta Constituição é de 1976 e as novas realidades têm de ser enquadradas nalguma coisa, tendo sido equiparado à correspondência; o meio de transmissão é que é diferente.

Relativamente ao 189.º do CPP, quando refere que se aplica também às comunicações que se encontrem guardadas em suporte digital, eu fiz uma interpretação superficial,

porque aqui têm de estar verificadas as operações todas do artigo 188.º, porque são operações e relações técnicas. Antigamente entendia-se que a partir do momento em que a comunicação já tinha sido recebida, já não eram puramente escutas telefónicas, pois já estava recebida no computador, ainda que não aberta. O legislador veio clarificar que um *e-mail* ainda não aberto é considerado comunicação – é o mesmo problema da carta fechada.

Questão 4 do 2.º guião) **Até que ponto considera a alínea *l)* do n.º 3 do artigo 7.º da LOIC (competência reservada da PJ para a investigação de crimes "informáticos e praticados com recurso a tecnologia informática"), como um entrave à recolha de prova digital, em particular o correio electrónico, por parte da PSP?**

Tudo isto obedece a uma dinâmica que se vai alterando com o tempo. Há à trinta anos eu era um extremo defensor que a Polícia não deveria ter competências de investigação e só as passou a ter essas competências por necessidade. A PJ normalmente diz assim: é tanta a criminalidade que nós não temos capacidade, ou aumentam o efectivo da PJ ou não temos hipótese…

A Polícia e a GNR tinham as funções policial de carácter geral, ou seja, de medidas cautelares. Depois, a evolução obrigou todas as policias a desenvolver os departamentos de investigação, a alargar a formação para a parte da investigação e hoje temos uma grande quantidade de gente a investigar, embora eu não saiba se isso é ou não útil. A PJ quando nasce, em 1945 era fundamentalmente para investigar um conjunto de crimes mais complexos, mais técnicos, porque eles é que têm os laboratórios e meios materiais necessários, e quando apareceram as escutas o que se queria era que fosse um departamento da PJ a fazer todas as escutas, até mesmo para efeitos de concentração da fiscalização. Depois começaram a multiplicar-se os departamentos. Portanto, este é sempre um problema de como devem ser organizadas as forças, que é dinâmico e vai mudando.

Depois cria-se também um fenomeno interessante: é que quem tem competência para fazer determinada coisa, procura ser eficaz, portanto, todas as limitações à sua competência não são agradáveis. E isso é normal, não querer recorrer a outras forças, toda a gente tem o seu brio e quer fazer as coisas como deve ser, já que têm essa autonomia.

Mas sem dúvida nenhuma que dentro de pouco tempo, os poderes da PJ ficarão reservados para crimes de investigação muito complexa. A PJ no fundo é importante para as relações internacionais para evitar a dispersão. Ficará reservada, por exemplo, para

comunicações com a INTERPOL, para ligações transfronteiriças, etc. Antigamente, não há muitos anos, não se podia estabelecer qualquer relação internacional a não ser a partir do ministro dos negócios estrangeiros. Eram ligações governamentais. Hoje, grande parte dos acordos são por contacto directo.

ANEXO 5 – Entrevista ao Dr. Pedro Verdelho (15/03/2011)

1) Tendo como principal objecto de estudo o correio electrónico, e atendendo à modernização das formas de comunicação e à crescente facilidade no seu acesso, considera útil o acreditar dos meios de (obtenção de) prova de qualidades direccionadas para a recolha de prova digital?

Obviamente. Cada vez mais há prova digital das coisas. Para começar porque todos estamos na internet neste momento, isto porque uma pessoa a primeira coisa que faz quando chega a qualquer lugar é ligar o computador. Há vinte ou trinta anos atrás o computador ligava-se quando era preciso escrever um despacho, agora estamos sempre ligados. De manhã, quando uma pessoa está em casa acorda e liga o computador, ou por causa do skype para falar com familiares ou amigos, liga as redes sociais, etc. O que significa que a nossa actividade nestas redes é cada vez mais importante na parte criminal. Cada vez existem mais crimes na internet, a internet propiciou mais crimes e não são só crimes da competência de investigação da PJ, são crimes comuns da vida real e, por isto, cada vez mais a prova digital é importante. Não há, portanto, nenhuma dúvida quanto a isto, não há reservas, é uma questão de abordagem porque no fundo tudo isto é apenas uma questão de pensar objectivamente sobre as coisas.

2) O artigo 189.º do CPP estende o regime aplicável às intercepções telefónicas ao correio electrónico. No entanto, também o artigo 179.º se refere à apreensão de qualquer tipo de correspondência, que não apenas a tradicional. Sob que tipo de regime considera que o correio electrónico e os respectivos anexos se devem reger, tendo actualmente também a Lei 109/2009 (Lei do Cibercrime) um prenúncio sobre este tipo de matéria?

Este regime do Código do Processo Penal hoje em dia é residual por causa do artigo 11.º da LC**.** Residual porque aplicando-se a LC a todos os processos que envolvam sistemas electrónicos, ou seja, computadores, e aplicando-se a todos os crimes que suponham a recolha de prova digital, o regime já não é o do 179.º ou 189.º, mas já é integralmente o da LC, onde há no artigo 18.º um regime especifico de intersecção de

comunicações, portanto, já afasta a extensão do artigo 189.º, e por outro lado, quanto à apreensão do correio electrónico também há uma norma especial que diz mesmo "apreensão de correio electrónico" – o artigo 17.º - que tem um regime diferente, portanto, deslocalizou-se a questão do artigo 179.º e 189.º do Código Processo Penal para a LC.

Portanto, aquilo que fica para o Código Processo Penal é muito residual, é aquilo que não couber no artigo 11.º da LC, por exemplo *e-mails* impressos ou faxes. Ambos são documentos em papel, e sendo em papel, nem sequer são comunicações, embora isto seja discutível. Não estou a ver de momento mais nada, a não ser uma comunicação *online* – um *chat* por exemplo, onde a pessoa pode imprimir a conversa, se quiser, ou então pode guardar *prints* e imprimir, vai dar à mesma coisa – no fundo qualquer tipo de comunicações electrónicas impressas. Até com as *sms* do telemóvel a pessoa pode fazê-lo se tiver possibilidades disso, e hoje em dia facilmente tem, se tiver software apropriado para o fazer.

Portanto, não é que esta discussão dos artigos 179.º e 189.º tenha deixado de existir. Ela também existe, pode haver essa discussão no Código de Processo Penal pois ele é muito deficiente, tem uma técnica legislativa péssima, está redigido de uma forma desinteressante, e talvez por isso a sua aplicabilidade prática neste momento é muito residual em matéria de prova digital. É só quando não for aplicável a LC, isto porque, quanto a correio tradicional (cartas em papel, envelopes) está em vigor o artigo 179.º. Agora o artigo 189.º que se refere a todas as comunicações electrónicas e ao regime das escutas, esse é que é residual. E, apesar de este artigo lá incluir uma referência directa ao correio electrónico, ela acaba por ser afastada pelo regime especial contido na LC, que afasta este regime geral desde que ela própria seja aplicável, mas isto passa-se numa gama de situações de tal forma alargada que o regime especial na prática tem mais aplicabilidade que o regime geral. Parece um contra-senso mas não é. E ainda bem que assim é, porque enquanto que a LC é efectivamente aplicável na prática, o artigo nº179 era completamente inviável e ninguém o conseguia aplicar. Até porque o que importa quando se faz uma busca, além da possibilidade de encontrar *e-mails* impressos, é pesquisar aquilo que está no computador, os *e-mails* que lá estão ou estão ainda alojados *on-line*, embora sim, possa acontecer que o disco do computador tenha sido formatado, ou a informação possa ser perdida de alguma outra forma.

a) E o que tem a dizer em relação a uma total autonomização de regime?

A autonomização do regime está resolvida pela lei de Cibercrime, ou seja, este regime especial da Lei de Cibercrime deixou o Código de Processo Penal residual em matéria de prova digital. Esta resolução é devido a um artigo especial para a apreensão de correio electrónico que afasta a aplicabilidade do artigo 179.º do Código de Processo Penal, e portanto é por aqui que se resolve o problema da autonomização. Se calhar o Código de Processo Penal já devia ter ido por este caminho há muito tempo, e por isso é que digo que quem fez o Código de Processo Penal não pensou bem no assunto, escreveu a lei mal escrita. O legislador foi claramente incompetente neste aspecto. Mas enfim, tudo isto se encontra agora bem resolvido na LC, não quanto ao texto, mas quanto à substância, isto porque o texto da LC é um texto muito atravessado, difícil de ler. O texto é difícil de entender porque numa só frase tem dez ou doze linhas, sem pontos, só com vírgulas e algumas condicionantes. A minha interpretação é que esse artigo (17.º) afasta o 179.º em tudo o que não estiver previsto nele, porque tem uma remissão residual para a aplicação do regime da correspondência do CPP. Ora, quando começa por dizer que "se no decurso de uma pesquisa se encontrar correio electrónico…" isto significa que não é preciso um despacho inicial. Se nos recordarmos do artigo 179.º do CPP, diz que é necessário um despacho inicial do juiz e além disso diz que o juiz deve ser o primeiro a tomar conhecimento da correspondência, enquanto que, na minha opinião, o que o artigo 17.º da LC diz é que não é necessário este despacho inicial nem que o juiz seja o primeiro a tomar conhecimento.

O que é necessário é que, uma vez detectado o correio electrónico, este se leve ao juiz para que ele possa decidir sobre a sua validação ou não validação. E isto veja-se: é uma exigência da vida prática. Não é possível para cada computador que se apreende o juiz dizer antecipadamente que se deve apreender o correio electrónico. Na vida prática isso não é possível porque qualquer processo mais sofisticado supõe apreender um computador, por exemplo uma busca a uma empresa quando estiver em causa por exemplo uma fraude fiscal pode ser necessário apreender um computador, outro exemplo é um homicídio no qual também pode ser necessário apreender um computador.

Ainda como exemplo, um blogue em que uma pessoa insulta outrem, supõe apreender um computador. Ou seja, isto é um processo bastante simples de injúrias, que nos Estados Unidos não seria crime sequer porque se considera como liberdade de expressão. O que significa que se se fizer intervir o juiz em todos estes casos simples seria

incomportável. Só se for necessário juntar ao processo o correio electrónico é que é necessária a intervenção do juiz. Porquê que a lei não manda intervir o juiz antes (do OPC aceder ao conteúdo)? Porque na minha opinião serial irrealizável porque o correio electrónico num computador é um ficheiro, e quando uma pessoa vê uma série de ficheiros no computador não sabe se é correio electrónico, se é um ficheiro de *word* ou se é um ficheiro de *excel*. É certo que cada ficheiro tem a sua extensão, e as de uns não são iguais às dos outros. Contudo, qualquer pessoa as pode alterar, e isso altera todo o rumo das coisas, porque com essa alteração o ficheiro vai perder o seu formato original, e o que era correio electrónico pode deixar de o ser, e vice-versa. Se por exemplo utilizar o Outlook, todo o correio electrónico está virtualmente num só ficheiro. Portanto, se eu quiser transportar o meu correio deste computador para outro, não é uma mensagem por ficheiro, são todas as mensagens num só ficheiro, o que significa que de fora não é possível detectar o que é ou não é mensagem. Não permite, por exemplo, distinguir uma simples mensagem de "bom dia" vinda de um amigo, de uma mensagem completamente confidencial.

