UNIVERSIDADE D
COIMBRA

Maria Inês de Almeida Vilar Matias

APREENSÃO DE CORREIO ELETRÓNICO E REGISTOS DE COMUNICAÇÕES DE NATUREZA SEMELHANTE

Dissertação no âmbito do Mestrado em Ciências Jurídico-Forenses orientada pela Professora Doutora Sónia Mariza Florêncio Fidalgo e apresentada à Faculdade de Direito da Universidade de Coimbra

Outubro de 2020

Maria Inês de Almeida Vilar Matias

A apreensão de correio eletrónico e registos de comunicações de natureza semelhante

The seizure of electronic mail and communication records of a similar nature

Dissertação apresentada à Faculdade de Direito da Universidade de Coimbra no âmbito do 2.º Ciclo de Estudos em Ciências Jurídico-Forenses (conducente ao grau de Mestre)

Orientadora: Professora Doutora Sónia Mariza Florêncio Fidalgo

Coimbra, 2020

Se o alastramento do uso do computador e das redes de telecomunicações vem potenciando a extensão da criminalidade, que chegue o momento em que se converta no melhor meio de a combater, sob a envolvência do Direito.

António Garcia Lourenço Martins[*]

[*] MARTINS, A.G. Lourenço, *Criminalidade Informática,* AA.VV., *Direito da Sociedade da Informação,* Vol. IV, Coimbra Editora, 2003, p. 41.

Agradecimentos

O meu primeiro agradecimento não poderia deixar de ser à Professora Doutora Sónia Fidalgo, não só pela curiosidade que despertou em mim, como também pela sua disponibilidade e amabilidade.

Dirijo igualmente uma palavra de apreço à Faculdade de Direito da Universidade de Coimbra da qual orgulhosamente fiz parte, especialmente ao Corpo Docente de Direito Processual Penal por ao longo da minha passagem por esta Casa ter fomentado o meu fascínio pela área.

Na esfera pessoal, em momento algum poderia deixar de agradecer às minhas Amigas de curso, com quem tive o gosto de partilhar as dores, as alegrias e as lições (de Direito e de vida) que levo do meu percurso académico; ao Miguel que com valiosas sugestões me auxiliou até ao último minuto.

As minhas derradeiras palavras de gratidão dedico-as aos meus queridos Pais, pelo seu apoio incondicional, pela confiança que sempre depositaram nas minhas capacidades e por, desde tenra idade, terem cultivado em mim o gosto pelas questões da justiça, impulsionando-me sobremaneira ao longo do rumo que fui escolhendo. Aos meus estimados Avós e Tia que com infinitas palavras de incentivo e constante amparo acompanharam de perto a minha passagem por Coimbra, um imenso obrigado.

Resumo

O legislador português, com o intuito de fazer face aos novos perigos da Era Digital e de forma a cumprir obrigações internacionais, numa tentativa de atualizar o ordenamento jurídico nacional regulando o que se está a tornar o cerne do processo penal – a prova digital –, decidiu consagrar em legislação avulsa uma série de meios de obtenção da mesma.

Entre eles encontra-se, problemática que tem dividido a doutrina e jurisprudência portuguesas, a apreensão de correio eletrónico e registos de comunicação de natureza semelhante disposta no art. 17.º da Lei do Cibercrime, Lei n.º 109/2009, de 15 de setembro, que, por sua vez, remete para o regime de apreensão de correspondência previsto nos art. 179.º e 252.º do CPP.

Começando por questionar se a escolha do legislador em estipular meios de obtenção de prova digital fora do Código de Processo Penal foi adequada, dado o crescente peso para a descoberta da verdade da prova em apreço e continuando o mesmo diploma a remeter o aplicador para o regime das escutas telefónicas; passando por refletir se de facto deve ser acolhida entre nós uma equiparação entre mensagens de correio eletrónico e semelhantes e o correio tradicional, atenta as gritantes diferenças técnicas entre ambos os tipos de prova e as dificuldades que a aplicação do regime garantístico da apreensão de correspondência, pautado por exigências processuais pensadas para o correio corpóreo fechado, implicam para a investigação criminal; culminando com uma breve abordagem de como o regime jurídico alemão, tradicionalmente fonte de inspiração para o nosso legislador, regula este meio de obtenção de prova, apurarei por que razão é impreterível reformar a lei nacional no que toca à apreensão de e-mails e semelhantes, evitando a tendência de atribuir às *novas* comunicações eletrónicas, as regras que outrora se delinearam para a *convencional* correspondência física.

Palavras-chave: Correio eletrónico e registos de comunicações de natureza semelhante; Apreensão de comunicações eletrónicas; Lei do Cibercrime.

Abstract

In order to comply with international obligations and face the Digital Age dangers, the Portuguese legislator has seen fit to enact separate legislation establishing a set of means of gathering evidence, in an attempt to update the national legal system and more deeply regulate what is becoming the core of criminal procedure – the digital evidence.

Among them is a problematic that has divided Portuguese doctrine and jurisprudence: the seizure of electronic mail and communication records of a similar nature enacted in Article 17 of the Cybercrime Act, Law 109/2009 of September 15, which points towards the seizure of correspondence practices laid down in Article 179 and 252 of the Code of criminal Procedure.

Opening by questioning whether the legislator's choice to stipulate the means of obtaining digital evidence outside the Code of Criminal Procedure was appropriate or not, given the ever-increasing importance of this kind of evidence in pursuit of truth and bearing in mind this legal document continues to direct the law enforcement officer towards the wiretapping regime; then by reflecting on whether we should accept equal treatment for both electronic messages and corporeal mail, considering not only the glaring technical differences between these two types of evidence but also the difficulties for the criminal investigation that the application of the strict system which regulates the seizure of correspondence entails, due to being based on the procedural requirements designed for traditional mail; and by concluding with a brief analysis on how the German legal regime, a long-established inspiration for the Portuguese legislator, regulates this means of gathering digital evidence, I shall ascertain why it is crucial to reform the national law regarding the seizure of e-mails and the like while avoiding the tendency to apply the same rules that were once devised for *traditional* mail to this *new* electronic communication.

Keywords: Electronic mail and communication records of a similar nature; Seizure of electronic communications; Cybercrime Law.

Lista de siglas e Abreviaturas

AA.VV. – Autores vários

Ac. – Acórdão

Al. – Alínea

Art. – Artigo

BVergF – Bundesverfassungsgericht (Tribunal Constitucional Federal Alemão)

CCiber – Convenção sobre o Cibercrime do Conselho da Europa

Cfr. – Conforme

CP – Código Penal

CPP – Código de Processo Penal

CRP – Constituição da República Portuguesa

DR – Diário da República

DL – Decreto-Lei

DLG – Direitos, Liberdades e Garantias

EMS – Enhanced Messaging Service

GG – Grundgesetz (Constituição Alemã)

IM – Instant Messenger

IP – Internet Protocol

IRC – Internet Relay Chat

JIC – Juiz de Instrução Criminal

LC – Lei do Cibercrime

LCI – Lei da Criminalidade Informática

MMS – Multimedia Messaging Service

MP – Ministério Público

N.º – Número

OPC – Órgãos de Polícia Criminal

P. – Página

PGR – Procuradoria-Geral da República

RECCiber – Relatório Explicativo da Convenção sobre o Cibercrime

SMS – Short Message Service

SS. – Seguintes

StPO – Strafprozeßordnung (Código de Processo Penal Alemão)

StGB – Strafgesetzbuch (Código Penal Alemão)

TC – Tribunal Constitucional

TCP – Transmission Control Protocol

TJUE – Tribunal de Justiça da União Europeia

TRE – Tribunal da Relação de Évora

TRG – Tribunal da Relação de Guimarães

TRL – Tribunal da Relação de Lisboa

TRP – Tribunal da Relação do Porto

UE – União Europeia

Vd. – Abreviatura de *vide* (ver)

V.g. – Abreviatura de *verbi gratia* (por exemplo)

Índice

Introdução

A disseminação das tecnologias de informação e comunicação veio inovar a forma como o cidadão comum comunica com os seus pares, despoletando o interesse das autoridades pelas comunicações eletrónicas privadas, cujo acesso, por serem passíveis de fornecer indícios sobre as infrações e seus infratores, pode ser decisivo para o sucesso da justiça.

Por conseguinte, inspirado por diplomas europeus que o despertaram para os novos problemas de uma época computorizada, o legislador português, através da Lei do Cibercrime, Lei n.º 109/2009, de 15 de setembro, veio munir a investigação criminal de novos instrumentos de obtenção de prova em ambiente digital. A LC, apesar da sua denominação, não tem o seu âmbito de aplicação restringido aos crimes informáticos, explicitando o seu art. 11.º que as disposições processuais aqui consagradas se aplicarão igualmente no caso de crimes em relação aos quais seja necessária a recolha de prova em suporte eletrónico.

Conferindo este preceito às diligências processuais consagradas na LC uma índole transversal a todo o processo penal e sendo facto incontornável que as comunicações eletrónicas desempenharão cada vez mais um papel de destaque na investigação penal, impõe-se analisar um dos meios de obtenção desta prova digital.

Assim, o meu estudo centrar-se-á no art. 17.º da LC que estipula a apreensão de correio eletrónico e registos de comunicações de natureza semelhante armazenados num sistema informático que tenha sido legitimamente acedido pelas autoridades, que remete para o regime da apreensão de correspondência consagrado nos artigos 179.º e 252.º do CPP.

A interpretação a dar a esta remissão tem feito correr tinta na doutrina nacional numa tentativa de responder à questão de se a aplicação do regime da apreensão de correspondência à apreensão de e-mails e registos semelhantes se deve fazer na sua totalidade, sem redução do seu âmbito, como o Tribunal da Relação de Lisboa tem considerado ou, pelo contrário, deve aquele regime ser objeto de uma cuidadosa adaptação à nova realidade aqui em jogo.

Além de averiguar que sentido deve o aplicador atribuir à lei vigente, parece-me fundamental aferir se a própria escolha do legislador em remeter a apreensão de e-mails e registos análogos para o regime de correspondência corpórea foi, ou não, apropriada.

1. A Era Digital e a consequente relevância das comunicações eletrónicas na investigação criminal

Foi na década de 1960, com o intuito de formar uma rede de comunicação entre dois ou mais computadores, atenta a possibilidade de ocorrência de uma guerra nuclear, que o governo americano criou a precursora da Internet – a ARPAnet.[1] Até finais da década de 80, utilizou-se a Internet exclusivamente para fins militares e académicos, altura em que se libertou e passou a ser um espaço sem fronteiras, sem dono e, assim alguns pretendem, com o seu quê de independência e anarquia.[2]

A partir de meados de 1990, os sistemas informáticos e a Internet invadiram o quotidiano do indivíduo e suas instituições, encerrando em si mesmos uma espécie de monopólio de grande parte dos setores da vida em sociedade que, gradualmente, se tornou dependente do tratamento automático de dados. Despedimo-nos, assim, da Sociedade dos Serviços e demos as boas-vindas à Sociedade da Informação – "*um verdadeiro modo de desenvolvimento económico e social baseado na aquisição, tratamento e difusão de informação por via das redes de comunicação digitais"*.[3]

A Sociedade da Informação, dada a sua crescente relevância social, cultural e económica, depressa se tornou o centro de preocupações legislativas da União Europeia e dos demais Estados Ocidentais, que se esforçam por fazer o Direito acompanhar as significativas mudanças que a difusão das novas tecnologias veio operar na criminalidade.[4]

---

[1] Acrónimo em inglês para *Advanced Research Projects Agency Network.*

[2] Indignado com tentativas governamentais de regulamentação da Internet, o ativista digital Perry Barlow, em fevereiro de 1996, escreveu a célebre carta "A Declaration of Independence of Cyberspace", onde podemos ler "Governos do mundo industrial, em nome do futuro, pedimos que nos deixem sós. São *personae non gratae* entre nós. Falta-lhes soberania e legitimidade ética para implantar regras ou métodos. O ciberespaço não se ajusta às vossas fronteiras". Disponível *online* em https://www.eff.org/cyberspace-independence [acedido a 24 de novembro de 2019].