Face a estas barreiras electrónicas, a lei diz que nestes casos se deve fazer uma triagem para tentar ou não encontrar mensagens, se encontrar, aí sim, deve levá-las ao juiz para este decidir se as valida ou não. Nestes casos o juiz tem que ponderar no caso em concreto se justifica ou não justifica a violação do interesse que está em causa, que é o sigilo das comunicações. De acordo com as regras gerais, as quais regem o correio físico em papel, quando o juiz o recebe as cartas e as abre, vê quais são ou não de interesse. Aqui foi preciso encontrar este regime diferenciado para o correio electrónico, com regras específicas, porque caso contrário não seria possível avançar. Se cada vez que se apreendesse correio electrónico no *microsoft outlook*, ou outra aplicação de *e-mail* com regras específicas, se levasse esse ficheiro que contém todas as mensagens, de por exemplo 5 *gigabytes*, a um juiz, não seria possível avançar, porque as mensagens seriam tantas que a diligência acabaria por não ser viável. Além disso, a lei também tem de ser realista, tem de saber que aquilo que prevê é aplicável na vida prática.

Este é o meu entendimento quanto ao artigo 17.º, mas também há dúvidas quanto à sua interpretação, no sentido em que há pessoas que acham que a interpretação não pode ser esta, ou seja, acham que o correio electrónico deve ser todo pegado e levado em bloco ao juiz quando se detecta que existe. Eu acho que não. O que os juízes estão a fazer na prática em relação a isto é o que se fazia precisamente há quinze anos com as escutas telefónicas, que é perguntar aos polícias o que é que realmente interessa naquela imensidão de dados. Nem existe outra forma.

3) O processo de envio de um *e-mail* pode, no essencial, dividir-se em dois momentos de diferente valência axiológico-material: o momento de transmissão e o momento de arquivo na plataforma receptora (momento posterior à comunicação). Até que ponto um *e-mail* recebido e aberto deve ter tratamento jurídico diferente de um não aberto, tendo em conta a possibilidade de se marcarem como não lidos os *e-mails* já abertos?

Aqui importa comparar esta realidade com a do correio físico. A Constituição Portuguesa só protege o correio fechado, isto é, o correio físico em papel. Ou seja, uma carta aberta não tem protecção constitucional. A qualificação legal de uma carta aberta é a de um simples documento. Portanto seja qual for o escrito, se não estiver fechado, do ponto de vista legal valem todos o mesmo. Como a Constituição não diz nada relativamente à correspondência aberta, a lei ordinária através do Código de Processo Penal só criou o regime especial no artigo 179.º para a correspondência fechada. Portanto, de modo a levar as coisas ao extremo, por exemplo se eu tiver um catálogo de uma loja selado, tem mais protecção do que eu ter uma carta aberta com todas as minhas informações bancárias.

Esta questão existia (e no fundo ainda existe) no Código do Processo Penal. Acontece que na LC deixou de ser uma questão tão abrangente, porque, como já referi, o Código de Processo Penal tem uma aplicação residual em matéria de prova digital. A norma que a LC aplica neste caso concreto não distingue o correio aberto do não aberto – artigo 17.º - isto porque tecnologicamente é indiferente (o facto de estar ou não aberto). Aliás, veja-se que num computador eu posso ler uma mensagem e marcá-la como não aberta, ou então, cada vez que recebo uma mensagem numa caixa de *e-mail*, ter um mecanismo automático de reencaminhamento para a receber em duplicado noutro lado. Ou posso inclusivamente abrir os *e-mails* no meu telemóvel sem que o *outlook* saiba. Por todos estes motivos é que tecnologicamente não há diferença entre correio lido e não lido. Esta diferença para a LC é completamente nula, e na minha opinião muito bem.

a) E qual o tratamento legal a dar aos *e-mails* impressos?

Relativamente a *e-mails* impressos, já são considerados documentos sem protecção, porque são simples papeis e a LC fala em comunicações electrónicas.

4) Em matéria de validações, regimes e prazos, até que ponto pode o princípio da subrogação do JIC às partes ausentes, interferir na recolha de prova digital, em particular no correio electrónico?

Considerou já ter respondido.

5) Aludindo ao tipo criminal previsto no artigo 194.º do CP e às relações de dependência entre as Autoridades Judiciárias e os OPC's, em que circunstâncias poderá a Polícia pisar o limiar da prática do crime de violação de correspondência ou de telecomunicações, em matéria de recolha de prova digital (em particular os *e-mails*)?

Antes da LC, o sistema era extremamente dúbio e era fácil os OPC's escorregarem para uma situação em que se ficava sem saber se certa correspondência o era ou não. No entanto, e agora mais que nunca, o crime do 194.º não se pode cometer nunca. Aqui a única novidade terá que ver talvez com o n.º 2 (porque o n.º 1 refere-se sempre a correio de papel. Este artigo tem um problema de conciliação com o artigo 384.º do CP (violação de segredo de correspondência ou de telecomunicações). O 384.º é exclusivamente aplicável a funcionários dos serviços de correios, telégrafos, telefones ou telecomunicações e é um crime hoje em dia quase virtual porque já não há funcionários dos serviços de correios, telégrafos, telefones e telecomunicações, só há funcionários dos serviços de correios e telégrafos porque como os de telefones e telecomunicações são todos privados – já não são funcionários. Isto porque os funcionários são aqueles que estão previstos no artigo 386.º - funcionários da administração pública ou outros do mesmo tipo que se estendem na qualificação… Ora, as comunicações electrónicas não são nunca um serviço publico, são um serviço puramente privado e portanto já não cabem ali.

Na altura em que foi escrito, o 384.º era suposto ter a ver com o conteúdo da comunicação em si, e o 194.º com o registo em papel. Ora, isto faz centrar o 194.º num registo que fica uma comunicação: o n.º 1 em papel escrito, o n.º 2 tem de ser interpretado à luz da intromissão no conteúdo da telecomunicação ou do seu conhecimento (previsto sobretudo para faxes e telexes, mas também é aplicável a *e-mails*, porque os *e-mails* cabem no conceito de telecomunicação.

Em todo caso o n.º 2 tem de ser limitado, mais uma vez, com a LC. Portanto o OPC comete o crime se estiver a aceder a comunicações electrónicas sem consentimento.

Como no artigo 17.º não é preciso haver o despacho prévio do juiz para o acesso, esta é uma questão importante mas que se for seguida a LC, torna-se bastante pequena, o que também é de certa forma confortável para os OPC's.

***Questão 2 do segundo guião*) Considera as Forças de Segurança – com competência de OPC – dotadas de suficientes capacidades operacionais para recolha de prova digital, em particular de correio electrónico?**

As capacidades operacionais para a recolha de prova digital cingem-se, no fundo, a duas questões: chegar ao local e apreender o computador ou fazer uma cópia. Mas para isto se fazer é necessário que se garantam condições de fiabilidade de modo que a cadeia de custódia seja mantida. Ou seja, o que importa é que a cópia que eu tenho seja exactamente igual à que está no computador. Agora, como é que esta cópia de imagem se faz? Bom a LC prevê que se possa fazer através da assinatura digital. Fora isto não há grande solução. A não ser fazer um auto a dizer que fiz uma cópia e certifico-a como sendo fiel ao original. Isto porque hoje em dia toda a gente sabe fazer uma cópia, obviamente, o que não se sabe é se essa cópia é mesmo igual em relação às definições e às características. Qualquer coisa que esteja no computador e que seja aberto já é diferente daquilo que estava antes de ser aberto mesmo que eu não mude uma vírgula, já é um ficheiro electrónico diferente.

***Questão 4 do segundo guião*) Até que ponto considera a alínea *l)* do n.º 3 do artigo 7.º da LOIC (competência reservada da PJ para a investigação de crimes "informáticos e praticados com recurso a tecnologia informática"), como um entrave à recolha de prova digital, em particular o correio electrónico, por parte da PSP?**

Se calhar não é entrave nenhum. Hoje em dia a prova digital por correio electrónico é um conceito completamente autonomizado do crime informático. Obviamente que o crime informático tem prova que está em registo digital, mas uma coisa e outra são completamente diferentes. Há prova digital de crimes que não têm nada a ver com o mundo "*ciber*", com o informático, com o acesso ilegítimo. Muitas vezes o que está em causa é um crime clássico cometido por uma via diferente… mas isso tem de ser interpretado com o espírito da altura em que foi feito. Quando a LOIC refere tecnologia

informática, refere-se à manipulação informática. Por exemplo, muitos são os casos em que se fala em burla informática e de telecomunicações, mas, na realidade nada mais são que a normal burla prevista no artigo 217.º do CP, pois não houve "tratamento de dados ou estruturação incorrecta de programa informático", no fundo não houve manipulação informática. Portanto, o espírito da LOIC é o de manipular a tecnologia, o que não é o caso.

Por outro lado, se assim fosse, a PJ ficava inundada com crimes que não fazem parte do perfil típico de crimes que a PJ investiga. Pelo contrário, esse é o tipo de crimes que a PSP investiga, mais até que a GNR. Mas a PSP e a GNR para estes efeitos são tratadas em paridade. Portanto, o artigo 11.º da LC (âmbito), é aquele que vai acabar por, mais tarde ou mais cedo, deixar claro que a PSP e a GNR, vão ter que ter uma actividade muito forte na investigação da prova digital, ou melhor, vão ter que perceber como é que se obtém prova digital, como é que a mesma se interpreta, como é que se retira dos suportes, como é que se garante que ela está fiável. No fundo o que está em causa é sempre obter e manter a cadeia de custódia, porque a prova digital é alterável, ou seja, tem que haver uma forma de a garantir fiel à original.

ANEXO 6 – Entrevista ao Subintendente Dário Prates (22/03/2011)

1) Tendo como principal objecto de estudo o correio electrónico, e atendendo à modernização das formas de comunicação e à crescente facilidade no seu acesso, considera útil o acreditar dos meios de (obtenção de) prova de qualidades direccionadas para a recolha de prova digital?

Penso que sim. Várias razões poder-lhe-ei indicar para essa convicção. Primeiro, hoje, os suspeitos da prática de crimes também procuram, nas novas tecnologias, formas de se contactarem, formas de desenvolver a sua actividade criminosa, com recurso, quer à internet, quer a tecnologia que possa servir de plataforma de troca informação, estando obviamente relacionada com prova digital. Hoje, o mero traficante de rua pode aceder a uma aplicação informática para se contactar e, através dessa aplicação informática, contactar outros suspeitos para executar o crime de tráfico de estupefacientes. Portanto, há uma panóplia muito grande de crimes que são praticados por suspeitos também conhecedores destas novas ferramentas. E, cada vez mais, a Polícia terá que estar preparada para trabalhar também neste mundo digital, neste mundo tecnológico em que, muitas vezes, o sucesso de uma investigação, a prova para sustentar uma pena de prisão concreta em determinado crime, em determinada investigação, pode estar na prova digital. Assim, é exigível à Polícia que acompanhe estas novas realidades. Portanto, é fundamental, actualmente, termos conhecimentos e competências para recolher esta prova digital nos nossos processos.

2) Considera as Forças de Segurança – com competência de OPC – dotadas de suficientes capacidades operacionais para recolha de prova digital, em particular de correio electrónico?

A minha perspectiva tem a ver mais com a experiência que tenho na PSP, portanto não tenho a noção da realidade das outras Forças de Segurança e dos outros OPC. Também entendo que a ênfase da questão não incidirá tanto na capacidade operacional. Colocaria talvez a questão na capacidade e recursos técnicos. Isto porque, para recolha da prova digital há necessidade de, à partida, logo no momento da sua apreensão (ou na apreensão

de equipamento que possa ter prova digital), uma série de cuidados, de procedimentos que carecem de meios adequados para o efeito – seja para selagem de computadores, para bloqueamento de portas USB, para bloqueamento de telemóveis ou *smartphones*, etc. – que ainda não estão distribuídos ao efectivo. Por outro lado, a utilização de software para "tirar uma fotografia" àquilo que está em ambiente digital em determinado equipamento também não é, ainda, software que esteja disponível na Polícia de Segurança Pública. Portanto, esta questão terá mais a ver com detalhes técnicos, do que propriamente com questões de capacidade operacional. Nessa área ainda temos um caminho a desenvolver. Estamos cientes da importância da prova digital. Temos já difundido algumas boas práticas para a recolha da prova digital, mas efectivamente, para concretizar um bom trabalho nesta área, há ainda necessidade de percorrer mais algum caminho.

3) Atendendo ao princípio da oportunidade da actividade policial, como pode a PSP ser promotora de diligências fundamentais na preservação e recolha de prova digital?

Neste momento, a Polícia de Segurança Pública tem implementado o manual de boas práticas para a recolha de prova digital. Esse manual de boas práticas foi feito em conjunto com o Departamento de Investigação e Acção Penal de Lisboa, através de procuradores que estão a trabalhar mais especificamente nesta área e também com o perito de informática daquele Departamento. Esse manual foi difundido para aplicação na área da Investigação Criminal. A par desse manual de boas práticas foi também recebido, da parte do DIAP de Lisboa, um guião para recolha de cabeçalhos técnicos, que é um documento de extrema importância para a recolha da prova digital quando o crime é praticado através de correio electrónico. Assim, conseguimos providenciar capacidade à PSP para, no momento da apresentação da queixa, através da análise dos cabeçalhos técnicos de correio electrónico utilizado para a prática do crime, conseguir salvaguardar e acautelar logo os meios de prova existentes. Portanto, estamos a falar do primeiro momento em que há o contacto da vítima com a polícia e, independentemente da competência de investigação do crime ser nossa, da PJ ou da GNR, teremos que ter, logo à partida, capacidade e competência técnica para receber a queixa, para salvaguardar de forma urgente os meios de prova. Isto no que respeita ao correio electrónico. No que diz respeito ao manual referido, foi um manual que se destina mais à vertente da Investigação Criminal. No âmbito da investigação em que são apreendidos equipamentos ou meios tecnológicos que possam, no

seu interior, conter prova digital. Como é que isso é feito? Como é que se apreende um computador portátil? Como é que se apreende um *smartphone*? Como é que se faz uma busca electrónica num sistema informático? Isso são tudo matérias que estão lá contidas, sendo certo que para conseguirmos acautelar a parte técnica que obriga esta actividade, sugere-se que no planeamento dessa busca ou operação policial, se recorra a um perito informático para salvaguardar as questões técnicas dessa apreensão. Orientou-se o manual para procedimentos que devem ser considerados em sede de apreensão, sendo certo que a recolha posterior da prova digital será feita por quem tem competência técnica para o fazer. Importa sempre manter a integridade da prova que é recolhida, ou seja, a custódia da prova, para se garantir que, em toda a fase da investigação até ao julgamento, essa prova possa ser valorada, escrutinada, sujeita a contraditório e que foi aquela que foi apreendida. E isto deve ser assegurado em todo o momento, desde a sua apreensão até à sua valoração em sede de julgamento.

Existem ainda dois pontos que também nos parecem importantes de realçar.

Um tem a ver com o facto de nós não termos ficado somente pela difusão para implementação, quer do manual de boas práticas para recolha de prova digital, quer com o guia para recolha de cabeçalhos técnicos. Depois da difusão dessa matéria, todos os comandos enviaram dois representantes ao DIAP de Lisboa para receber formação nesta área. E esses dois representantes teriam que ter um perfil específico. Um tinha que ser da investigação criminal e o outro teria que ter conhecimentos aprofundados de informática. E isto para quê? Para que a difusão da documentação fosse acompanhada com formação específica na área. Assim, os dois representantes ficaram com a responsabilidade de replicar esta formação em cada um dos comandos, quer na vertente da investigação criminal, quer até na vertente territorial, no sentido de quem receber a queixa saber trabalhar ou saber recolher os cabeçalhos técnicos quando os crimes são praticados por correio electrónico. Esse é um aspecto que consideramos importante.

A outra questão tem a ver com os procedimentos técnicos que dizem respeito à recolha da prova digital. Aí, como já se disse, a nossa primeira preocupação é salvaguardar a integridade da prova digital, no momento da apreensão. Vamos imaginar uma questão de uma busca domiciliária em que se vê um computador portátil que pode conter prova digital. Há, logo ali, determinados procedimentos a ter em conta para se fazer a apreensão, que vão desde fotografar o ecrã que está ligado, à etiquetagem dos cabos, à questão da colocação de fita inviolável em todas as portas USB para não permitir que hajam discos rígidos externos a trabalhar ou a modificar a prova que lá está contida. Portanto, há aqui

uma série de procedimentos técnicos que são acautelados pelos procedimentos operacionais. Isto na questão da apreensão. No passo seguinte, na recolha da prova digital aí chamamos a particular atenção para a necessidade de, muitas vezes, recorrermos a um perito de informática. E isto porquê? Porque há necessidade de software específico e certificado para recolha da prova digital. Por exemplo, para fazer uma cópia de imagem ou obter uma "fotografia do conteúdo do computador". E é essa fotografia que depois serve como meio de investigação ao longo do processo, sendo certo que ao longo de todo o processo, incluindo a parte do julgamento, é possível o contraditório, ou seja, é possível o escrutínio da prova que foi logo ao início recolhida naquele computador. Se alguma dúvida houver, durante a fase de inquérito ou na fase de julgamento, a prova pode ser sempre questionada, pode ser sempre contraditada, pode ser sempre valorada tendo em conta esse escrutínio. Convém salvaguardar que a apreensão e a recolha da prova digital requerem uma parte técnica subjacente para serem devidamente asseguradas. E é importante termos a noção disto, pois muitas vezes poderemos criar aqui entraves à investigação ou poderemos estar na convicção de ter prova digital quando efectivamente ela não está salvaguardada na sua integridade.

4) Até que ponto considera a alínea *l)* do n.º 3 do artigo 7.º da LOIC (competência reservada da PJ para a investigação de crimes "informáticos e praticados com recurso a tecnologia informática"), como um entrave à recolha de prova digital, em particular o correio electrónico, por parte da PSP?

Esta questão já a colocámos por diversas vezes, quer ao MP, quer mesmo em reuniões de coordenação internas da PSP. Objectivamente, pergunta-se se da letra da LOIC resulta a interpretação de que todos os crimes em que, de alguma forma, seja utilizada tecnologia informática cabem na alçada da competência reservada da PJ. Isto inclui, por exemplo, uma injúria, inclui uma ameaça, pode incluir um crime de tráfico de droga. Portanto, pode incluir uma grande variedade de crimes que, na sua execução, podem recorrer à tecnologia informática. Por outro lado, temos os verdadeiros crimes informáticos. Um crime informático é um núcleo bastante mais restrito do que todos os crimes que possam recorrer à tecnologia informática. E tem havido alguma necessidade de tentar esclarecer o que é que cai na alçada da PJ e o que é que cai na alçada dos OPC de proximidade. Não havendo, a montante, um crime de competência reservada da PJ, a questão levanta-se com mais profundidade. Um crime de injúrias, à partida da competência

da PSP, se for praticado através do recurso informático, fica a dúvida se há ou não necessidade de passar essa investigação para a PJ. O DIAP de Lisboa, em sede de reunião de articulação com os OPC, entendeu que à PJ devem ser delegados os crimes cometidos através da informática, mas que tenham como atributo o uso ou ataque à tecnologia informática, através da sua manipulação, e não tanto como é o caso de um crime de ameaças, por exemplo, em que apenas se recorre à tecnologia informática. Ou seja, nestes casos a informática traduz-se numa mera plataforma não essencial como atributo da conduta criminosa, meramente instrumental, sendo que sem ela o crime poder-se-ia dar de outra forma. A título de exemplo, eu posso ter dois traficantes na rua a utilizar o *skype* ou o *e-mail* num computador portátil ou num *smartphone*, para procederem ao tráfico, e não é por causa disso que o crime passa para a PJ.

Nesta perspectiva, há a possibilidade de, ainda que hajam crimes cometidos com recurso a tecnologia informática, se isso for feito numa perspectiva meramente instrumental, essa investigação poderá ser delegada nos OPC de proximidade, se o crime não for de competência reservada.

Nós acompanhamos esta opinião uma vez que a investigação destes crimes, ainda que com recurso instrumental à informática, não requer especiais conhecimentos de informática e aproveita o «conhecimento de rua» dos OPC de proximidade.

Caso haja necessidade de recorrer, em termos técnicos, a peritos informáticos, tal se fará à semelhança do que se faz num crime de ofensas à integridade física, quando recorremos a um perito médico para o exame médico-legal.

Portanto há que salvaguardar a questão da prova digital, salvaguardando também a natureza dos OPC de proximidade e daquilo que podem acrescentar de mais-valia à própria actividade de investigação criminal.

ANEXO 7 – Manual de Boas Práticas para Recolha e Apreensão de Prova Digital – Departamento de Investigação Criminal da PSP

POLÍCIA DE SEGURANÇA PÚBLICA

DEPARTAMENTO DE INVESTIGAÇÃO CRIMINAL

MANUAL DE BOAS PRÁTICAS

Para recolha e apreensão de Prova Digital

VERSÃO 1

Dezembro de 2010

ÍNDICE

Índice	2
Histórico	3
Preâmbulo	4
Objectivo	5
Referências	6
Definições	7
Orientações Práticas	10
Responsável pela gestão do local do crime	10
Procedimentos operacionais	12
Preservação de provas	13
Computador Pessoal	13
Rede Doméstica/Computador Pessoal	15
Servidor de Rede / Rede de Trabalho	17
Meios Tecnológicos de Armazenamento de Dados	18
PDA (Assistentes pessoais digitais) /Telemóveis/GPS/Câmaras Digitais	19
Consentimento	21
Mandado de busca	21
Situações especiais	22
Elementos de uma rede doméstica	24
Vários exemplos de dispositivos	25

1. HISTÓRICO

A expressão «boas práticas», oriunda da gestão (do inglês *best practices*), designa os modos mais eficientes e mais eficazes de levar a cabo uma tarefa, segundo determinados procedimentos estabelecidos e comprovados ao longo do tempo por um grande número de pessoas.