[3] VERDELHO, Pedro, *Cibercrime,* AA.VV., *Direito da Sociedade da Informação,* Vol. IV, Coimbra Editora, 2003, p. 348 e 349.

[4] Sobre os fatores que potenciam a deslocação criminosa na web, *vd.* SANTOS, Paulo; BESSA, Ricardo; PIMENTEL, Carlos, *Cyberwar – O Fenómeno, as Tecnologias e os Atores*, FCA – Editora de Informática, 2008, p. 6 e 7.

Para além de terem surgido novos tipos de crimes,[5] as características inerentes ao ciberespaço[6] propiciam que seja um célere motor de atos ilícitos a uma escala planetária.[7]

Todavia, *"dir-se-á que a tecnologia constitui uma parte do problema e também da sua solução",*[8] uma vez que a par dos novos problemas que relevam no âmbito criminal, a era digital trouxe consigo uma série de modernos instrumentos capazes de contribuir para os colmatar, como é o caso da prova digital.

Definida por Benjamim Silva Rodrigues como *"qualquer tipo de informação, com valor probatório, armazenada (em repositório eletrónico-digital de armazenamento) ou transmitida (em sistemas e redes informáticas ou redes de comunicações eletrónicas, privadas ou publicamente acessíveis), sob forma binária ou digital",*[9] a utilidade da prova

---

[5] Por um lado, surgiram crimes contra os próprios computadores ou sistemas de computadores, como é o caso do dano informático, do acesso ilegítimo ou da sabotagem informática; bem como crimes que só podem ocorrer no ambiente informático, como a burla informática ou a devassa por meio de informática. Por outro lado, apareceram crimes que, não obstante terem sido cometidos através de computadores ou sistemas de computadores, correspondem a crimes tradicionais, que poderiam ter sido cometidos por outras vias, como por exemplo o abuso de liberdade de imprensa cometido por um jornal online ou o branqueamento de capitais através de um banco virtual. Cfr. VERDELHO, Pedro, *Cibercrime, ob. cit.*, p. 348;
Sobre o desenvolvimento da legislação acerca da criminalidade informática *vd.* MARTINS, A. G. Lourenço; MARQUES, J. A. Garcia; DIAS, Pedro Simões, *Cyberlaw em Portugal: O direito das tecnologias da informação e da comunicação*, Centro Atlântico, 2004, p. 425.

[6] Termo usado pela primeira vez por William Gibson, escritor americano de ficção científica, na sua obra "*Burning Chrome*", anos mais tarde popularizado na obra também de sua autoria "*Neuromancer".*

[7] Estamos a falar de uma infinita quantidade de dados que são transmitidos a uma velocidade estonteante – comunicações a nível mundial que desconhecem fronteiras nacionais, frustrando, assim, a aplicação do direito nacional. Os infratores sentem-se protegidos por um certo anonimato que a rede lhes proporciona, tal a dificuldade de, por vezes, se restituir o "trajeto criminoso" na web. Também a reprovação social de quem pratica crimes informáticos continua a ser de longe mais leve em relação ao criminoso "comum". Este último corre o risco de ser arrastado para um pesado e humilhante processo onde o rotulam e perseguem como delinquente, estigmatização esta que nem sempre acontece com a mesma intensidade no mundo virtual (onde o próprio infrator virtual de nome *hacker* pode até ser considerado uma espécie de justiceiro a quem deve ser reconhecido o devido valor, por usar os seus conhecimentos informáticos de forma a expor a corrupção de pessoas comummente consideradas inatingíveis, o que acaba por tornar este criminoso aos olhos da lei, num denunciante aos olhos do povo – como tivemos oportunidade de testemunhar em Portugal com todo o clamor social que se fez ouvir em torno do caso Rui Pinto). E mesmo quando está em causa um crime em que valores tradicionais foram ameaçados por via informática, a ausência de controlo a nível social ainda releva através da ainda deficiente ação reguladora das instâncias formais de combate ao crime que usa a tecnologia como meio. (*Vd.* SANTOS, Paulo; BESSA, Ricardo; PIMENTEL, Carlos, *ob. cit.*, p. 5). Sendo que a dificuldade que as instâncias formais enfrentam deve-se não só ao facto do Direito se cruzar aqui com uma realidade que implica profundos conhecimentos técnicos para que a regule adequadamente, como também ao incessante desenvolvimento do mundo virtual, que faz com que o que é verdade hoje dentro do nosso território nacional, amanhã, noutro local do globo, possa já ser mentira, por via de um qualquer avanço tecnológico que tornou obsoleta a regra pensada para uma realidade já desatualizada.

[8] MARTINS, A.G. Lourenço, *ob. cit.*, p. 15.

[9] RODRIGUES, Benjamim Silva, *Direito Penal, Parte Especial – Direito Penal Informático-Digital*, Tomo I, Coimbra Editora, 2009, p. 722;
Na terminologia de Armando Dias Ramos, a prova digital traduz-se em *"informação passível de ser obtida ou extraída de um dispositivo eletrónico (local, virtual ou remoto) ou de uma rede de comunicações"*, o que leva a que a mesma *"para além de ser admissível, deve ser também autêntica, precisa e completa"* (Cfr.

digital vai muito além de estarmos perante crimes informáticos ou de crimes praticados através de um sistema informático, pois, tendo em conta que vivemos numa sociedade cada vez mais subordinada às novas tecnologias, é apenas natural que o acesso à prova digital seja fulcral para a prossecução penal de todo e qualquer tipo de crime.

Com efeito, a prova digital já marca presença na maioria dos processos criminais, podendo ser encontrada num amplo leque de sistemas eletrónicos que podem conter diversas categorias de prova que, devido à sua especificidade, implicam diferentes meios de recolha que diferem anos-luz dos meios de recolha empregues para a prova física.[10]

Possuindo esta *nova* categoria probatória natureza intrinsecamente imaterial, efémera e facilmente alterável, afigura-se uma prova complexa e "frágil" (na medida em que um mero descuido pode torná-la inutilizável), impondo a quem trata da mesma uma série de conhecimentos técnicos qualificados, o que leva Armando Dias Ramos a considerar que a prova digital, entre as classificações probatórias tipificadas, se deve considerar prova pericial.[11/12]

Uma das áreas que o advento das novas tecnologias veio revolucionar foi, sem dúvida, a comunicação privada. Dotadas de características como a celeridade, o baixo custo e o fácil acesso, que as tornaram um meio de comunicação privilegiado, as comunicações eletrónicas, desde o correio eletrónico[13] (cuja utilização, a meu ver, está cada vez mais reduzida a comunicações formais, por exemplo, entre empregador e trabalhador) passando pelas SMS, até às aplicações de mensagens instantâneas como o *Messenger* ou o *WhatsApp*,

---

RAMOS, Armando Dias, *A prova digital em processo penal: O Correio Eletrónico,* 2.ª Edição, Chiado Editora, 2017, p. 96);
Acerca da distinção entre prova digital e prova eletrónica *vd.* RAMALHO, David Silva, *Métodos ocultos de investigação criminal em ambiente digital*, Almedina, 2017, p. 98-102).

[10] CONSELHO DA EUROPA, *Electronic Evidence Guide – A basic guide for police officers, prosecutors and judges*, p. 16-31. Disponível *online* em https://rm.coe.int/c-proc-electronic-evidence-guide-2-1-en-june-2020-web2/16809ed4b4 [acedido a 7 de setembro de 2020].

[11] RAMOS, Armando Dias, *A Prova Digital em Processo Penal, cit.*, p. 96 e ss.

[12] Sobre a Ciência Forense Digital, o método científico subjacente às atividades de recolha, exame, análise, preservação e apresentação da prova digital *vd.* RAMALHO, David Silva, *ob. cit.*, p. 108 e ss.

[13] Tom Van Vleck acredita que o que é atualmente chamado correio eletrónico possa ter sido inventado várias vezes de forma independente, porém desconhece registo de qualquer programa de correio eletrónico anterior ao que ele ajudou a criar juntamente com o seu colega Noel Morris em 1965. Mais informação sobre os primeiros programas de correio eletrónico em Tom Van Vleck, *The History of Eletronic Mail*, em https://www.multicians.org/thvv/mail-history.html [acedido a 24 de novembro de 2019];
Mais tarde, em 1971, Ray Tomlinson, considerado o "pai" do correio eletrónico como o conhecemos hoje, implementa o primeiro sistema de correio eletrónico da ARPAnet e cria o "@" que significa *at* (em tal lugar), que usou para separar a pessoa e o servidor que iria hospedar a mensagem. Mais informações em https://www.internethalloffame.org/blog/2012/07/30/meet-man-who-put-%E2%80%98%E2%80%99-your-e-mail [acedido a 24 de novembro de 2019].

são usadas pelo grosso dos cidadãos diariamente, nas mais variadas relações humanas. Traduzindo-se em mensagens de texto, de voz, imagens, vídeos, transmitidos via computador, telemóvel ou aparelhos que inicialmente desempenhavam funções meramente mecânicas, como o relógio e o automóvel, mas que atualmente são verdadeiros aparelhos eletrónicos que permitem ao seu utilizador comunicar.

A realidade virtual está tão enraizada, mormente nas gerações mais novas, que redes sociais como o *Facebook* e o *Instagram* podem ser consideradas uma extensão da vida "real", quando utilizadas tal e qual um diário virtual onde as informações de cariz pessoal que se partilham variam entre um mero gosto musical e o mais ínfimo detalhe do dia a dia.[14]

Assim, as mensagens eletrónicas armazenadas num sistema informático, potenciais repositórios de valiosas informações sobre a vida dos transgressores e seus crimes, possuem grande valor probatório, especialmente serviços como o *WhatsApp* que costumam ser palco de trocas de informação tão pessoal como uma conversa telefónica privada, mas, ao contrário desta, o conteúdo daquelas comunicações fica automaticamente armazenado no suporte eletrónico do destinatário.

Sendo a aquisição de prova um momento essencial no processo penal e dada uma considerável fatia das nossas interações sociais estar a realizar-se por via eletrónica, é de esperar que o legislador sinta a necessidade de adaptar a investigação criminal a este novo meio de comunicação, de forma a lançar mão do que pode ser uma poderosa ferramenta para a descoberta da verdade.

[14] Repare-se no crescente interesse dos empregadores pela "pegada digital" dos seus trabalhadores. Já há empresas que fornecem à entidade empregadora um serviço exclusivamente dedicado a avaliar o perfil psicológico de um candidato através dos dados que o mesmo partilha nas suas redes sociais, de forma a averiguar se o conteúdo que decide expor se coaduna com os valores da empresa ou se, pelo contrário, indicia potenciais riscos para o bom nome do empregador, como por exemplo, algum tipo de fanatismo, sexismo ou assédio. A título de exemplo *vd*. https://apnews.com/press-release/pr-businesswire/83451cf9ed6c49f094ef946975e7f772 [acedido a 3 de julho de 2020].