O *Manual de Boas Práticas* constitui uma ferramenta que permite homogeneizar e normalizar procedimentos que, para além de garantirem a qualidade do serviço prestado, devem também permitir a uniformização de protocolos de actuação e a padronização de processos. Este manual pretende ser um instrumento de apoio aos elementos policiais na sua actividade diária, procurando responder mais facilmente às questões colocadas e simultaneamente levar ao empenho da instituição no estabelecimento de condições para a prestação de um serviço eficaz.

Tem-se como princípio que a prova rainha é a prova pericial.

2. PREÂMBULO

O presente manual foi preparado pelo Departamento de Investigação Criminal, com o objectivo principal de definir os procedimentos para apreensão de artigos ou objectos que sejam susceptíveis de conter prova digital, no âmbito de um inquérito crime, nomeadamente as normas para a recolha, transporte e preservação da prova digital.

Os procedimentos estabelecidos no presente manual são os que devem ser aplicados por parte dos investigadores criminais da PSP.

Os critérios estão redigidos tendo em vista, sobretudo, servirem como critérios gerais, abrangendo a preservação da prova na sua generalidade.

Este Manual contou com a colaboração do Departamento de Investigação e Acção Penal de Lisboa, visando uma uniformização de procedimentos.

Estes procedimentos só se aplicam quando for previsível a recolha de prova digital.

3. OBJECTIVO

A sociedade actual potencia a utilização de diversos dispositivos electrónicos e computadores. Os criminosos não são excepção, e procuram recorrer a uma variedade de *meios electrónicos* e *digitais* no intuito de facilitar a execução das suas actividades ilegais.

A tecnologia moderna permite aos suspeitos cometer crimes de âmbito internacional de forma remota, obter informações e fazer contra-informação mediante anonimato. A comunicação instantânea e o correio electrónico fornecem um espaço para comunicação entre os suspeitos, e destes últimos com as suas vítimas.

Ora, quaisquer *meios electrónicos* podem ser utilizados para cometer crimes, armazenar provas de crimes e fornecer informações sobre suspeitos e vítimas.

O presente Manual foi concebido para auxiliar o investigador a reconhecer os *meios electrónicos* como instrumentos passíveis de utilização em crimes ou como dispositivos de armazenamento de dados de crimes. Destina-se a ser utilizada pelos elementos da estrutura de Investigação Criminal, e visa orientar a actividade policial de modo a distinguir, com base nas apreensões, as diferentes situações que se apresentam. De igual forma, visa ainda ajudar a proteger correctamente a prova digital e assegurar a cadeia da prova, através do cumprimento dos procedimentos à recolha, transporte e preservação da mesma para o cumprimento de alguns procedimentos inerentes ao transporte de provas para exame forense (cadeia de prova). Visa também detectar a presença de possíveis complicações, adoptando critérios de exclusão, de forma a intervir eficazmente, aconselhando e acompanhando o procedimento através das medidas consideradas mais adequadas.

Não obstante o supracitado, recomendamos que o investigador consulte e procure assistência dos recursos disponíveis na Instituição ou de outros organismos. Isso deve incluir o Procurador titular do inquérito.

4. REFERÊNCIAS

- **Best Practices For Seizing Electronic Evidence** v.3
  A Pocket Guide for First Responders
  U.S. Department of Homeland Security
  United States Secret Service

- Lei n º 109/2009 de 15SET, Lei do Cibercrime

- Lei n.º 32/2008, de 17JUL, Lei da conservação de dados (...) de redes públicas de comunicações

- Portaria n.º 469/2009 de 6MAI, condições técnicas e de segurança em que se processa a comunicação electrónica para efeitos da transmissão de dados de tráfego e de localização

- Portaria n.º 915/2009 de 18AGO, período experimental de cerca de três meses no sentido de aprofundar e incrementar a funcionalidade e usabilidade da aplicação informática assim como permitir uma adaptação gradual dos profissionais a novos procedimentos de trabalho

5. DEFINIÇÕES

AGENDA PESSOAL OU ASSISTENTE PESSOAL DIGITAL (PDA): São máquinas de bolso, geralmente contendo telefones e listas de endereços, diários e outras informações.

BACKUP: Cópia dos dados/informações fora de um computador.

BOOT: Para carregar a primeira peça de software para começar um computador.

BIT: Unidade base dos sistemas digitais, com valor binário (zero ou um).

BYTE: Unidade de dados em geral, constituído por 8 bits.

Kilobytes (KB): um kilobyte tem 1024 bytes.

Megabyte (MB): Um Megabyte representa 1024 Kilobytes.

Gigabyte (GB): A Gigabyte corresponde a 1024 Megabytes.

CARTÕES DE MEIOS ELETRÓNICOS REMOVÍVEIS: Pequenos meios electrónicos de armazenamento de dados que são mais comummente encontrados em outros dispositivos digitais como câmaras fotográficas, PDAs e aparelhos de música digital (xD, SD, MMC, SMC, etc.)

CARTÃO DE REDE WIRELESS: Um cartão de expansão presente num computador que permite uma ligação sem fios entre o computador e outros dispositivos em uma rede. O cartão comunica por sinais de rádio para outros dispositivos presentes na rede.

CD-R (Compact Disc – Recordable): Disco compacto no qual os dados podem ser gravados, mas não apagados.

CD-RW (Compact Disc ReWritable): Disco compacto no qual os dados podem ser gravados e removidos/apagados.

CPU (Central Processing Unit): Unidade central de processamento. É o "cérebro" que realiza toda a aritmética, a lógica e funções de controlo.

DDOS (Denial of Service): Interrupção do serviço disponível. Um "assalto" a uma rede que a inunda com imensos pedidos adicionais, provocando um retardamento ou uma interrupção no tráfego regular.

DISCO RÍGIDO (HARD DISK): O disco rígido está normalmente dentro do PC. Armazena informações da mesma forma que as disquetes, mas pode reunir muito mais dados. Os discos rígidos mais populares são: IDE, SCSI e SATA.

DISPOSITIVOS DE ARMAZENAMENTO USB: Pequenos dispositivos de armazenamento que podem ser acedidos através de um computador. Armazenam grandes volumes de arquivos de dados. São facilmente removidos, transportados e ocultados.

DONGLE: Um dispositivo que conecta a um computador para controlar o acesso a um determinado pedido. *Dongles* são um dos meios mais eficazes de protecção dos direitos de autor.

DVD (DVD-RW): *Digital Versatile Disc*, ou disco de vídeo digital. Semelhante em aparência a um disco compacto, mas que pode armazenar grandes quantidades de dados (normalmente um mínimo de 4,7 GB de dados).

ENCRIPTAÇÃO: O processo de bloqueamento ou de codificação de informações no intuito de garantir que somente o destinatário pretendido possa ter acesso à leitura da informação.

FIREWALL: Um firewall permite ou bloqueia o tráfego de entrada e saída de uma rede privada ou usuários do computador. Um firewall é um método para manter os computadores protegidos contra intrusos.

GPS (Global Positioning System) : Sistema de Posicionamento Global

HARDWARE: A parte física de um computador (componentes).

ISP (Internet Service Provider): Fornecedor de serviços de Internet.

MALWARE: proveniente do inglês ***mal****icious soft****ware***; é um software destinado a se infiltrar em um sistema de computador alheio de forma ilícita, com o intuito de causar algum dano ou roubo de informações (confidenciais ou não).

MEIOS ELECTRÓNICOS REMOVÍVEIS: Disquetes, CDs, DVDs, cartuchos e fitas que armazenam dados que podem ser facilmente removidos.

MEMÓRIA: O local de armazenamento electrónico para instruções e para dados que um microprocessador de computador pode chegar rapidamente.

MODEM: Um dispositivo que liga um computador a uma linha de transmissão de dados.

MONITOR: Um dispositivo electrónico do computador que exibe e permite a visualização de informações.

RAM (Random Access Memory): Memória de curto prazo do computador que é perdida quando o computador é desligado.

SISTEMA OPERATIVO: Este software é normalmente carregado na memória do computador após ligar a máquina. É um pré-requisito para o funcionamento de qualquer outro software.

SOFTWARE PIRATA: Software que tenha sido copiado ilegalmente.

ROUTER: Um dispositivo de rede que encaminha informação de uma rede para outra.

WARDRIVING: Condução em torno de uma área com um computador portátil e de um adaptador de rede sem fios no intuito de localizar redes sem fios não seguras.

ZIP DRIVE / DISCO: Uma unidade de disco removível de 3,5 polegadas. A unidade vem com software que pode catalogar discos e bloquear arquivos por questões de segurança.

6. ORIENTAÇÕES PRÁTICAS

6.1 RESPONSÁVEL PELA GESTÃO DO LOCAL DO CRIME

A segurança e a rigorosa gestão do local do crime são fundamentais na investigação de qualquer ilícito criminal. Hoje em dia, uma grande parte dos crimes tem uma componente electrónica. Os computadores e outra tecnologia electrónica são facilitadores e, em alguns casos, motores da prática criminal, contendo uma série de provas relacionadas com o ilícito em investigação, seja um crime convencional ou um acto terrorista.

Os investigadores não devem ser complacentes com indivíduos suspeitos ou menosprezar os seus "ambientes de trabalho", simplesmente porque o crime pode envolver apenas um qualquer dispositivo electrónico (um computador, por exemplo).

Durante a investigação de crimes, ou aquando a apreensão de computadores e de outros artigos electrónicos, devemos estar cientes de que, como em qualquer outro crime, poderão ocorrer algumas mudanças inesperadas ou o envolvimento do sujeito.

Nesta senda, a utilização de procedimentos e de tácticas correctas visam garantir a segurança pessoal dos investigadores e demais intervenientes, bem como acautelar a segurança, preservação e recolha de prova do local com interesse investigatório ou do cenário de crime electrónico.

6.2 PROCEDIMENTOS OPERACIONAIS

Existem procedimentos operacionais gerais a respeitar aquando da abordagem de qualquer cenário de crime, sempre que computadores e/ou outro tipo de tecnologia electrónica[1] possam ser detectados no mesmo, que se passam a descrever:

- O responsável pela operação policial deve procurar, criar e manter as condições de segurança do local a buscar, de forma a permitir a recolha de prova.
- Se houver quaisquer factos que indiciem o envolvimento do *meio tecnológico* ao crime que está a ser investigado, importa acautelar o material necessário para a apreensão e a correcta recolha do suporte desse meio tecnológico.
- Não aceder aos arquivos do *meio tecnológico*.
    - Tratando-se, por exemplo, de um computador, importa mantê-lo desligado caso assim seja encontrado. Se, porventura, estiver ligado, importa seguir os procedimentos apropriados e referenciados no presente manual/guia quanto à forma correcta de o desligar e de o preparar para transporte como meio de prova.
- No caso de haver suspeitas que o *meio tecnológico* está a destruir provas é de todo conveniente desligá-lo imediatamente.
    - Se estivermos perante um computador ligado à corrente eléctrica, parar as aplicações que estejam a correr. Ter em atenção que o puxar do cabo de alimentação pode danificar dados; deve esta situação ser usada apenas em caso de urgência.
- Esteja o *meio tecnológico* ligado ou desligado, não deve ser esquecida a realização de reportagem fotográfica em plano geral e particular.
    - Quando um computador se encontra em funcionamento, deve haver a preocupação de fotografar o monitor.
    - Se o computador estiver desligado, convém fotografar o computador no seu todo, a sua localização e qualquer dispositivo electrónico anexo ao mesmo.
- Catalogar e identificar o meio tecnológico.
    - Esta acção é fundamental para garantir a custódia da prova e relacionar o meio com o acto e com o indivíduo.

[1] Os computadores e outro tipo de tecnologia electrónica serão adiante designados como ***"meios tecnológicos"***.

- Na definição dos quesitos para a Perícia /Exame forense deve ser indicado para cada dispositivo o que se procura (tipo de ficheiros, datas, assuntos, entre outros), em consonância com o objecto do processo. Esta informação incrementará a resposta adequada e célere dos peritos.

6.3 PRESERVAÇÃO DE PROVAS

Computador Pessoal

Para a preservação da prova propriamente dita, respeite os seguintes procedimentos de acordo com a ordem estabelecida.

1. **Se estiver ligado à rede (ligado ao *router* e ao *modem*), veja as instruções na página seguinte.**
2. Não mova ou utilize o computador, nem tente procurar quaisquer provas.
3. Fotografe toda a área circundante ao computador.
4. Fotografe a frente e a parte de trás do computador, bem como cabos e dispositivos ligados.
5. Se o computador estiver desligado, não ligue.
6. Se o computador estiver ligado e algo é exibido no monitor, fotografe o monitor.
7. Se o computador estiver ligado e o monitor está em branco, mova o "rato" ou pressione barra de espaço (irá mostrar a imagem activa no monitor). Após a imagem aparecer, fotografe o monitor.
8. Desligue o computador no menu iniciar  -> Encerrar.
    a. Em situações urgentes desligue o cabo de alimentação do computador.
    b. Em situação urgente e tratando-se de um computador portátil, localize e retire a bateria após remover o cabo de alimentação.
    c. A bateria é geralmente colocada ao fundo e na parte inferior do portátil.
    d. É frequente a existência de um botão ou de um interruptor que permite a remoção da bateria.

e. Depois de removida não deve ser recolocada no computador portátil (deve ser catalogada e relacionada com o visado e com o portátil).

f. A remoção da bateria impedirá o ligar acidental do computador portátil.

9. Faça um diagrama de cabos e etiquete-os para depois identificar os dispositivos ligados.
10. Desligue todos os cabos e dispositivos do computador.
11. Selar em local visível com autocolante de segurança todas as portas pelas quais é possível adulterar/apagar/acrescentar dados ao computador, deixando apenas de fora as entradas de rato, monitor e alimentação.
12. Empacote todos os componentes para transporte/armazenamento, tratando-os como carga frágil.
13. Mantenha todos os dispositivos de comunicação longe de ímanes, transmissores de rádio e outros elementos potencialmente prejudiciais.
14. Recolha o manual de instruções, documentação e apontamentos.
15. Documente todos os passos envolvidos na apreensão de um computador e seus componentes.
16. Consulte o responsável pelo inquérito sobre questões importantes da investigação.
17. **Catalogue o material apreendido: Apenso A, Apenso B, Apenso C.... e para cada Apenso:**

    a. Colocar etiqueta autocolante com a indicação "Apenso X" em local visível;

    b. No Auto de Busca e Apreensão:

        i. Identificar o apenso por marca + modelo + Numero de série + cor;

            1. Se não forem visíveis fazer descrição sumária e inequívoca do material

        ii. A quem foi apreendido;

        iii. Onde foi apreendido (designação de local (quarto, escritório, secretária de Funcionário Y) incluir fotos;

        iv. Descrever os componentes (cabos de alimentação e ligação, transformador, bolsa de transporte)

Rede Doméstica/Computador Pessoal

Para uma correcta preservação da prova, siga os seguintes procedimentos de acordo com a ordem estabelecida.

1. Desligue a energia do *router* ou do *modem*.
2. Não use o computador ou tente pesquisar eventuais provas.
3. Fotografe o computador de frente e os cabos que se encontram à volta, bem como todos os dispositivos ligados, sem alterar as posições iniciais. Fotografe igualmente a placa de identificação do computador e dos dispositivos digitais.
4. Fotografe a área circundante antes de mover qualquer prova.
5. Se o computador estiver desligado, não o ligue.
6. Se o computador estiver ligado e algo é exibido no monitor, fotografe o monitor.
7. Se o computador estiver ligado e o monitor está em branco, mova o "rato" ou pressione barra de espaço (irá mostrar a imagem activa no monitor). Após a imagem aparecer, fotografe o monitor.
8. Desligue o computador no menu iniciar  -> Encerrar.
    a. Em situações urgentes desligue o cabo de alimentação do computador.
    b. Em situação urgente e tratando-se de um computador portátil, localize e retire a bateria após remover o cabo de alimentação.

c. A bateria é geralmente colocada ao fundo e na parte inferior do portátil.

d. É frequente a existência de um botão ou de um interruptor que permite a remoção da bateria.

e. Depois de removida não deve ser recolocada no computador portátil.

f. A remoção da bateria impedirá o ligar acidental do computador portátil.

9. Faça um diagrama de cabos e etiquete-os para depois identificar os dispositivos.
10. Desligue todos os cabos e dispositivos do computador.
11. Selar em local visível com autocolante de segurança todas as portas pelas quais é possível adulterar/apagar/acrescentar dados ao computador, deixando apenas de fora as entradas de rato, monitor e alimentação.
12. Empacote todos os componentes (incluindo *router* e *modem*) e transporte/armazene os componentes como de carga frágil se tratasse.
13. Mantenha todos os dispositivos de comunicação longe de ímanes, transmissores de rádio e outros elementos potencialmente prejudiciais.
14. Recolha manual de instruções, documentação e apontamentos.
15. Documente todos os passos envolvidos na apreensão de um computador e seus componentes.
16. Consulte o responsável pelo inquérito sobre questões importantes da investigação.
17. **Catalogue o material apreendido: Apenso A, Apenso B, Apenso C.... e para cada Apenso:**

    a. Colocar etiqueta autocolante com a indicação "Apenso X" em local visível;

    b. No Auto de Busca e apreensão Indicar:

        i. Identificar o apenso por marca + modelo + Numero de série + cor;

            1. Se não forem visíveis fazer descrição sumária e inequívoca do material

        ii. A quem foi apreendido;

        iii. Onde foi apreendido (designação de local (quarto, escritório, secretária de Funcionário Y) incluir fotos;

        iv. Descrever os componentes (cabos de alimentação e ligação, transformador, bolsa de transporte)

Servidor de Rede / Rede de Trabalho

1. Consulte e solicite apoio técnico de um especialista em informática (perito informático).
2. Garanta a segurança do local e não deixe que alguém toque nos *meios tecnológicos*, excepto pessoal preparado para lidar com sistemas de rede.
3. Estas situações devem ser planeadas e coordenadas com um perito/ especialista.

ATENÇÃO:

- **Tem sido recomendado o procedimento para desligar as fontes de alimentação de vário equipamento tecnológico. Porém, nesta situação, não é permitido desligar a fonte de alimentação do servidor sob pena de:**
  a. **Provocar graves danos no sistema**
  b. **Interromper o normal funcionamento do sistema**
  c. **Causar danos, o que poderá acarretar responsabilidade civil.**

Meios Tecnológicos de Armazenamento de Dados

Os *meios tecnológicos* de armazenamento são usados para recolher/guardar dados de dispositivos electrónicos, podendo variar consoante a sua capacidade de memória.

- Recolha o manual de instruções, documentação e apontamentos
- Mantenha todos os dispositivos de comunicação longe de ímanes, transmissores de rádio e outros elementos potencialmente prejudiciais.
- Documente todos os passos envolvidos na apreensão dos *meios tecnológicos* de armazenamento e seus componentes.
- Selar em local visível com autocolante de segurança todas as portas pelas quais é possível adulterar/apagar/acrescentar dados ao computador, deixando apenas de fora as entradas de rato, monitor e alimentação.
- **Catalogue o material apreendido: Apenso A, Apenso B, Apenso C…. e para cada Apenso.**

Os cabos de alimentação/ligação e transformadores devem acompanhar o material

PDA (Assistentes pessoais digitais) /Telemóveis/GPS/Câmaras Digitais

PDA (assistentes pessoais digitais), Telemóveis e Câmaras Digitais podem armazenar dados directamente na memória interna ou podem conter memória removível.

Para uma correcta preservação da prova e recolha/apreensão destes *meios tecnológicos* e dispositivos removíveis associados, siga os seguintes procedimentos de acordo com a ordem estabelecida:

1. Se o dispositivo estiver desligado, não o ligue.
2. Quando se deparar com PDA's ou Telemóveis ligados, não os desligue.
    a. Desligar estes *meios tecnológicos* pode originar a perda da respectiva senha (password) e consequentemente impedir o acesso às provas neles existentes.
3. Fotografe o *meio tecnológico* e o respectivo monitor (se disponível).
4. Procure etiquetar e recolher todos os cabos (incluindo os de fornecimento de energia) e transporte-os juntamente com o *meio tecnológico*.
5. Mantenha a bateria do *meio tecnológico* devidamente carregada.
6. Se o *meio tecnológico* não puder ser mantido com carga, a análise/exame pericial por parte de um especialista deve ser concluído antes de a bateria descarregar (ou dos dados podem ser perdidos).
7. Etiquete os dispositivos de armazenamento adicionais (cartões de memória, *pen drive*, entre outros).
8. Documente todos os passos envolvidos na apreensão dos *meios tecnológicos* e seus componentes.

9. **Catalogue o material apreendido: Apenso A, Apenso B, Apenso C…. e para cada Apenso.**

CONSENTIMENTO

Quando obtido o consentimento, garanta que o documento tem linguagem específica tanto para a apreensão como para futuros exames forenses do hardware do computador, do software, de meios/dispositivos electrónicos e de dados a realizar por parte de examinadores/peritos forenses ou analistas.

Se o seu serviço tem um formulário de consentimento exclusivo para computador ou meios/dispositivos electrónicos e a análise é realizada por um examinador/perito forense de computadores, deve pois utilizá-lo.

Se não tem um formulário e tem de elaborar um termo de consentimento, procure consultar o Procurador titular do inquérito no intuito de obter recomendações sobre a linguagem adequada e a documentação a aplicar.

MANDADO DE BUSCA

Os Mandados de Busca permitem a busca e a apreensão de provas electrónicas predefinidas no âmbito do mandado. Este método é o preferido e é sucessivamente executado com o mínimo de resistência, tanto no local a buscar como em Tribunal.