2. No plano Internacional

Não foi somente o galopante avanço tecnológico que ditou a pertinência da Lei do Cibercrime. Também o Direito Internacional, através de dois diplomas, veio exigir a sua elaboração: a LC adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa e transpõe 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.[15]

2.1. Convenção sobre o Cibercrime do Conselho da Europa

Ciente de que os novos desafios resultantes da evolução tecnológica tornaram os instrumentos clássicos de cooperação internacional em matéria penal deficitários, pois pensados para uma realidade completamente ultrapassada, o Conselho da Europa criou um Comité de Peritos sobre Criminalidade no Ciberespaço (PC-CY), ao qual foi atribuída a tarefa de criar um instrumento jurídico eficaz e vinculatório, com mais peso que a Recomendação n.º R (89) 9 do Conselho da Europa.[16] No dia 23 de novembro de 2001, no âmbito da Conferência Internacional sobre a Criminalidade, foi aberta à assinatura em Budapeste a Convenção sobre o Cibercrime do Conselho da Europa, entrando em vigor a 1 de julho de 2004.[17]

Portugal assinou-a naquela mesma data, porém, no plano nacional, só oito anos mais tarde teve lugar a sua aprovação, com a Resolução da Assembleia da República n.º 88/2009 e ratificação pelo Decreto do Presidente da República n.º 91/2009, ambas a 15 de setembro de 2009.[18]

---

[15] A Diretiva 2013/40/EU do Parlamento Europeu e do Conselho, de 12.08.2013, relativa a ataques contra os sistemas de informação, veio substituir a Decisão-Quadro 2005/222/JAI do Conselho.

[16] A CCiber traduziu-se numa evolução da Recomendação n.º R (89) 9 do Conselho da Europa, substituindo-a, Recomendação esta que versa sobre a criminalidade relacionada com computadores e que já em 1991 impulsionou, entre nós, o nascimento da Lei da Criminalidade Informática.

[17] Para entrar em vigor a Convenção tinha de ser ratificada por cinco Estados, três deles obrigatoriamente Estados-Membros do Conselho da Europa; Cfr. RODRIGUES, Benjamim Silva, *Da Prova Penal, Da Prova – Eletrónico-Digital e da Criminalidade Informático-Digital*, Tomo IV, Rei Dos Livros, 2011, p. 329-334.
Não obstante ter tido origem num contexto Europeu, na sua elaboração participaram outros países que não integravam o Conselho da Europa, como os Estados Unidos da América, o Canadá, o Japão e a África do Sul, reflexo da ambição universal deste Tratado Internacional, esperando-se que viesse a ser aceite pelos demais países do globo. VERDELHO, Pedro, *Cibercrime, cit.*, p. 370.

[18] VENÂNCIO, Pedro Dias, *Lei do Cibercrime Anotada e Comentada,* Coimbra Editora, 2011, p. 23.

Tendo a cibercriminalidade uma natureza transnacional, a CCiber, considerada pelo legislador português "*o primeiro e mais importante trabalho internacional de fundo sobre crime no ciberespaço",*[19] procurou definir um quadro comum de repressão de forma a proteger a sociedade da informação da cibercriminalidade, através da adoção de legislação adequada, tanto a nível de direito substantivo (definindo infrações informáticas e suas sanções) como a nível de direito processual (determinando diligências processuais aplicáveis ao mundo virtual) e estabelecendo medidas de cooperação internacional das polícias e magistraturas.[20]

No que ao presente estudo importa, centrar-me-ei no Capítulo II, Secção II da CCiber, salientando aquela que é uma das suas mais relevantes normas: o n.º 2 do art. 14.º que, ditando que as medidas processuais consagradas neste diploma internacional não se aplicam apenas aos crimes nele previstos, mas também a crimes cometidos por meio de um sistema informático e ainda a crimes relativamente aos quais seja necessário proceder à recolha probatória em suporte eletrónico, confere às regras processuais consagradas na Convenção um âmbito transversal a todo o processo penal.[21]

A opinião de Pedro Dias Venâncio, segundo a qual o art. 17.º, juntamente com os artigos 16.º (apreensão de dados informáticos) e 18.º (interceção de comunicações) da LC, é o resultado da transposição para a ordem jurídica interna do art. 19.º da CCiber que regula a busca e apreensão de dados armazenados num computador, não é unânime.[22] No entanto,

---

[19] Exposição dos Motivos da Proposta de Lei n.º 289/X/4.ª – Lei do Cibercrime, p. 2.

[20] Ponto 16 do Relatório Explicativo da CCiber.

[21] Urge explicitar que esta extensão das diligências processuais da Convenção, para outros tipos de crimes não consagrados na mesma, deve ser aplicada tendo sempre em conta o artigo 15.º que dita que a aplicação das medidas previstas na própria Convenção se faça não descurando as normas de direito interno e de direito internacional que defendam os direitos humanos, impondo uma atuação à luz do princípio da proporcionalidade. Assim, a Convenção não proíbe a aplicação das normas de direito nacional aquando da aplicação de qualquer mecanismo de investigação criminal. SANTOS, Paulo; BESSA, Ricardo; PIMENTEL, Carlos, *ob. cit.*, p. 28.

[22] VENÂNCIO, Pedro Dias, *ob. cit.*, p. 116;
A discórdia entre os diferentes autores que se debruçaram sobre o regime em discussão começa, desde logo, quanto à origem do art. 17.º da LC. Ao contrário de Pedro Dias Venâncio, Rui Cardoso é da opinião que, por a CCiber não se referir expressamente à apreensão de correio eletrónico (no seu art. 19.º apenas refere "dados informáticos"), a origem do art. 17.º está somente na Proposta de Lei n.º 289/X/4.ª no seu art. 19.º, tendo este a mesma redação que o art. 17.º da LC. (Cfr. CARDOSO, Rui, "Apreensão de correio eletrónico e registos de comunicações de natureza semelhante – art. 17.º da Lei n.º 109/2009, de 15.IX", *Revista do Ministério Público*, n.º 153, 2018, p. 169); Já Pedro Verdelho, ao encontro do também entendido por Duarte Rodrigues Nunes, vai mais longe e considera o art. 17.º um artigo inovador quanto ao conteúdo, onde o legislador português procurou, no fundo, adaptar os princípios processuais da apreensão de correspondência previstos no nosso CPP aos novos meios de comunicação. (Cfr. VERDELHO, Pedro, "A nova Lei do Cibercrime", *Scientia Iuridica*, Tomo LVIII, n.º 320, 2009, Universidade do Minho, p. 740 e NUNES, Duarte Rodrigues, *Os meios de obtenção de prova previstos na Lei do Cibercrime*, Gestlegal, 2018, p. 139).

considero que se há medida processual consagrada na Convenção que merece atenção redobrada é a do art. 19.º da CCiber, pois, apesar de ter como epígrafe "Busca e apreensão de dados informáticos armazenados", não se referindo expressamente a "comunicações eletrónicas", trata da apreensão da prova digital já armazenada num sistema informático, possuindo, assim, semelhanças com o art. 17.º da LC.

Estipula o art. 19.º da CCiber no seu n.º 1 que "cada parte adotará as medidas legislativas e outras que se revelem necessárias para habilitar as suas autoridades competentes para proceder a buscas ou aceder de modo semelhante a um sistema informático ou a uma parte do mesmo, bem como a dados informáticos que nele se encontrem armazenados; e a um suporte que permita armazenar dados informáticos".

Já no seu n.º 2, o art. 19.º da CCiber vem introduzir uma possibilidade, na altura estranha à legislação portuguesa, ditando que se numa busca feita a um sistema de computadores nos termos do n.º 1, se tome conhecimento que os dados que se procuram estão armazenados noutro sistema de computadores situado em território nacional,[23] a busca pode ser estendida a este último – opção que a LC abarca no art. 17.º na parte em que consagra "(…) ou noutro a que seja permitido o acesso legítimo a partir do primeiro (…)".

Concretamente quanto a apreensões, importa-nos o n.º 3 do art. 19.º da CCiber nos termos do qual cada Estado deve legislar no sentido de apreender ou obter de forma semelhante um sistema informático: apreendendo-se simplesmente o equipamento informático; efetuando-se uma cópia total ou parcial, em suporte de papel ou em suporte magnético, da informação pretendida; ou procedendo-se à apreensão de um meio de armazenamento de dados (um dispositivo, fixo ou amovível que possa conter informação), variando a técnica empregue consoante a exigência do caso concreto.

É de salientar que a exigência de "determinação judicial" também se encontra dependente do caso concreto, não pretendendo este artigo modificar os pressupostos da autorização judicial ou do consentimento para a realização das buscas dos ordenamentos jurídicos dos países que aderirem à Convenção.[24]

O n.º 3 do mesmo artigo exige ainda que se preserve a integridade dos dados pertinentes (os que foram copiados ou removidos devem manter-se inalterados desde a sua

[23] Todos os artigos desta secção dizem apenas respeito às medidas que devem ser tomadas a nível nacional. Ponto 192 do Relatório Explicativo da CCiber.

[24] VERDELHO, Pedro; BRAVO, Rogério; ROCHA, Manuel Lopes, *Leis do Cibercrime*, Volume 1, Centro Atlântico, 2003, p. 56.

apreensão até ser intentada a ação penal, salvaguardando-se assim a *cadeia de posse*) e que os mesmos se tornem inacessíveis ou sejam removidos do computador, tal não significando uma eliminação definitiva dos dados apreendidos.[25]

Ambos os meios de obtenção de prova aqui em questão – buscas e apreensões – existiam em qualquer ordenamento jurídico para objetos tangíveis. No nosso caso, as buscas e apreensões estavam previstas nos artigos 174.º e 178.º do CPP, respetivamente. A novidade do art. 19.º reside no facto de vir permitir que os dados informáticos passem a ser considerados coisas apropriáveis e, por isso, suscetíveis de serem obtidos *"com fins de investigação ou de um procedimento penal da mesma forma que os objetos tangíveis"*.[26]

No entanto, o próprio Relatório Explicativo da CCiber no seu ponto 187 explica a necessidade de consagração de um regime de busca e apreensão distintos dos que já existem no ordenamento interno de cada país, pois estes têm como objeto bens corpóreos, ao passo que na prova eletrónica está em causa uma realidade intangível e, como tal, merecedora de uma abordagem distinta.

No mesmo sentido, antes da publicação da atual Lei do Cibercrime, já Pedro Verdelho alertava para o facto de que as medidas processuais em causa no art. 19.º da CCiber estão reguladas no nosso CPP de uma forma que as torna ineficazes no ciberespaço, defendendo, por isso, a necessidade do legislador adaptar o processo penal ao universo virtual.[27]

Também Benjamim Silva Rodrigues defendia a autonomização daquilo a que o apelidou de *Direito (Processual) Penal Informático* como resultado de uma revisão integral dos regimes de meios de prova e meios de obtenção de prova, adaptados à nova realidade informática.[28]

Onze anos depois da aprovação da Convenção de Budapeste por Portugal, parecem ainda ser ignoradas algumas das preocupações que estiveram na origem da elaboração deste tratado internacional, na medida em que, mesmo com a nova Lei do Cibercrime, ainda se

---

[25] Já o dever de colaboração plasmado no n.º 4 do art. 19.º traduz-se numa medida coerciva de que as autoridades competentes podem lançar mão, de forma a obrigar um administrador do sistema, em virtude dos seus conhecimentos técnicos acerca do sistema informático, a colaborar. No entanto, esta medida que se destina a facilitar a busca e apreensão dos dados informatizados, deve ser conduzida sempre à luz de um princípio de razoabilidade. Ponto 197 a 202 do RECCiber (STE n.º 185). Por último, o n.º 5 do mesmo artigo consagra como limitações a estes procedimentos, o que consta dos artigos 14.º e 15.º da CCiber.

[26] Ponto 184 do RECCiber.

[27] VERDELHO, Pedro, *Cibercrime, cit.*, p. 377 e 378.

[28] RODRIGUES, Benjamim Silva, *Da prova penal, Da prova – eletrónico-digital e da criminalidade informático-digital, cit.*, p. 351.

parece tratar de forma leviana o facto da prova digital ter uma natureza intrinsecamente distinta da prova corpórea, o que inevitavelmente leva a incongruências práticas quando a letra da lei manda aplicar o mesmo regime a ambas, como terei oportunidade de desenvolver.