Os Mandados de Busca para dispositivos de armazenamento electrónico concentram-se geralmente em duas fontes principais de informação:

Mandados de Busca para Dispositivos Electrónicos de Armazenamento

- Busca e apreensão de hardware, software, documentação, anotações de usuários e meios de armazenamento.
- Exame / pesquisa e apreensão de dados – no sentido de salvaguardar a custódia da prova, esta operação de exame/pesquisa e apreensão de dados devem ser realizadas por perito informático. Inexistindo perito informático no local proceder à apreensão, elaboração de expediente (ex: fotografia) e selagem dos meios tecnológicos.

Mandados de Busca para prestadores de serviços

- Registos de serviço, registos de facturação, informação sobre assinantes, etc.
- Obter informação de identificação para fins de investigação adicional.

Finalidade do computador

- O relatório deve indicar qual é o papel do computador no ilícito criminal e porque é que contém elementos de prova.

Nexo de causalidade

- Estabelecer porque é que se espera encontrar provas digitais no local de busca.

Especificar as provas procuradas

- Descrever especificamente as provas que têm uma causa provável para pesquisar e qualquer evidência de apropriação do computador.

Linguagem Pré-definida

- Adapte toda a linguagem de busca para os factos específicos do seu caso. Evite o uso de textos pré-definidos.

Não Divulgação

- Pode ser necessário proteger a integridade da investigação, proteger informadores ou impedir a divulgação de segredos comerciais / de propriedade intelectual.

SITUAÇÕES ESPECIAIS

- Considerações jurídicas especiais envolvendo médicos, advogados, cônjuges, editores, clero, etc. (Nestas situações deve ser indicado especificamente pelo JIC o que deve ser recolhido e presenciado pelo representante da Ordem profissional)

O texto adiante apresentado é uma directriz geral de referência para formulários de consentimento relativos a computadores e a meio electrónicos. Solicite o auxílio do Ministério Público (Procurador titular do Inquérito) quanto à linguagem jurídica aplicável.

DECLARAÇÃO

Eu, _____, nascido em __/__/____, declaro autorizar agentes da P.S.P., afectos à Divisão de Investigação Policial do Comando _____ e qualquer outra pessoa (s), incluindo um examinador/perito forense de computadores, para prestar assistência, remover, tomar posse e / ou realizar uma busca completa do seguinte: Sistema Operativo, Aplicações e Sistema de Ficheiros de Dados, dispositivos de armazenamento de dados, disquetes de armazenamento de dados de computador, CD/DVD ou qualquer outro equipamento electrónico capaz de armazenar, recuperar, tratar e/ou aceder a dados.

Os dados constantes do equipamento acima mencionado estão sujeitos a clonagem para imagem forense, para posterior análise de todos os dados pertinentes relativos ao incidente / investigação criminal.

Declaro conceder autorização para pesquisa livre e voluntária sem medo, coacção, ameaça ou promessas de qualquer tipo, com pleno conhecimento do meu direito constitucional de recusar a dar o meu consentimento para a remoção e/ou pesquisa no equipamento supracitado / de dados, que renuncio por este meio

Este consentimento de pesquisa é dado por mim no presente dia _____ de _____, 20_____, às _____ H _____.

Localização itens retirados: _____

Assinatura do Autorizante: _____

Assinatura da Testemunha: _____

Assinatura da Testemunha: _____

6.4 ELEMENTOS DE UMA REDE DOMÉSTICA

Tal como demonstrado no esquema acima projectado, uma rede doméstica é geralmente composta por *modem*, *router* e computador desktop ou computador portátil.

O objectivo típico de uma rede doméstica é permitir que vários computadores possam compartilhar uma única ligação à Internet, como *ADSL*, *Cabo* ou *DIAL-UP*. A rede doméstica também admite que os múltiplos utilizadores compartilhem informações com outros computadores na rede.

Quando nos confrontamos com uma rede doméstica, é imperioso desactivar a conexão de rede para a Internet. Isto é conseguido mediante a desconexão da fonte de alimentação do *modem* e/ou do *router*. (deve ser indicado no Auto a data hora a que foi desligado)

Em muitos casos, as redes domésticas estão ligadas através de *routers* sem fio ou sem pontos de acesso, que podem ser facilmente escondidos.

Cada vez mais, as redes domésticas servem também como pequenos escritórios ou empresas. Ao detectar este tipo de redes "caseiras", é de todo conveniente contactar ou fazer-se acompanhar de um técnico/perito para auxiliar no processo de preservação da possível prova digital e apreensão do computador e restantes *meios tecnológicos*.

VÁRIOS EXEMPLOS DE DISPOSITIVOS


SAMSUNG
Yellowpages
Address Book
Games & Apps
Settings
AT&T GPS
Messaging
Media Net
Tools
AT&T Music
CV
Media Mall
My Stuff


Canon


• 6 Pager Cap Codes
• 8 Line Display
• Synthesized Frequency
• Zooms to 4 line
• Windows Programmable
• Store up to 60 messages
• Priority Override
• Up to 700hrs Battery Life
CommtechWireless


PHILIPS
DOUBLE LAYER


HD DVD
30GB
Dual Layer
TOSHIBA


Blu-ray Disc


HD DVD


zip
100


LINKSYS


iPod
Music
Photos
Videos
Extras
Settings
Shuffle Songs
Now Playing
6 of 15
Feel Good, Inc.
Gorillaz
Demon Days
3:41
-1:20
MENU


LACIE

ANEXO 8 – Guia para Recolha e Interpretação dos Cabeçalhos Técnicos dos *E-mails* - DIAP de Lisboa

S. R.
MINISTÉRIO PÚBLICO
DISTRITO JUDICIAL DE LISBOA
DEPARTAMENTO DE INVESTIGAÇÃO E ACÇÃO PENAL

Sempre que for denunciado um crime em que tenha sido utilizado o correio electrónico como via para a prática do mesmo existem três passos a dar para se chegar à identificação do indivíduo que enviou a mensagem:

1.º - Recolha dos cabeçalhos técnicos da mensagem de correio electrónico

Para se poder identificar o IP do remetente da mensagem é necessário que o destinatário da mesma forneça os cabeçalhos técnicos.

Estes cabeçalhos técnicos permitem fazer o percurso da mensagem desde a sua origem até ao seu destino, por isso tem de ser o destinatário da mensagem, a vítima, a retirar da sua máquina ou de um terceiro esta informação não podendo a mesma ser reencaminhada.

Consoante o webmail utilizado assim se procede à recolha dos cabeçalhos técnicos.

Para Microsoft Outlook:

1. Abrir a mensagem (duplo *click* sobre a mesma).
2. Na opção de menu "Ver *(View)"* seleccionar "Opções (Options)".
3. Na janela que abriu (conforme Imagem 1), na caixa "Cabeçalhos de Internet *(Internet headers)" clicar* com botão direito do rato, seleccionar "Seleccionar tudo *(Select All)",* depois *clicar* novamente com o botão direito do rato e seleccionar "Copiar *(Copy)".*

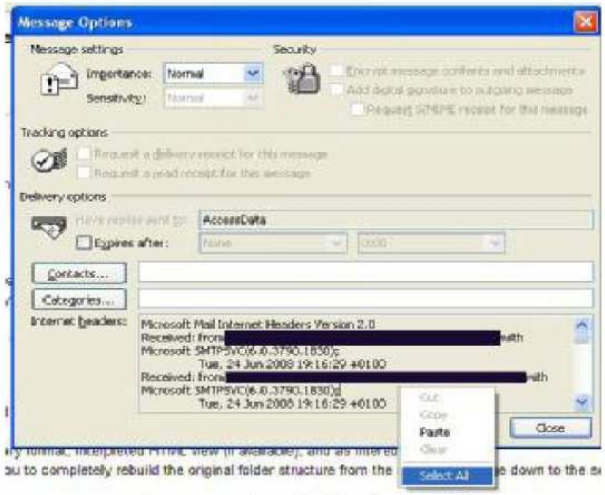


Imagem 1 - Outlook

4. Abrir um documento novo no Word e realizar Colar *(Paste)* através da Opção de Menu "*Edit/Paste"* ou botão direito do rato e *"Paste".*

Para Microsoft Outlook Express:

1. Existem pelo menos duas formas de aceder aos cabeçalhos das mensagens. Se a mensagem for aberta, a partir do menu *"File"* acede-se à opção *"Properties"* ou então ao *clicar* com o botão direito do rato em cima da mesma e seleccionar *"Propertied"* conforme Imagem 2.

S. R.

MINISTÉRIO PÚBLICO
DISTRITO JUDICIAL DE LISBOA
DEPARTAMENTO DE INVESTIGAÇÃO E ACÇÃO PENAL

Imagem 2 – Outlook Express

2. Depois visualiza-se o conteúdo da Imagem 3.

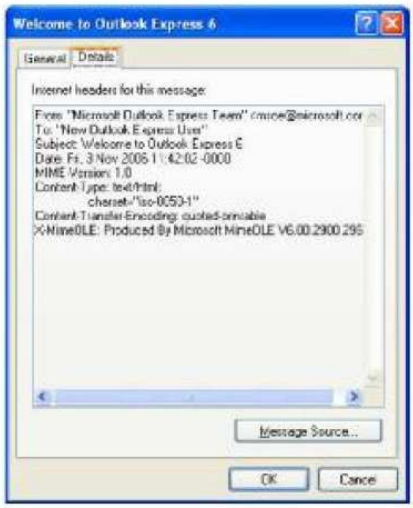


Imagem 3 - Detalhes das propriedades do Outlook Express

3. No tabulador *"Details" clicar* com botão direito do rato, seleccionar "Seleccionar tudo *(Select All)*", depois *clicar* novamente com o botão direito do rato e seleccionar "Copiar *(Copy)".*
4. Abrir um documento novo no Word e realizar Colar *(Paste)* através da Opção de Menu *"Edit/Paste"* ou botão direito do rato, opção *"Paste".*

Para Hotmail (versão Live):

1. Em cima da mensagem *clicar* botão direito e seleccionar a opção *"View source",* conforme Imagem 4.

S. R.

MINISTÉRIO PÚBLICO
DISTRITO JUDICIAL DE LISBOA
DEPARTAMENTO DE INVESTIGAÇÃO E ACÇÃO PENAL

Imagem 4 – Hotmail Live

2. Vai ser aberta automaticamente uma nova janela do *browser.*
3. Seleccionar tudo (Crtl + A)
4. Copiar (Ctrl + C)
5. Abrir um documento novo no Word e realizar Colar (Ctrl + V).

Para Hotmail (versão Clássica):

1. Seleccionar o menu "Options", posteriormente a opção *"Preferences".* Encontrar a opção *"Headers"* e seleccionar a opção *"Advanced headers".*
2. Guardar as alterações
3. Voltar à mensagem. Já se encontram visíveis os cabeçalhos técnicos.