2.2. Decisão-Quadro n.º 2005/222/JAI relativa a ataques contra sistemas de informação

A 16 de março de 2005, foi publicada no Jornal Oficial da União Europeia a Decisão-Quadro n.º 2005/222/JAI, de 24 de fevereiro de 2005, relativa a ataques contra sistemas de informação. No entanto, ao contrário da CCiber, a Decisão-Quadro não contém normas processuais, limitando-se a definir um conjunto de infrações penais e consequentes sanções.

A Decisão-Quadro n.º 2005/222/JAI esclarece *ab initio* que os ataques contra os sistemas de informação, que considera constituírem a infraestrutura vital dos Estados-Membros, ao colocarem em causa a sociedade da informação tal como a conhecemos, onde valores como a liberdade, segurança e justiça carecem de uma defesa contínua, exigem uma abordagem internacionalmente organizada que os combata. Com efeito, este diploma tem como principal objetivo reforçar a cooperação judiciária entre os Estados-Membros, *mediante uma aproximação das suas disposições de direito penal em matéria dos ataques contra sistemas de informação.* É a dimensão transfronteiriça destes ataques que implica uma mudança legislativa a nível global, que preencha as lacunas das legislações internas dos Estados-Membros e harmonize as várias legislações penais, respondendo eficazmente a esta ameaça igualmente global.[29]

Segundo o art. 12.º deste diploma, os Estados-Membros teriam de tomar as medidas necessárias à adequação da sua legislação interna a esta decisão-quadro até 16 de março de 2007, de modo que, em relação a esta, a LC já vem com dois anos de atraso, já que Portugal apenas a transpôs para o ordenamento nacional em 2009 através da Lei n.º 109/2009, de 15 de setembro.

Esta Decisão-Quadro, apesar de ter estado na base da LC, teve o seu termo de validade a 2 de setembro de 2013, data em que foi substituída pela Diretiva 2013/40/EU de

[29] Ponto (1) a (5) da Decisão-Quadro 2005/222/JAI.

12 de agosto de 2013, do Parlamento Europeu e do Conselho, relativa a ataques contra os sistemas de informação. Visou a Diretiva alargar o âmbito de aplicação da Decisão-Quadro. É o que decorre do n.º 1 do seu art. 16.º onde podemos ler "*Os Estados-Membros põem em vigor as disposições legislativas, regulamentares e administrativas necessárias para dar cumprimento à presente diretiva até 4 de setembro de 2015".*

Contudo, a maior parte dos tipos legais constantes nesta Diretiva já se encontravam na Decisão-Quadro que a mesma pretendeu revogar, tendo sido adotada pela generalidade dos Estados-Membros. Daí a opinião de Armando Dias Ramos, segundo a qual a Diretiva não veio fazer frente ao *"panorama atual das práticas criminosas, revelando-se, por isso, desajustada da realidade"*.[30]

3. No plano nacional

3.1. O regime que (ainda) consta do Código de Processo Penal

No ano de entrada em vigor do nosso Código de Processo Penal – 1988 – os meios de transmissão à distância de notícias ou dados cingiam-se fundamentalmente ao telefone fixo, telegrama, fax, rádio, teletexto, aparelhos que nos dias de hoje detêm uma porção cada vez mais diminuta dos atos de telecomunicação. Além do mais, o processo telecomunicacional tinha um cariz *intrinsecamente fugaz e transitório.* A telecomunicação "esgotava-se" no momento em que acontecia, só nesse momento podendo ser intercetada e registada, incidindo esta interceção e registo principalmente sobre o seu conteúdo. Com o surgimento da era digital, a telecomunicação ganhou um caráter duradouro, melhor dizendo, passou a deixar um rasto – uma série de dados de tráfego que, muitas vezes, são mais relevantes que o próprio conteúdo, muito dizendo acerca das partes intervenientes na comunicação.[31]

[30] Sobre as novidades, ou falta delas, que a Diretiva 2013/40/EU trouxe consigo *vd.* RAMOS, Armando Dias, "A Novíssima Diretiva sobre o Cibercrime", texto que diz respeito à apresentação na Conferência de 30.05.2013, na Universidade Autónoma de Lisboa, sob a temática "Espaço de Liberdade, Segurança e Justiça", 2013. Disponível para consulta em https://www.academia.edu/8696174 [acedido a 27 de novembro de 2019].

[31] ANDRADE, Manuel da Costa, *Bruscamente no verão passado, A reforma do Código de Processo Penal*, Coimbra Editora, 2009, p. 155 e 156.

Com a revisão de 1998 o legislador estendeu o regime das escutas telefónicas às comunicações transmitidas por qualquer meio técnico diferente de telefone, onde se incluiu o correio eletrónico ou outras formas de transmissão de dados por via telemática.[32]

Anos mais tarde, na reforma de 2007 acrescentou-se uma especificação ao n.º 1 do art. 189.º do CPP relativamente à interceção de correio eletrónico e outras formas de transmissão de dados por via telemática: "mesmo que se encontrem guardadas em suporte digital". Este aditamento, *prima facie* inofensivo, leva Paulo Dá Mesquita a encarar a revisão de 2007 como uma *oportunidade perdida*, na medida em que, não obstante o avanço tecnológico e consequentes novas exigências, manteve inalterada a sistematização original do capítulo Escutas Telefónicas. Assim, continuando a vigorar a extensão para o regime das mesmas, a inovação que a revisão trouxe consigo – alargou a extensão a uma fase superveniente em que os dados já se encontram armazenados, fora do âmbito do fornecedor do serviço – é, nas palavras do autor, *teleologicamente infundada e imprecisa.*

O n.º 1 do art. 189.º, onde se lê "comunicações guardadas em suporte digital", torna claro que não é porque a comunicação em si termina, que termina a tutela extensiva do regime das escutas, que, por sua vez, determina a exigência de integração num dos crimes de catálogo e a reserva judicial. Ora, foi ignorada a diferença que existe entre a comunicação através de redes eletrónicas e os aparelhos eletrónicos como simples forma de registo e arquivo, conferindo à mensagem guardada num documento em forma digital um regime mais garantístico do aplicado a uma mensagem imprimida e guardada em suporte papel, apesar de ambos terem características idênticas em termos de *relações de confiança comunicacional.* Qual é o fundamento desta discriminação se, na opinião do mesmo autor, é mais fácil avaliar a fidedignidade de um documento em suporte digital pois ele será o *original ou, correspondendo a um ficheiro renomeado, ainda poderá ter um lastro informático do original, indetetável no suporte papel?*[33]

O atual CPP no art. 189.º continua a estipular que o regime das escutas telefónicas consagrado nos artigos 187.º e 188.º é "correspondentemente aplicável às conversações ou comunicações transmitidas por qualquer meio técnico diferente do telefone, *designadamente*

[32] NEVES, Rita Castanheira, *As ingerências nas comunicações eletrónicas em processo penal, Natureza e respetivo regime jurídico do correio eletrónico enquanto meio de obtenção de prova,* Coimbra Editora, 2011, p. 139.
[33] MESQUITA, Paulo Dá, "Prolegómenos sobre prova eletrónica e interceção de telecomunicações no Direito Processual Penal Português – o Código e a Lei do Cibercrime", *Processo Penal, Prova e Sistema Judiciário*, Coimbra Editora, 2010, p. 90 e 91.

correio eletrónico ou outras formas de transmissão de dados por via telemática, mesmo que se encontrem guardadas em suporte digital, e à interceção das comunicações entre presentes". Esta cláusula de extensão, para além de misturar realidades técnicas totalmente diferentes,[34] por exigir estarmos perante um dos crimes de catálogo do n.º 1 do art. 187.º, onera escusadamente a investigação criminal, na medida em que assegura ao e-mail uma maior tutela do que a que é oferecida pelo regime das buscas, regime este que deveria ser o aplicado a estes documentos.[35]

Porém, o legislador de 2009, com o art. 17.º da LC, ao regular a apreensão de correio eletrónico e registos de comunicações de natureza semelhante, aditou no final do preceito *"(…) aplicando-se correspondentemente o regime da apreensão de correspondência previsto no Código de Processo Penal*". Ao remeter-nos, não para o regime das escutas telefónicas, mas sim para o regime de apreensão de correspondência, o art. 17.º vem revogar tacitamente, por força do princípio *lex specialis derogat legi generali,* o art. 189.º do CPP.

Independentemente de saber se o regime da apreensão de correspondência será (ou não, como analisaremos) o mais adequado quando estamos perante correio eletrónico e registos semelhantes, se a lei extravagante se sobrepõe ao regime geral, por que razão o legislador não o revogou formalmente, evitando assim que se continue a invocar erradamente a sua vigência?

3.2 A Lei do Cibercrime

Antes de nos ocuparmos do regime que consta da Lei do Cibercrime, é necessário aludir ao seu surgimento e ao que podemos chamar de sua antecessora – a Lei n.º 109/91 de 17 de agosto, conhecida como a Lei da Criminalidade Informática. Esta Lei veio dar resposta à Recomendação n.º R (89) 9 do Conselho da Europa e teve como objetivo punir aquilo a que chamou de crimes informáticos.[36]

Curiosamente, foi a partir do ano da entrada em vigor da LCI que os portugueses passaram a ter a oportunidade de aceder à *Internet* fora do âmbito das redes científicas e

[34] Acompanhe-se a explicação de ANDRADE, Manuel da Costa, *Bruscamente no Verão passado, cit.,* p. 169-185.
[35] ANDRADE, Manuel da Costa, *Bruscamente no Verão passado, cit.,* p. 185.
[36] Sendo eles, a falsidade informática, o dano relativo a dados ou programas informáticos, a sabotagem informática, o acesso ilegítimo, a interceção ilegítima e a reprodução ilegítima de programa protegido (art. 4.º a 9.º, respetivamente).

universitárias da altura.[37] Para além da velha lei de 1991, pensada para a realidade desse ano, depressa se ter tornado desatualizada face às evoluções tecnológicas que a sucederam, era igualmente necessário satisfazer os compromissos internacionais impostos pela Convenção do Cibercrime e pela Decisão-Quadro 222/2005/JAI. Foi neste contexto que surgiu a Lei n.º 109/2009, de 15 de setembro, que aprovou a Lei do Cibercrime.

Apesar do art. 31.º da LC deixar claro que esta vem revogar a Lei n.º 109/91, insinuar que a Lei do Cibercrime se limitou a rever os tipos legais de crimes informáticos constantes da LCI de 1991 é, no mínimo, redutor. Este diploma, ao consagrar regras de direito processual e cooperação internacional, introduziu novos meios de investigação especificamente pensados para combater a criminalidade informática, respeitando, como vimos, as indicações da Convenção sobre o Cibercrime.[38]

A 15 de setembro de 2009, no seguimento da ratificação da CCiber, a Assembleia da República aprovou a Lei do Cibercrime. Esta Lei, através de uma estrutura tripartida entre normas materiais, normas processuais e normas relativas à cooperação internacional, pretendeu reunir num só diploma todas as regras respeitantes à criminalidade informática.

Se, no que toca aos crimes informáticos, a nova lei respeitou, na sua maioria, a tipologia prevista na Lei da Criminalidade Informática, é na sua dimensão processual que a LC introduziu significativas novidades no nosso ordenamento interno através da criação de novas figuras processuais.

Vejamos: relativamente às disposições de direito processual, a mais importante novidade é a norma do art. 11.º, relativa ao âmbito material de aplicação das disposições da LC. Vem este artigo explicitar que "com exceção do disposto nos artigos 18.º e 19.º as disposições processuais previstas no presente capítulo aplicam-se a processos relativos a crimes: *a)* previstos na presente lei; *b)* cometidos por meio de um sistema informático; ou *c) em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico".* Para além da aplicabilidade, que me parece óbvia, de que fala a al. *a)*, este artigo vem estender as diligências processuais consagradas nesta lei – ressalvando a interceção de comunicações (art. 18.º) e as ações encobertas (art. 19.º) – a crimes cujo sucesso da investigação esteja dependente da utilização de meios de obtenção de prova especiais previstos na LC, como é o caso de crimes cometidos através de um sistema informático e

[37] VERDELHO, Pedro, "A nova lei do Cibercrime", *cit.*, p. 717 e 718.
[38] NEVES, Rita Castanheira, *ob. cit.*, p. 268.

dos crimes cuja prova esteja armazenada num sistema digital, atribuindo, desta forma, à Lei do Cibercrime o estatuto de *pedra angular em matéria de prova.*[39/40]

Já no que toca às diligências processuais em si, a nova Lei, por um lado, criou novos meios de obtenção de prova, como a preservação expedita de dados armazenados num sistema informático, a preservação expedita e revelação de dados de tráfego e a injunção para apresentação ou concessão do acesso a dados (artigos 12.º a 14.º da LC) que transpõem as obrigações resultantes dos artigos 16.º a 18.º da CCiber, e, por outro, adaptou ao ambiente digital medidas processuais já existentes, mas inadequadas à nova realidade que se pretende regular – os clássicos regimes das buscas e das apreensões, como é o caso da apreensão de dados informáticos, a apreensão de correio eletrónico e registos de comunicações de natureza semelhante e a interceção de comunicações (artigos 16.º a 18.º da LC), também eles transposições das normas que constam dos artigos 19.º a 21.º da CCiber.[41]

Importa, desde já, alertar, na linha de pensamento de João Conde Correia, para o facto de que, por vezes, adaptar regimes clássicos a um novo contexto, isto é, adaptar o conhecido (soluções vigentes) ao desconhecido (novos problemas) pode não ser o melhor caminho.[42]

E que dizer da autonomização deste regime fora do nosso Código de Processo Penal?

Se, como vimos, graças ao amplo âmbito de aplicação conferido pelo art. 11.º às normas processuais da LC, a Lei do Cibercrime pode ser considerada um verdadeiro regime geral da prova digital, por que razão o legislador optou por consagrar diligências processuais aplicáveis a qualquer tipo de crime na lei sobre cibercriminalidade e não proceder a uma alteração no regime geral do nosso CPP, para o qual a mesma LC remete inúmeras vezes?

A Exposição de Motivos da LC tenta dar resposta a esta opção do legislador, apontando três ordens de razões: a tradição portuguesa, onde existem outros diplomas estruturantes de matérias na especialidade (*v.g.* criminalidade relacionada com estupefacientes e criminalidade fiscal); a inconveniência de plasmar regras especiais em diplomas estruturantes do ordenamento penal; e a conveniência prática, para os operadores

[39] A expressão é de CORREIA, João Conde, "Prova digital: as leis que temos e a lei que devíamos ter", *Revista do Ministério Público,* n.º 139, Jul/Set, 2014, p. 34.
[40] Como previamente referi, esta não foi uma inovação do nosso legislador, mas a reprodução, para o ordenamento interno, do art. 14.º da Convenção sobre Cibercrime do Conselho da Europa.
[41] VERDELHO, Pedro, "A nova lei do cibercrime*", cit.,* p. 734 e 735.
[42] CORREIA, João Conde, *ob. cit.,* p. 35.

judiciários, de ver sistematizados todos os normativos referentes a um setor específico da criminalidade.[43]

Todos estes argumentos foram refutados por Paulo Dá Mesquita. Relativamente ao argumento tradição, o autor reconhece que ela existe desde 1991 com a LCI, por se ter consagrado em lei extravagante normas de direito material. No entanto, para além da LC ser original no que toca a normas processuais, as legislações mencionadas na exposição de motivos são na verdade regras especiais relativas aos tipos de crime consagrados nesses diplomas, faltando-lhes o caráter geral que têm as diligências da LC que são aplicáveis a qualquer tipo de crime.

O que, por sua vez, deita por terra o terceiro argumento, visto que as normas em causa não se restringem a um "setor específico de criminalidade", pelo que seria até favorável para os operadores judiciários que não estejam inseridas em legislação que, à primeira vista, é dirigida a um "setor específico de criminalidade".

Já o segundo argumento é ultrapassado devido às regras em questão não serem normas especiais em sentido técnico-jurídico, mas sim meios de obtenção de prova em suporte digital, aplicáveis a um conjunto de crimes que vai para além dos catalogados nas escutas telefónicas do nosso CPP.

Terminando o autor por encarar o Capítulo III da LC como um *envergonhado* novo Capítulo V, que se deveria denominar "Da prova eletrónica", inserido no Título III que consagra os meios de obtenção de prova do CPP.[44]

A meu ver, a crescente utilização no processo penal da prova digital, em especial das mensagens de correio eletrónico e registos análogos, torna-a merecedora de um lugar ao lado dos restantes meios de prova, naturalmente dispostos no que é o nosso diploma legal fundamental em matéria de Direito Processual Penal.

Hoje continua sem se compreender por que motivo o legislador não inseriu estas diligências processuais de recolha de prova digital no nosso CPP, evitando, talvez assim, a dificuldade de harmonização com normas do próprio Código (artigos 179.º e 189.º)[45] e aproveitando, já agora, para proceder à revogação formal do art. 189.º do CPP, já que o art. 17.º da LC o substitui.

---

[43] Exposição de Motivos da Proposta de Lei n.º 289/X/4.ª, p. 3.
[44] MESQUITA, Paulo Dá, *ob. cit.*, p. 99-101.
[45] FIDALGO, Sónia, "Apreensão de correio eletrónico e utilização noutro processo das mensagens apreendidas", *Revista Portuguesa de Ciência Criminal*, n.º 1, IDPEE, 2019, p. 61.

De qualquer modo, ao introduzir regras especiais de recolha de prova em suporte eletrónico, esta foi uma Lei inovadora no ordenamento jurídico português, uma vez que, antes da sua entrada em vigor, a investigação de crimes relacionados com informática fazia-se recorrendo às regras gerais no CPP, [46] pois, pese embora já existir uma lei de nome Lei de Criminalidade Informática, dela só constavam normas substantivas que em nada auxiliavam a investigação dos crimes que tipificava.

4. Regime da apreensão de correio eletrónico e registos de comunicação de natureza semelhante

O art. 17.º da LC dispõe *"quando, no decurso de uma pesquisa informática ou outro acesso legítimo a um sistema informático, forem encontrados, armazenados nesse sistema informático ou noutro a que seja permitido o acesso legítimo a partir do primeiro, mensagens de correio eletrónico 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 de correspondência previsto no Código de Processo Penal".* Suscitando dificuldades de compatibilização com o consagrado no nosso CPP, a interpretação deste regime está longe de ser consensual entre a doutrina e a jurisprudência portuguesas.

Antes de mais, não posso deixar de esclarecer que a aplicação do art. 17.º da LC está dependente da forma como as comunicações chegam ao conhecimento das instâncias de controlo. A *ratio* da intervenção judicial na determinação de um meio de obtenção de prova, seja ela *a priori* ou *a posteriori*, radica no caráter intrusivo deste meio de obtenção de prova, pelo que o art. 17.º da LC só tem lugar se a apreensão de e-mails e registos análogos for coercivamente encetada. Por conseguinte, ficam de fora tanto a comunicação eletrónica voluntariamente disponibilizada, como a comunicação eletrónica publicamente acessível.[47]

---

[46] FIDALGO, Sónia, *ob. cit.*, p. 59.

[47] SILVA, Flávio Manuel Carneiro da, AA.VV., *Meios de obtenção de prova e medidas cautelares e de polícia.* Lisboa: Centro de Estudos Judiciários, 2019, p. 21-25 e 31. *Ebook* disponível em http://www.cej.mj.pt/cej/recursos/ebooks/penal/eb_MeiosProva.pdf [acedido a 10 de julho de 2020].

No primeiro caso, o TRP no Ac. de 03.04.2013[48/49] considerou que SMS recebidas no telemóvel da ofendida e por ela disponibilizadas de forma espontânea são um meio de prova válido que não requer qualquer validação judicial por ter sido fornecido por quem é o seu legítimo detentor;[50]

No segundo caso, relativamente a publicações em redes sociais, pode-se ler no Ac. do TRP de 13.04.2016[51] que "*uma publicação realizada pelo arguido no mural do seu perfil do Facebook (…) não reveste o carácter de comunicações semelhante a correio eletrónico na medida em que foi colocado pelo próprio num perfil, público, acessível, livre e indiscriminadamente a qualquer pessoa".* Considerando-se um mero documento, está sujeito aos mecanismos dos n.os 1 e 3 do art. 16.º da LC.

Outro ponto que me compete clarificar é o alcance do preceito *"Quando, no decorrer de uma pesquisa informática, ou outro acesso legítimo a um sistema informático (…)".* Se, quanto à primeira parte, não restam dúvidas – está em causa uma pesquisa informática nos termos do art. 15.º da LC –, quanto à segunda parte ("ou outro acesso legítimo a um sistema informático") sustento-me no entendimento de Rui Cardoso que inclui aqui tanto as perícias (quando realizadas antes da apreensão) como o acesso aos dados que estejam na disponibilidade ou controlo de outra entidade, por esta concedido (previsto no n.º 1 do art. 14.º da LC e nunca no art. 18.º, pois este aplica-se aos dados em trânsito).[52]

Chamo, ainda, a atenção para o facto destas mensagens terem de estar *armazenadas* no suporte eletrónico, o que pressupõe que as mesmas já não se encontram "em trânsito", sendo que para a interceção em tempo real de e-mails e registos análogos aplica-se o disposto nos artigos 187.º e 188.º do CPP, que consagra o regime das escutas telefónicas, a tudo o que não for contrariado pelo art. 18.º da LC, que estipula a interceção das comunicações, por força da remissão deste último.[53]

---

[48] Disponível em http://www.dgsi.pt/jtrp.nsf/d1d5ce625d24df5380257583004ee7d7/d21c6752627b971780257b4f003caa5d [acedido a 10 de julho de 2020].

[49] Neste sentido também TRL 29.03.2012 ou TRP 20.01.2016. Ambos disponíveis em www.dgsi.pt [acedidos a 10 de julho de 2020].

[50] Recentemente, o TRL no Ac. 21.02.2019 considerou que a nulidade decorrente da apreensão de e-mails sem autorização judicial pode ser sanada com autorização, *a posteriori*, da sua leitura, pelo titular do direito ao sigilo da correspondência. Disponível em www.dgsi.pt [acedido a 12 de julho de 2020].

[51] Disponível em http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/ef54d51d3972157d80257fa4002e2d75 [acedido a 11 de julho de 2020].

[52] Veja-se CARDOSO, Rui, *ob. cit.*, p. 170, 171 e 179*;* RAMALHO, David Silva, *ob. cit.*, p. 134-140 e 268-270.

[53] Acrescento o entendimento de Rui Cardoso, nos termos do qual a interceção em tempo real de comunicações de natureza semelhante realizadas via serviço telefónico (SMS, EMS, MMS) se deve fazer segundo as regras

4.1. Direitos fundamentais restringidos

Apesar do elevado valor probatório das mensagens eletrónicas, a sua utilização em processos penais implica uma séria invasão estadual na esfera constitucionalmente protegida dos direitos, liberdades e garantias do cidadão. Não descurando a importância da tutela dos mesmos, limitar-me-ei a abordá-los na estrita medida em que se relacionam com a problemática da minha investigação.