Para Sapo (novo Webmail Beta):

1. Em cima da mensagem fazer duplo *click.*
2. Vai ser aberta uma nova janela com a mensagem, conforme Imagem 5.

Imagem 5 – Sapo Webmail Beta

3. Seleccionar a opção "CÓDIGO-FONTE DA MENSAGEM".
4. Vai ser aberta automaticamente uma nova janela do *browser.*
5. Seleccionar tudo (Crtl + A)
6. Copiar (Ctrl + C)
7. Abrir um documento novo no Word e realizar Colar (Ctrl + V).

S. R.

MINISTÉRIO PÚBLICO
DISTRITO JUDICIAL DE LISBOA
DEPARTAMENTO DE INVESTIGAÇÃO E ACÇÃO PENAL

Para Sapo (Webmail):

Existe outra forma de exibir os cabeçalhos, mas por problemas relacionados com a impressão das mensagens, deve ser utilizada esta opção.

1. Abrir a mensagem.
2. Seleccionar a opção "Código-fonte da Mensagem", conforme Imagem 6.
3. Vai ser aberta automaticamente uma nova janela do *browser.*
4. Seleccionar tudo (Crtl + A)
5. Copiar (Ctrl + C)
6. Abrir um documento novo no Word e realizar Colar (Ctrl + V).

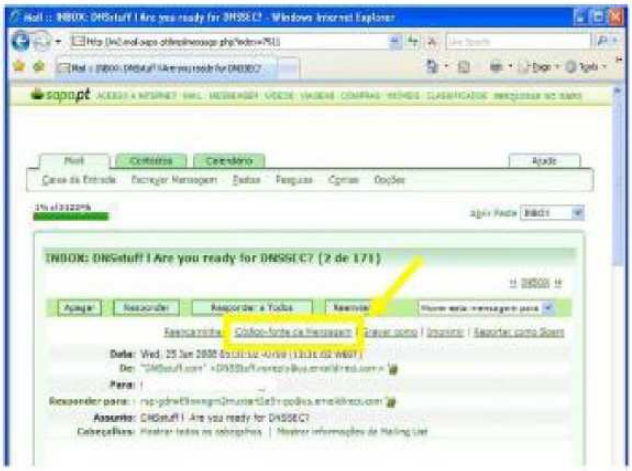


Imagem 6 – Sapo Webmail

Para Gmail:

1. Seleccionar o menu ao *clicar* na  posteriormente a opção *"Show Original",* conforme Imagem 7.
2. Vai ser aberta automaticamente uma nova janela do *browser.*
3. Seleccionar tudo (Crtl + A)
4. Copiar (Ctrl + C)
5. Abrir um documento novo no Word e realizar Colar (Ctrl + V).

Imagem 7 -

S. R.

MINISTÉRIO PÚBLICO
DISTRITO JUDICIAL DE LISBOA
DEPARTAMENTO DE INVESTIGAÇÃO E ACÇÃO PENAL

No Yahoo! Mail (Nova versão) :

1. Em cima da mensagem *clicar* botão direito e seleccionar a opção *"View full headers"*, conforme Imagem 8.

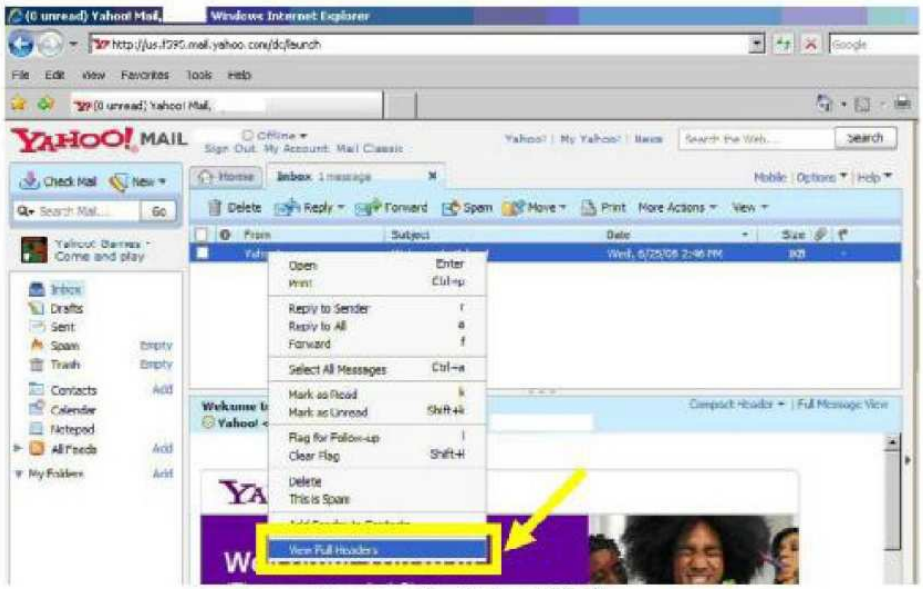


Imagem 8 – Yahoo! Mail

2. Vai abrir uma nova janela, conforme Imagem 9.
3. *Clicar* com botão direito do rato, seleccionar "Seleccionar tudo *(Select Ali)"*, depois *clicar* novamente com o botão direito do rato e seleccionar "Copiar *(Copy)"*.
4. Abrir um documento novo no Word e realizar Colar *(Paste)* através da Opção de Menu *"Edit/Paste"* ou botão direito do rato, opção *"Paste"*.

Imagem 9 - Cabeçalhos do Yahoo! Mail

No Yahoo (antigo):

1. Seleccionar o menu *"Options"*, posteriormente a opção *"Mail Preferences"*. Na opção *"Mail Viewing Preferences"*, na parte dos *"Message Headers"* seleccionar a opção "All".

S. R.

MINISTÉRIO PÚBLICO
DISTRITO JUDICIAL DE LISBOA
DEPARTAMENTO DE INVESTIGAÇÃO E ACÇÃO PENAL

No Clix:

1. *Clicar* na opção  conforme Imagem 10.

Imagem 10 – Seleccionar visualização dos cabeçalhos do Clix

2. Vai ser aberta automaticamente uma nova janela do *browser,* conforme Imagem 11.
3. Seleccionar tudo (Crtl + A)
4. Copiar (Ctrl + C)
5. Abrir um documento novo no Word e realizar Colar (Ctrl + V)

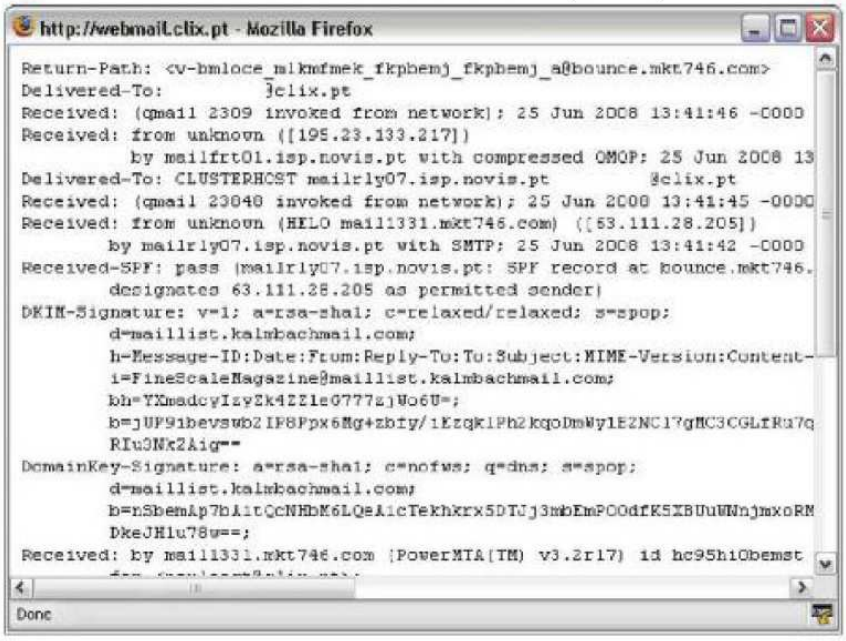


Imagem 11 - Cabeçalhos do Clix

S. R.

MINISTÉRIO PÚBLICO
DISTRITO JUDICIAL DE LISBOA
DEPARTAMENTO DE INVESTIGAÇÃO E ACÇÃO PENAL

2.º - Leitura dos cabeçalhos técnicos da mensagem

A leitura dos cabeçalhos técnicos é sempre feita de baixo para cima.

Desta leitura poderá resultar a recolha de vários elementos, nomeadamente:

a) Endereço IP do computador que se ligou ao *webmail* que enviou a mensagem;

b) Endereço de correio electrónico do remetente;

c) Data, hora e fuso horário da mensagem;

d) Identificação da mensagem (*Message ID*);

e) Campos "*received*" referentes aos diversos servidores por onde a mensagem circulou;

f) Endereço de correio electrónico do destinatário.

A título de exemplo:

```
Delivered-To: matosss@gmail.com
Received: by 10.223.120.3 with SMTP id b3cs221153far;
        Thu, 18 Mar 2010 07:54:14 -0700 (PDT)
Received: by 10.204.4.89 with SMTP id 25mr2654129bkq.19.1268924053105;
        Thu, 18 Mar 2010 07:54:13 -0700 (PDT)
Return-Path: <maria@sapo.pt>
Received: from relay2.ptmail.sapo.pt (relay1.ptmail.sapo.pt
[212.55.154.21])
        by mx.google.com with SMTP id
f15si111637bka.2.2010.03.18.07.54.11;
        Thu, 18 Mar 2010 07:54:13 -0700 (PDT)
Received-SPF: pass (google.com: domain of maria@sapo.pt designates
212.55.154.21 as permitted sender) client-ip=212.55.154.21;
Authentication-Results: mx.google.com; spf=pass (google.com: domain of
maria@sapo.pt designates 212.55.154.21 as permitted sender)
smtp.mail=maria@sapo.pt
Received: (qmail 27398 invoked from network); 18 Mar 2010 14:54:11 -
0000
Received: from unknown (HELO php02) (10.134.37.51)
  by relay1 with SMTP; 18 Mar 2010 14:54:11 -0000
Received: (qmail 15250 invoked by uid 64140); 18 Mar 2010 14:54:11 -
0000
Received: from bl10-81-125.dsl.telepac.pt (bl10-81-125.dsl.telepac.pt
        [85.243.81.125]) by w0.mail.sapo.pt (Horde Framework) with
HTTP; Thu, 18
        Mar 2010 14:54:11 +0000
Message-ID: 20100318145411.14293dp95mn8qheb@w0.mail.sapo.pt
Date: Thu, 18 Mar 2010 14:54:11 +0000
From: maria@sapo.pt
To: elis m <matosss@gmail.com>
Subject: Re: =?iso-8859-15?b?bW9u82xvZ29zLi4u?=
References:
<1d3a92a71003171640x70614720n2da84a5d6c9d7388@mail.gmail.com>
In-Reply-To:
<1d3a92a71003171640x70614720n2da84a5d6c9d7388@mail.gmail.com>
MIME-Version: 1.0
Content-Type: multipart/alternative;
        boundary="=_3d804gyg19jn"
Content-Transfer-Encoding: 7bit
User-Agent: Dynamic Internet Messaging Program (DIMP) 3.3.1
X-Originating-IP: 85.243.81.125
X-PTMail-Version: 3.3.1
```

S. R.

MINISTÉRIO PÚBLICO
DISTRITO JUDICIAL DE LISBOA
DEPARTAMENTO DE INVESTIGAÇÃO E ACÇÃO PENAL

```
This message is in MIME format.

--=_3d804gyg19jn
Content-Type: text/plain;
        charset=ISO-8859-15
Content-Description: =?iso-8859-15?b?VmVyc+Nv?= da mensagem em texto
        simples
Content-Disposition: inline
Content-Transfer-Encoding: quoted-printable
```

Mensagem remetida através do computador com o IP 85.243.81.125 utilizando o endereço de correio electrónico maria@sapo.pt no dia 18 de Março de 2010 às 14:54:11 horas no fuso horário GMT +0000 e cujo destinatário é o endereço de correio electrónico matosss@gmail.com.