O direito à privacidade encontra-se plasmado no n.º 1 do art. 26.º da CRP que reconhece o direito à identidade pessoal, ao desenvolvimento da personalidade e à reserva da intimidade da vida privada e familiar. Não obstante a dificuldade de delimitação da esfera da privacidade,[54] entende-se hoje que a salvaguarda do direito à privacidade significa tanto a proibição de intromissão estatal e social na esfera de intimidade do indivíduo como, mesmo que essa intromissão tenha sido permitida pelo mesmo, a proibição da divulgação do que é próprio dessa esfera. Tem sido esta a posição do nosso Tribunal Constitucional desde o Ac. n.º 128/92, de 01.04.1992,[55] onde afirma fazerem parte do direito à privacidade, "a vida pessoal, a vida familiar, a relação com outras esferas de privacidade (*v.g.* a amizade), o lugar próprio da vida pessoal e familiar (o lar ou domicílio), *e bem assim os meios de expressão e de comunicação privados (a correspondência, o telefone, as conversas orais, etc.)".*

O advento tecnológico, que trouxe consigo novos meios de intromissão na intimidade do cidadão, tornou premente alargar o âmbito de proteção da privacidade, surgindo, nas palavras de Rita Castanheira Neves, *uma espécie de privacidade informática,* com um âmbito de proteção próprio (distinto do direito à privacidade), pretendendo-se aqui *proteger o indivíduo nos momentos informatizados de recolha, armazenamento, utilização e transmissão dos seus dados pessoais.*[56]

Denominado direito à autodeterminação informacional, encontra-se consagrado no art. 35.º da CRP e implica: o direito a acedermos aos nossos dados informatizados e de

---

dos artigos 187.º e 188.º do CPP que consagram o regime das escutas telefónicas, ao passo que a interceção em tempo real de mensagens de correio eletrónico, de *WhatsApp*, *Messenger*, *Skype*, etc., deve seguir o indicado no art. 18.º da LC. (Cfr. CARDOSO, Rui, *ob. cit.*, p. 182 e 183). Uma vez que que o n.º 1 do art. 187.º do CPP é expresso no que toca àquela diligência se aplicar a "conversações ou comunicações telefónicas", concordo com esta destrinça.

[54] *Vd.* NEVES, Rita Castanheira, *ob. cit.*, p. 37-45.

[55] Disponível em https://www.tribunalconstitucional.pt/tc/acordaos/19920128.html [24 de abril de 2020].

[56] NEVES, Rita Castanheira, *ob. cit.*, p. 58; Mais desenvolvimentos acerca do direito à autodeterminação informacional em RODRIGUES, Benjamim Silva, *Das escutas telefónicas – à obtenção da prova [em ambiente] digital*, Tomo II, 2.ª Edição, Coimbra Editora, 2008, p. 255-271.

conhecer a finalidade do tratamento dos mesmos; a proibição do tratamento de dados pessoais respeitantes a convicções filosóficas, políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica (salvo determinadas exceções); a proibição de acedermos a dados pessoais de outrem; e a proibição de atribuição de um número nacional único aos cidadãos. Este direito tem vindo a ser entendido, a par do direito à solidão ("pretensão de isolamento, tranquilidade e exclusão do acesso dos outros a si próprio") e do direito ao anonimato ("impedimento à ingerência dos outros"), como uma das três manifestações do direito à reserva sobre a intimidade da vida privada, relevante no presente trabalho por se traduzir na concretização do direito à privacidade no campo das novas tecnologias.[57]

Como defende o mesmo Acórdão do TC, *as comunicações privadas, englobando o conteúdo e o circunstancialismo em que as mesmas têm lugar, são reconhecidas como um meio através do qual se manifestam aspetos da vida privada da pessoa e que, por isso, caem no âmbito de proteção constitucional da reserva da vida privada.*

Uma vez que na apreensão de e-mails e registos semelhantes estão em causa comunicações eletrónicas e que, não raras vezes, o conteúdo das mesmas traduz-se na palavra, escrita ou falada, das partes envolvidas na comunicação, merece referência no presente capítulo o direito à palavra a que o n.º 1 do art. 26.º da CRP alude.

A doutrina tem sido da opinião de que este artigo diz respeito à palavra falada e não à palavra escrita,[58] pela convicção de que a primeira requer uma maior proteção dada a sua volatilidade e expetativa de quem a profere de que a mesma não seja reproduzida fora do círculo de pessoas, naquele exato momento e local, com quem, onde e quando se decidiu partilhar a palavra, ao passo que a palavra escrita, quando ganha forma no mundo real fica *perpetuada*, não obstante merecer, ainda que de forma mais atenuada, tutela legal. A tutela legal da palavra escrita no uso do correio eletrónico e registos semelhantes, no momento em que as mensagens deixam de ser comunicação, dá-se, assim, não em sede do art. 26.º da CRP

[57] Veja-se, a título de exemplo, o Ac. do TC n.º 403/2015, de 17.09.2015. Disponível em https://dre.pt/home/-/dre/70300353/details/maximized?p_auth=OsYd65lz [acedido a 24 de abril de 2020].

[58] Gomes Canotilho e Vital Moreira distinguem três direitos que se encontram aqui abrangidos, designadamente, o direito à voz, atributo de personalidade para cujo registo e/ou divulgação é necessário o consentimento da pessoa, o direito às "palavras ditas", pretendendo-se salvaguardar a autenticidade e o rigor da reprodução das mesmas e o direito ao auditório, traduzindo-se este no direito da pessoa que profere as palavras a decidir a que pessoas as quer transmitir (Cfr. CANOTILHO, José Gomes; MOREIRA, Vital, *Constituição da República Portuguesa Anotada*, Vol. I, 4.ª Edição Revista, Coimbra Editora, 2014, p. 467); E ainda ANDRADE, Manuel da Costa, *Sobre as proibições de prova em processo penal*, Reimpressão, Coimbra Editora, 2013, p. 70 e 71.

(que se entende apenas abranger a palavra falada), mas sim no âmbito do direito à autodeterminação informacional que consta no art. 35.º da CRP, enquanto proteção da privacidade no meio informático.[59]

Porém, o correio eletrónico e registos semelhantes pode conter tanto palavra escrita como falada, como é o caso, por exemplo, de uma chamada feita via *Skype*, fazendo aqui todo o sentido tutelar a palavra como palavra falada e já não como escrita, caindo então no âmbito de proteção do art. 26.º da CRP, independentemente de se ter transmitido virtualmente. [60/61]

Em jeito de conclusão, embora no âmbito de uma apreensão de correio eletrónico e registos de semelhantes o acesso aos dados informáticos não seja indiscriminado, tendo de incidir apenas sobre os dados que sejam *necessários para a descoberta da verdade ou para a prova*, estes são dados altamente pessoais e, portanto, legalmente protegidos da devassa alheia pela nossa Lei Fundamental, tanto através do direito à autodeterminação informacional que decorre do direito à privacidade, como do direito à palavra (virtual), escrita ou falada, transmitida via comunicação eletrónica.[62]

Estamos perante um clássico exemplo da *natureza conflitual* do processo penal, já há muito desenvolvida por Jorge de Figueiredo Dias, traduzindo-se no *conflito entre o dever geral do Estado de realização de um processo penal eficiente, capaz de em tempo côngruo*

---

[59] NEVES, Rita Castanheira, *ob. cit.* P. 46 e 47.

[60] Nestes termos, NEVES, Rita Castanheira, *ob. cit.* p. 50.

[61] José de Faria Costa distingue a palavra virtual das restantes palavras escrita e falada: *"A palavra, compreendida agora como depositária de informação, não é só palavra escrita, nem tão-pouco palavra à distância: já é – e de maneira absolutamente indesmentível – a palavra virtual. (…) A informatização em rede, veio trazer a possibilidade de a palavra não ser escrita nem falada, estar virtualmente visível em um écran por força de um jogo complexo cingido à simples lógica binária. O que permite a possibilidade de a palavra estar e não estar e, todavia, se se quiser, estando ou não estando, trazê-la ao mundo normal da palavra escrita em suporte papel"*. (Cfr. COSTA, José de Faria "As telecomunicações e a privacidade: o olhar (in)discreto de um penalista", *Direito Penal da Comunicação – Alguns escritos*, Coimbra Editora, 1998, p. 56); Também Catarina Sarmento e Castro se refere à palavra virtual que *assume um papel especial quando falamos de correio eletrónico. Através dela são definidos os conteúdos de cada mensagem, de que é possível retirar variadíssimas informações que podem ajudar a conhecer aspetos significativos do seu emissor e recetor. Por outro lado, o controlo da utilização do correio eletrónico permite saber quem contactou quem, quando e acerca de que assunto."* (Cfr. CASTRO, Catarina Sarmento e, "O direito à autodeterminação informativa e os novos desafios gerados pelo direito à liberdade e à segurança no pós 11 de setembro", *Estudos de Homenagem ao Conselheiro José Manuel Cardoso da Costa*, Vol. II, Coimbra Editora, 2005, p. 86).

[62] Recentemente, ao direito ao esquecimento na Internet, afirmado pela primeira vez pelo TJUE, no Ac. *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González,*, de 13.05.2014, que pode ser consultado em https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131 [acedido a 16 de julho de 2020], tem agora consagração expressa no Regulamento (EU) 2016/679, do Parlamento Europeu e do Conselho (art. 17.º).

alcançar decisões justas dos casos da vida, e o não menos indeclinável dever estadual de proteção das liberdades fundamentais da pessoa.[63]

Estará igualmente aqui em causa o direito à inviolabilidade das comunicações, outro direito chamado muitas vezes à colação por justificar a atribuição à apreensão da correspondência de um regime mais garantístico do que o que é aplicado à apreensão de outros objetos? Esta é a próxima questão que se impõe e à qual procurarei dar resposta *infra*.

4.2. O que se entende por correio eletrónico e delimitação de "registos de comunicações de natureza semelhante"

Na Lei do Cibercrime, não obstante incluir um artigo de epígrafe "definições", o legislador não define o que é correio eletrónico, tão-pouco esclarece o que são registos de comunicações de natureza semelhante, a que alude no art. 17.º.

Segundo o Direito da União Europeia, correio eletrónico é *"qualquer mensagem textual, vocal, sonora ou gráfica enviada através de uma rede pública de comunicações que pode ser armazenada na rede ou no equipamento terminal do destinatário até o destinatário a recolher".*[64] Apesar da expressão *"qualquer mensagem (…) que pode ser armazenada na rede ou no equipamento terminal do destinatário"* ser bastante ampla, podendo caber aqui mensagens que não se subsumem no conceito de correio eletrónico (como um comentário deixado num blog, ou uma fotografia que se publique online),[65] é este o conceito legal de e-mail adotado no nosso ordenamento jurídico na al. *b)* do n.º 1 do art. 2.º da Lei n.º 41/2004, de 18 de agosto, na redação que lhe foi dada pela Lei n.º 46/2012, de 29 de agosto.

Na doutrina nacional, ressalto duas definições pela sua clareza e simplicidade, designadamente a de Armando Dias Ramos que o descreve como um *"programa informático que permite a comunicação instantânea, de modo diferido, entre quem a envia e quem a recebe, através das redes de informação e comunicação, independentemente do local em que estes se encontrem, sem a necessidade deste se encontrar instalado no*

[63] DIAS, Jorge de Figueiredo, "Revisitação de algumas ideias-mestras da teoria das proibições de prova em processo penal (também à luz da jurisprudência constitucional portuguesa)", *Revista de Legislação e de Jurisprudência*, n.º 146, 2016, p. 9.
[64] Al. *h)* do art. 2.º da Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas.
[65] RAMOS, Armando Dias, *A Prova Digital em Processo Penal, cit.*, p. 29 e 30.

computador";[66] e o entendimento de Rui Cardoso segundo o qual o correio eletrónico traduz-se em mensagens transmitidas via *Internet*,[67] através de servidores de correio eletrónico, entre duas pastas, a do remetente, quem envia ou encaminha a mensagem, e a do destinatário, quem acede à sua pasta no seu servidor de correio eletrónico e aí a lê (mantendo-a ou arquivando-a) ou descarrega-a para um programa de correio eletrónico no seu sistema informático.[68]

Já o alcance da parte do art. 17.º que dispõe "registos de comunicações de natureza semelhante" revela-se mais obscuro.[69]

Se interpretarmos o preceito de forma literal, podemos ser levados a considerar que, relativamente às comunicações de natureza semelhante, o art. 17.º da LC respeita apenas aos seus dados de tráfego. Enquanto a expressão "mensagens de correio eletrónico" dá a entender que se refere ao conteúdo das mensagens, o termo "registos" para se referir às "comunicações de natureza semelhante" parece, à primeira vista, dizer apenas respeito à ocorrência das comunicações e não ao seu conteúdo. No entanto, não é plausível excluir o conteúdo das mensagens de natureza semelhante, caso contrário, estaríamos perante uma incoerência da tutela de direitos, conferindo maior proteção à apreensão dos dados de tráfego das comunicações (que fica dependente de decisão judicial e do critério de exigência de grande interesse para descoberta da verdade ou para a prova) do que ao próprio conteúdo (sendo apenas necessária decisão do MP e bastando qualquer interesse para a prova).

As comunicações de natureza semelhante podem ser feitas via serviço telefónico, em que o utilizador se encontra identificado pelo seu número de telefone, estando aqui incluídas as SMS *(short message service)*, as EMS *(enhanced messaging service)* e as MMS *(multimedia messaging service*); como também via Internet, utilizando para tal um conjunto de protocolos TCP (*transmission control protocol*) ou IP (*Internet Protocol*),[70] que atribuem ao utilizador um endereço IP (que muito sucintamente é o que identifica um computador ou servidor), abrangendo tanto as comunicações por IM (*Instant Messenger*), como por *Chatrooms*. Nos primeiros, as comunicações por mensagens instantâneas, estamos a falar

[66] RAMOS, Armando Dias, *A Prova Digital em Processo Penal, cit.*, p. 31 e 32;.
[67] Ou via *Intranet:* Rede de computadores privada de uso exclusivo de um determinado local por determinadas pessoas (*v.g.* rede de uma empresa).
[68] CARDOSO, Rui, *ob. cit.*, p. 181.
[69] Acompanho de perto a delimitação feita por CARDOSO, Rui, *ob. cit.*, 181-183.
[70] Para uma explicação mais detalhada sobre o funcionamento destes protocolos, consultar RAMALHO, David, *ob. cit.*, p. 52-56.

em programas como o *Skype, Facebook, WhatsApp, Snapchat, Telegram*, entre outros, que permitem o envio e receção instantâneos de mensagens em tempo real, não exigindo ao seu destinatário qualquer ato que não o de ter o seu sistema informático ligado, sendo que normalmente estas mensagens ficam automaticamente armazenadas nos sistemas informáticos dos intervenientes na comunicação, suscetíveis de ser apreendidas. Quanto aos segundos, antigamente feitos através de programas próprios como o IRC (*Internet Relay Chat*) e hoje em dia em desuso dada a popularidade das mensagens instantâneas, são locais *online,* públicos ou privados, onde duas ou mais pessoas podem trocar mensagens e ficheiros, utilizados lícita, mas também ilicitamente, neste último caso, por exemplo, costumando muitas vezes ser o palco de redes de partilha de pornografia infantil. [71]

Destas mensagens de correio eletrónico e registos semelhantes fazem parte os dados de conteúdo e os dados de tráfego. Os primeiros não necessitam de grandes esclarecimentos – traduzem-se no conteúdo da comunicação em si, isto é, a mensagem, o documento, a imagem, etc., que é transmitida. Já a definição de dados de tráfego mereceu consagração na própria LC que os define como *"dados informáticos relacionados com uma comunicação efetuada por meio de um sistema informático, gerados por este sistema como elemento de uma cadeia de comunicação, indicando a origem da comunicação, o destino, o trajeto, a hora, a data, o tamanho, a duração ou o tipo do serviço subjacente".* [72]

Nas palavras de Rui Cardoso devem ser aqui incluídas todas as comunicações, mais propriamente, "*dados informáticos que constituam correio eletrónico ou registos de comunicações de natureza semelhante"* independentemente do seu conteúdo ser, ou não, privado (*v.g.* publicidade) desde que trocadas entre pessoas e nunca entre máquinas. Por outro lado, o autor exclui outros dados armazenados no sistema, ainda que transmitidos via e-mail ou registos de natureza semelhante.[73] Exclusão esta que no meu ponto de vista faz todo o sentido: imagine-se o pesadelo que seria para os OPC terem de apurar, em relação a cada documento encontrado num sistema eletrónico mas dissociado de qualquer comunicação eletrónica (cuja apreensão segue os trâmites do art. 16.º da LC), se o mesmo

[71] CARDOSO, Rui, *ob. cit*., p. 182 e 183.
[72] Al. *c)* do art. 2.º da LC, transposição para o nosso ordenamento jurídico da al. *d)* do art. 1.º da CCiber.
[73] Encontradas faturas eletrónicas de serviços de telecomunicações, mesmo que detalhadas (lista de telefonemas feitos e mensagens enviadas), armazenadas no sistema informático, mas separadas da mensagem que as transmitiu, Rui Cardoso defende que devem ser consideradas dados informáticos iguais aos restantes ali armazenados. Exatamente como acontece às faturas recebidas em papel por correio tradicional: depois da carta ser aberta, a fatura é um documento igual a qualquer outro. Cfr. CARDOSO, Rui, *ob. cit.*, p. 180.

teve origem numa qualquer comunicação eletrónica para, nesse caso, ser sujeito ao regime do art. 17.º da LC (tendo presente que nem sempre é possível proceder a tal rastreio).

4.3. Âmbito de aplicação

Relativamente ao âmbito objetivo, enquanto na apreensão de correspondência estão em causa *cartas, encomendas, valores, telegramas ou qualquer outra correspondência*, desde que se encontre em trânsito ou, mesmo que já chegada à esfera do destinatário, ainda não tenha sido aberta (cfr. n.º 1, art. 179.º do CPP); no artigo 17.º da LC estamos perante mensagens de correio eletrónico e registos semelhantes (nos termos que defini e delimitei no capítulo anterior) sem que haja uma diferenciação de tratamento entre mensagens abertas e lidas das mensagens fechadas e não lidas[74] que forem encontradas decurso de uma pesquisa informática ou outro acesso legítimo a um sistema informático.

Para além disso, o regime de apreensão de correspondência sofre uma redução no seu âmbito objetivo pela al. *b)* do art. 179.º do CPP, segundo a qual este meio de obtenção de prova só será admissível em crimes puníveis *com pena de prisão superior, no seu máximo, a 3 anos.* Contudo, nem a própria LC pune com pena de prisão superior a 3 anos alguns dos tipos legais que prevê,[75] nem esta é uma exigência no atual[76] regime de apreensão de correio eletrónico e registos semelhantes, por força do art. 11.º da LC. Este, de epígrafe "Âmbito de aplicação das disposições processuais", possibilita a aplicação das mesmas a crimes em relação aos quais seja necessário a recolha probatória em suporte eletrónico, isto é, este meio de obtenção de prova não se encontra dependente de um catálogo de crimes, podendo-se aplicar relativamente a *qualquer crime*.[77]

---

[74] Não obstante a crítica de alguma doutrina, inclusive decisões judiciais, no sentido da necessidade de distinguir correio eletrónico lido e não lido que abordarei de seguida.

[75] É o caso do dano relativo a programas ou outros dados informáticos (n.os 1 e 3 do art. 4.º), do acesso ilegítimo a sistema informático (n.os 1, 2 e 3 do art. 6.º), da interceção ilegítima de dados informáticos (n.os 1 e 3 do art. 7.º) e a reprodução ilegítima de programa protegido (n.os 1 e 2 do art. 8.º).

[76] Antes da entrada em vigor da LC, segundo o regime das escutas telefónicas aplicado por remissão do art. 189.º do CPP, a apreensão de correio eletrónico estava sujeita a um catálogo de crimes previsto no n.º 1 do art. 187.º do CPP, catálogo este que só incluía crimes com pena de prisão superior, no seu máximo, a 3 anos, pelo que ficavam de fora desta diligência processual a maior parte dos crimes tipificados na antiga Lei n.º 109/91.

[77] Sobre a aplicação geral das medidas processuais da LC, *vd.* NEVES, Rita Castanheira, *ob. cit.*, p. 274; MESQUITA, Paulo Dá, *ob. cit.*, p. 108 e ss.; FIDALGO, Sónia, *ob. cit.*, p. 65; e ainda, a título de exemplo, Ac. do TRE de 20.01.2015, disponível em www.dgsi.pt. [acedido a 5 de fevereiro de 2020].

Todavia, à semelhança de Sónia Fidalgo, tenho dúvidas quanto à intenção do legislador ser a de permitir a apreensão de e-mails e registos análogos em qualquer processo penal *independentemente da gravidade do crime investigado.*[78] Ora, como qualquer meio de obtenção de prova, a apreensão de emails e registos semelhantes está vinculada a um dos princípios balizadores da atividade probatória: o princípio da proporcionalidade. O art. 17.º da LC, suscetível de ferir direitos fundamentais pessoalíssimos do indivíduo, convoca um sopesar de interesses entre o prejuízo que implica (a violação da privacidade) e o bem jurídico que se visa tutelar na busca pela verdade material. Assim, fazendo funcionar o disposto no n.º 2 do art. 18.º da CRP que estipula que a limitação de DLG seja feita na medida do estritamente necessário para salvaguardar outros direitos constitucionais, conjugado com o n.º 8 do art. 32.º da CRP onde se consagra a proibição de prova que resulte de uma intromissão abusiva nas telecomunicações, considero que a gravidade do crime que se imputa ao arguido deve relevar no despacho sobre a admissibilidade da apreensão de e-mails e registos semelhantes. Haverá casos em que o bem jurídico em questão, (alegadamente) ameaçado por um delito menos grave, não é suficiente para justificar o sacrifício do direito à autodeterminação informacional e do direito à palavra.

No que toca ao âmbito de aplicação subjetivo, apesar de na al. *a)* do art. 179.º do CPP constar que a correspondência alvo deste meio de obtenção de prova tem de ter sido e*xpedida pelo suspeito ou lhe é dirigida, mesmo que sob nome diverso ou através de pessoa diversa,* no caso da apreensão de e-mails e registos semelhantes, o artigo 11.º da LC que regula o âmbito de aplicação não faz qualquer restrição ao seu âmbito subjetivo, pelo que, na opinião de Rui Cardoso, este regime deve aplicar-se a qualquer pessoa, uma vez que o art. 11.º da LC é a transposição do art. 14.º da CCiber e a lei nacional deve, por força do n.º 2 do art. 18.º da CRP, ser interpretada e aplicada de acordo com a Convenção.[79]

Também Pedro Verdelho considera que o requisito da al. *a)* do art. 179.º do CPP não é exigido no caso da apreensão de correio eletrónico e registos semelhantes, uma vez que o legislador, dos três requisitos consagrados no n.º 1 do art. 179.º do CPP, apenas transcreveu para o art. 17.º da LC o requisito de grande interesse para a descoberta da verdade e para a prova que consta da al. *c)* e a opção pela não consagração no art. 17.º da

[78] FIDALGO, Sónia, *ob. cit.,* p. 66.
[79] CARDOSO, Rui, *ob. cit.,* p. 192.

LC das alíneas *a)* e *b)* deve levar o intérprete a entender que a intenção do legislador era deixar as mesmas de fora.[80]

Na verdade, o TRL no Ac. 08.05.2018[81] pronunciou-se no sentido de deferir a apreensão de *quaisquer objetos relacionados com um crime ou que possam servir de prova*, ainda que em poder de ou pertencentes a terceiros, incluindo a conta e-mail de terceiro não suspeito, se tal apreensão se revelar proporcional e imperativa, face aos elementos recolhidos no local.