Importa, pois, identificar o utilizador que efectuou a comunicação de dados através do IP identificado.

3.º - Identificação do endereço IP por consulta ao ISP (Internet Service Provider)

Para identificar o ISP que atribuiu o endereço IP e fornecer informação sobre o utilizador que expediu a mensagem será necessário aceder a http://whois.domaintools.com

Mediante a informação obtida oficiar à entidade respectiva fornecendo sempre os seguintes elementos:

IP	Data / Hora dd,mm,yy / hh,mm,ss	Fuso horário
85.243.81.125	18 Mar 2010 / 14:54:11	GMT +0000

Quando da leitura dos cabeçalhos técnicos não é possível identificar o IP remetente

Nestes casos é necessário identificar o domínio do endereço de correio electrónico, ou seja, o que surge após "@", devendo socorrer-nos do site acima referido para identificar o ISP responsável.

Quando se trate de um ISP não nacional (v.g. Gmail, Hotmail, hi5) os pedidos deverão ser feitos também em inglês, conforme exemplos que seguem.

Nota:

Os pedidos para GOOGLE podem ser efectuado via e-mail, devendo neste caso ser anexado em formato pdf os cabeçalhos técnicos bem como o próprio pedido.

Os pedidos para a MICROSOFT devem ser endereçados em envelope dirigido à Dra. Paula Martinho da Silva, Avenida da Liberdade, n.º 224 – 1250-148 Lisboa que se encarregará de os fazer chegar à Microsoft Corporation.

S. R.

MINISTÉRIO PÚBLICO
DISTRITO JUDICIAL DE LISBOA
DEPARTAMENTO DE INVESTIGAÇÃO E ACÇÃO PENAL

Hi5 Networks, Inc
55 Second Street, Suite 400
San Francisco
CA 94105 - US

Fax: 4159790327

N/ Referência:

Inquérito n.º	ª Secção	Ofício n.º Data:

A fim de instruir o processo-crime 249/10.8JDLSB, cuja investigação corre no DIAP de Lisboa, relativamente à prática de um crime de devassa da vida privada, praticado através de correio electrónico, solicita-se a v/ colaboração no sentido de prestarem informações relativas a:

1. Registos de IPs, grupo data/hora e fuso horário da criação da conta (identificação da conta) http://hi5.com/friend/p508433136--liliana--html e perfil associado.
2. Registos de IPs, grupo data/hora e fuso horário da actualização da conta (identificação a conta) http://hi5.com/friend/p508433136--liliana--html
3. Contas de mail secundárias registadas e associadas com estes endereços.
4. Total remoção ou suspensão da conta (se for caso disso) (identificação da conta) http://hi5.com/friend/p508433136--liliana--html

A informação pretendida é essencial para a recolha da prova para se poder incriminar o suspeito pela prática do referido crime, sendo essencial obter os elementos que a Hi5 Networks, Inc possui relativamente à identificação da pessoa que criou tais contas.

(Descrição sumária dos factos) O processo é respeitante a um suspeito cuja actividade delituosa se investiga neste processo criou esta conta onde se faz passar pela vítima para manter contactos de cariz sexual com terceiros, revelando assim factos da sua vida sexual, o que faz contra a vontade daquela.

To instruct criminal proceedings 249/10.8JDLSB, whose investigation runs on Lisbon DIAP, relatively to a crime of inquest of privacy, done by e-mail, requests your collaboration to give information about:
1. Any records of IP addresses, group, date/time and timezone on account creation of http://hi5.com/friend/p508433136--liliana--html and profile associated.
2. Any records of IP addresses, group, date/time and timezone on account updates of http://hi5.com/friend/p508433136--liliana--html and profile associated.
3. Any alternative mail accounts registered and associated with those registries.
4. Total removal or suspension of http://hi5.com/friend/p508433136--liliana--html

S. R.

MINISTÉRIO PÚBLICO
DISTRITO JUDICIAL DE LISBOA
DEPARTAMENTO DE INVESTIGAÇÃO E ACÇÃO PENAL

The requested information it's very important to collection of evidence to incriminate the suspect from practicing that crime, it's of the most importance to obtain all data Hi5 Networks, Inc has concerning the identification of the person who created those site.

A suspect that is under investigation on thin process created several accounts and has threatened to disclose and reveal to others the victim sexual intimacy photos. He has already revealed one of those photos, moreover, using these account he created, impersonates the victim to keep sexual contacts with others, revealing facts from victims personal and sexual life against his will.

Com os melhores cumprimentos | Yours Sincerely
O Magistrado do Ministério Público | Public Prosecuter

_____

Lic.

S. R.

MINISTÉRIO PÚBLICO
DISTRITO JUDICIAL DE LISBOA
DEPARTAMENTO DE INVESTIGAÇÃO E ACÇÃO PENAL

Google Inc.
1600 Amphitheatre Parkway
Mountain View
CA 94043 - US

Fax: 16504690622
Email: lis-global@google.com

N/ Referência:

Inquérito n.º	ª Secção	Ofício n.º Data:

A fim de instruir o processo-crime 249/10.8JDLSB, cuja investigação corre no DIAP de Lisboa, relativamente à prática de um crime de devassa da vida privada, praticado através de correio electrónico, solicita-se a v/ colaboração no sentido de prestarem informações relativas a:

1. Registos de IPs, grupo data/hora e fuso horário da criação da conta (identificação da conta) liliana-cecilia@gmail.com e perfil associado
2. Registos de IPs, grupo data/hora e fuso horário da actualização da conta (identificação a conta) liliana-cecilia@gmail.com
3. Contas de mail secundárias registadas e associadas com estes endereços.
4. Total remoção ou suspensão da conta (se for caso disso) (identificação da conta) liliana-cecilia@gmail.com

A informação pretendida é essencial para a recolha da prova para se poder incriminar o suspeito pela prática do referido crime, sendo essencial obter os elementos que a Google Inc. possui relativamente à identificação da pessoa que criou tais contas.

(Descrição sumária dos factos) O processo é respeitante a um suspeito cuja actividade delituosa se investiga neste processo criou esta conta onde se faz passar pela vítima para manter contactos de cariz sexual com terceiros, revelando assim factos da sua vida sexual, o que faz contra a vontade daquela.

To instruct criminal proceedings 249/10.8JDLSB, whose investigation runs on Lisbon DIAP, relatively to a crime of inquest of privacy, done by e-mail, requests your collaboration to give information about:

1. Any records of IP addresses, group, date/time and timezone on account creation of liliana-cecilia@gmail.com and profile associated.
2. Any records of IP addresses, group, date/time and timezone on account updates of liliana-cecilia@gmail.com and profile associated.
3. Any alternative mail accounts registered and associated with those registries.
4. Total removal or suspension of liliana-cecilia@gmail.com

S. R.

MINISTÉRIO PÚBLICO
DISTRITO JUDICIAL DE LISBOA
DEPARTAMENTO DE INVESTIGAÇÃO E ACÇÃO PENAL

The requested information it's very important to collection of evidence to incriminate the suspect from practicing that crime, it's of the most importance to obtain all data Google Inc. has concerning the identification of the person who created those site.

A suspect that is under investigation on thin process created several accounts and has threatened to disclose and reveal to others the victim sexual intimacy photos. He has already revealed one of those photos, moreover, using these account he created, impersonates the victim to keep sexual contacts with others, revealing facts from victims personal and sexual life against his will.

Com os melhores cumprimentos | Yours Sincerely
O Magistrado do Ministério Público | Public Prosecuter

_____

Lic.

S. R.

MINISTÉRIO PÚBLICO
DISTRITO JUDICIAL DE LISBOA
DEPARTAMENTO DE INVESTIGAÇÃO E ACÇÃO PENAL

Microsoft Corporation
One Microsoft Way
Redmond
WA 98052-6399
US

N/ Referência:

Inquérito n.º	ª Secção	Ofício n.º Data:

A fim de instruir o processo-crime 249/10.8JDLSB, cuja investigação corre no DIAP de Lisboa, relativamente à prática de um crime de devassa da vida privada, praticado através de correio electrónico, solicita-se a v/ colaboração no sentido de prestarem informações relativas a:

1. Registos de IPs, grupo data/hora e fuso horário da criação da conta (identificação da conta) liliana-cecilia@hotmail.com e perfil associado
2. Registos de IPs, grupo data/hora e fuso horário da actualização da conta (identificação a conta) liliana-cecilia@hotmail.com
3. Contas de mail secundárias registadas e associadas com estes endereços.
4. Total remoção ou suspensão da conta (se for caso disso) (identificação da conta) liliana-cecilia@hotmail.com

A informação pretendida é essencial para a recolha da prova para se poder incriminar o suspeito pela prática do referido crime, sendo essencial obter os elementos que a Microsoft possui relativamente à identificação da pessoa que criou tais contas.

(Descrição sumária dos factos) O processo é respeitante a um suspeito cuja actividade delituosa se investiga neste processo criou esta conta onde se faz passar pela vítima para manter contactos de cariz sexual com terceiros, revelando assim factos da sua vida sexual, o que faz contra a vontade daquela.

To instruct criminal proceedings 249/10.8JDLSB, whose investigation runs on Lisbon DIAP, relatively to a crime of inquest of privacy, done by e-mail, requests your collaboration to give information about:

1. Any records of IP addresses, group, date/time and timezone on account creation of liliana-cecilia@hotmail.com and profile associated.
2. Any records of IP addresses, group, date/time and timezone on account updates of liliana-cecilia@hotmail.com and profile associated.
3. Any alternative mail accounts registered and associated with those registries.
4. Total removal or suspension of liliana-cecilia@hotmail.com

S. R.

MINISTÉRIO PÚBLICO
DISTRITO JUDICIAL DE LISBOA
DEPARTAMENTO DE INVESTIGAÇÃO E ACÇÃO PENAL

The requested information it's very important to collection of evidence to incriminate the suspect from practicing that crime, it's of the most importance to obtain all data Google Inc. has concerning the identification of the person who created those site.

A suspect that is under investigation on thin process created several accounts and has threatened to disclose and reveal to others the victim sexual intimacy photos. He has already revealed one of those photos, moreover, using these account he created, impersonates the victim to keep sexual contacts with others, revealing facts from victims personal and sexual life against his will.

Com os melhores cumprimentos | Yours Sincerely

O Magistrado do Ministério Público | Public Prosecuter

_____

Lic.