Entendimento diferente é o de Rita Castanheira Neves e Duarte Rodrigues Nunes, que, ao enumerarem os requisitos que o regime de apreensão de correio eletrónico e registos semelhantes deve observar, vêm defender que a remissão deste regime para o da apreensão de correspondência, embora não abranja a exigência de estarmos perante crimes puníveis com pena de prisão superior a 3 anos, abrange a exigência de ter sido enviado ou recebido pelo suspeito, mesmo que de endereço eletrónico de pessoa diversa, tal como se encontra disposto na al. *a)* do art. 179.º do CPP.[82]

Não sendo a lei totalmente clara quanto a este ponto, não me parece que o simples facto de o legislador ter deixado de fora a al. *a)* do n.º 1 do art. 179.º do CPP aquando da formulação do art. 17.º da LC, seja suficiente para se poder concluir, *per se*, que a sua intenção fosse a de não aplicar o requisito legal aqui consagrado à apreensão de e-mails e registos semelhantes, uma vez que a última parte do art. 17.º remete para o regime da apreensão de correspondência que consta do CPP, da qual faz parte a exigência da al. *a)*, não havendo nenhuma norma que afaste expressamente a sua aplicação.

Já o n.º 2 do art. 179.º do CPP reduz o âmbito subjetivo desta diligência processual quando se estipula a proibição de apreensão de correspondência entre o arguido e o seu

---

[80] VERDELHO, Pedro, "A nova lei do cibercrime", *cit.*, p. 745 e 746.
[81] Disponível em http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/e48d47e75466b9da802582b00053061e [acedido a 6 de setembro de 2020].
[82] NEVES, Rita Castanheira, *ob. cit.*, p. 274; no mesmo sentido NUNES, Duarte Rodrigues, *ob. cit.*, p. 151.

defensor, a menos que o juiz tenha fundadas razões para crer que aquela constitui objeto ou elemento de um crime.[83/84]

No que diz respeito ao requisito que consta da al. *c)* do art. 179.º do CPP para a apreensão de correspondência, sendo ele o *grande interesse para a descoberta da verdade ou para a prova*, encontra-se expressamente consagrado no próprio art. 17.º da LC, pelo que a sua aplicação à apreensão de e-mails e semelhantes se afigura indiscutível. A escolha pelo "grande interesse" ao invés do simples "interesse" leva-me a crer que o juiz deve levar a cabo uma cautelosa ponderação das necessidades da investigação em virtude da danosidade para os DLG que tal meio de obtenção de prova acarreta.

Em suma, sou da opinião de que tanto a al. *a)* (correspondência expedida pelo suspeito ou lhe é dirigida) como a al. *c)* (grande interesse para a descoberta da verdade ou para a prova) do n.º 1 do art. 179.º do CPP se devem aplicar à apreensão de e-mails e semelhantes, ficando unicamente de fora a exigência estipulada na al. *b)* (crime punível com pena de prisão superior, no seu máximo, a 3 anos) do art. 179.º do CPP, em razão da al. *c)* do art. 11.º da LC.

4.4. O Princípio da inviolabilidade da comunicação e a exequibilidade da distinção entre mensagens lidas e não lidas

O princípio da inviolabilidade das comunicações encontra-se estabelecido na nossa Lei Fundamental no n.º 1 do seu art. 34.º, de epígrafe "Inviolabilidade do domicílio e da correspondência", segundo o qual *o domicílio e o sigilo da correspondência e dos outros meios de comunicação privada são invioláveis.* No entanto, o Estado que proíbe que ele

[83] Rodrigo Santiago apelida estes profissionais de "confidentes necessários" para se referir às atividades profissionais às quais *as pessoas se veem obrigadas a recorrer por força das suas próprias incapacidades ou insuficiências*, como é o caso do advogado, do médico, do bancário, do padre, etc. (cfr. SANTIAGO, Rodrigo, "Considerações acerca do regime estatutário do segredo profissional dos advogados", *Revista da Ordem dos Advogados*, Ano 57, 1, 1997, p. 230);
Mais informações sobre a proteção das esferas do segredo na apreensão de e-mails e semelhantes em NEVES, Rita Castanheira, *ob. cit.*, p. 287-307; e também NUNES, Duarte Rodrigues, *ob. cit.*, p. 151 e 152.
[84] Acerca do grau de envolvimento do advogado no crime para deixar de se aplicar a proibição do n.º 2 do 179.º do CPP, ver ANDRADE, Manuel da Costa, "Sobre o regime processual penal das escutas telefónicas", *Revista Portuguesa de Ciência Criminal*, Ano I, 3, Jul/Set, 1991, Aequitas, p. 388-396 e ALBUQUERQUE, Paulo Pinto de, *Comentário do Código de Processo Penal: à luz da Constituição da República e da Convenção dos Direitos do Homem*, 4.ª Edição, Universidade Católica Editora, 2011, p. 527.

mesmo[85] interfira nas comunicações dos seus cidadãos, vem de seguida, no n.º 4 do mesmo artigo, defender a possibilidade de que, às mãos do próprio Estado, haja uma limitação à garantia de não ingerência nas comunicações, no âmbito do processo penal: "é proibida toda a ingerência das autoridades públicas na correspondência, nas telecomunicações e dos demais meios de comunicação, *salvos os casos previstos na lei em matéria de processo criminal".*

É esta exceção constitucional à inviolabilidade da correspondência que está na base da admissão de meios de obtenção de prova como a apreensão de correspondência ou as escutas telefónicas, não obstante os regimes dos mesmos fazerem-se depender de rígidos requisitos, cumprindo o disposto no n.º 2 do art. 18.º da Constituição que exige que a restrição aos DLG se faça na medida do estritamente necessário e sempre respeitando o princípio da reserva de lei.[86]

Como defendem Gomes Canotilho e Vital Moreira no seu comentário ao art. 34.º da CRP, "*o direito ao sigilo da correspondência e de outros meios de comunicação privada tem como objeto de proteção a comunicação individual",* abrangendo assim toda a espécie de correspondência de pessoa para pessoa (cobrindo mesmo as hipóteses de encomendas que não contêm qualquer comunicação escrita) e todas as telecomunicações (incluindo não apenas o seu conteúdo mas também os dados de tráfego), onde naturalmente se insere o correio eletrónico e mensagens semelhantes, ficando de fora as informações dirigidas através, por exemplo, dos média, via rádio ou televisão, que se destinem a uma generalidade de indivíduos. Este direito implica, por um lado, a proibição de devassa das comunicações privadas e, por outro, o direito de que terceiros que tenham acesso às mesmas não as divulguem, dever este que impende sobretudo sobre aqueles que, por motivos funcionais, como empregados de serviços telefónicos, têm acesso às comunicações, nascendo daqui um dever de segredo profissional.[87]

---

[85] É, desde já, necessário referir que apesar deste artigo aludir somente às "autoridades públicas", o n.º 1 do art. 18.º da CRP vem esclarecer que *os preceitos constitucionais respeitantes aos DLG são diretamente aplicáveis e vinculam as entidades públicas e privadas* e o art. 194.º do CP criminaliza a ingerência na correspondência tradicional ou nas telecomunicações, seja por quem for, pelo que, por maioria de razão, o dever de não devassar a correspondência ou telecomunicação de outrem impõe-se não só na relação do Estado com o cidadão mas também aos cidadãos entre si.

[86] NEVES, Rita Castanheira, *ob. cit.*, p. 55.

[87] CANOTILHO, José Gomes; MOREIRA, Vital, *Constituição da República Portuguesa Anotada*, *ob. cit.*, 2014, p. 544 e ss.

O direito ao respeito pela correspondência encontra consagração expressa no n.º 1 do art. 8.º da Convenção Europeia dos Direitos Humanos, sendo que o Tribunal Europeu dos Direitos Humanos tem considerado que a correspondência aqui em causa tem um amplo escopo onde se incluem mensagens eletrónicas como o e-mail, o uso da internet, dados armazenados em servidores informáticos ou noutros suportes.[88]

Na esteira do pensamento de Manuel da Costa Andrade, sustentado pelo que tem vindo a ser o entendimento do Tribunal Constitucional Federal Alemão (*Bundesverfassungsgericht)*, o princípio da inviolabilidade das comunicações tem como objetivo proteger o que o BVerfG entende por *"privacidade à distância"*: estamos perante uma comunicação entre pessoas que, por se encontrarem separadas no espaço, estão dependentes de um terceiro que fornece serviços de comunicação à distância, ao qual, irremediavelmente, confiam tanto o conteúdo como os dados de tráfego que nascem com a comunicação, uma vez que as partes que comunicam não estão em condições de controlar a sua confidencialidade, pelo que o objetivo desta tutela jurídica é colocar as partes, na medida do possível, na situação igual à que estariam se estivessem a comunicar presencialmente.

O autor defende, assim, que este princípio fundamental assenta na *"específica situação de perigo"* a que as partes envolvidas na comunicação se encontram expostas, decorrente do domínio que o terceiro detém – e, portanto, somente *enquanto* o detém – sobre a comunicação, sendo o propósito aqui proteger as partes das empresas de serviços de comunicação e nunca a confiança entre os interlocutores.

Posto que este princípio fundamental está vinculado ao *processamento da comunicação sob o domínio da empresa fornecedora do serviço de telecomunicações,* a tutela do sigilo das comunicações só existe durante o processo de comunicação à distância, que, por sua vez, termina no momento em que o e-mail entra na esfera de domínio do destinatário (que para Manuel da Costa Andrade equivale ao momento em que o e-mail é *recebido e lido* – não se deve identificar o fim do processo dinâmico da transmissão com a mera chegada ao aparelho do destinatário, pois também aí ela pode estar exposta a intromissões arbitrárias dos sistemas de comunicações à revelia das partes), sendo a partir deste momento que ele deixa de estar na *específica situação de perigo,* fazendo com que se esgote a necessidade de tutela da inviolabilidade da comunicação, pois o próprio destinatário

[88] Cfr. TRIBUNAL EUROPEU DOS DIREITOS HUMANOS, *Guide on Article 8 of the European Convention on Human Rights*, 31.08.2020, p. 105, disponível em https://www.echr.coe.int/documents/guide_art_8_eng.pdf [acedido a 28 de setembro de 2020].

passa a dispor de meios de autotutela como a instalação dos mais diversos sistemas de segurança ou, pura e simplesmente, ao apagamento e destruição dos dados. O e-mail deixa, assim, de pertencer à área de tutela das comunicações, devendo valer como um normal escrito, um ficheiro produzido pelo utilizador do sistema informático e nele guardado e, como não é pelo facto de já não cair na área de tutela do sigilo das comunicações que estas comunicações, já recebidas e lidas, passam a estar à mercê de toda e qualquer devassa, ficam assim, no âmbito da obtenção de meios de prova, sujeitas a um regime próprio, ainda que menos exigente, podendo ser objeto de busca através de apreensão do próprio sistema informático, ou, preferencialmente porque menos lesiva, sob forma de cópia.[89]

Contudo, não foi este o raciocínio que o nosso legislador adotou na regulação da apreensão de e-mails e semelhantes. Ao passo que o regime de apreensão de correspondência, disposto no art. 179.º do CPP, incide somente sobre correspondência fechada (estando a correspondência aberta sujeita ao regime geral das apreensões por ser considerada mera prova documental), a LC não faz qualquer menção à diferença entre as mensagens abertas e lidas das demais, o que leva o intérprete a aplicar o art. 17.º da LC a ambas.

Fica desta forma a apreensão de todos os e-mails e semelhantes encontrados num sistema informático, abertos e lidos, ou não, dependente de autorização judicial. Haverá razão de ser deste privilégio dado ao correio eletrónico e outras comunicações, já lidas pelo seu destinatário, em relação ao correio tradicional também ele já aberto e lido?

Particularmente crítico desta solução é João Conde Correia, considerando que, atendendo apenas ao sentido literal, se a lei não diferencia o correio eletrónico lido do não lido, assumimos que o legislador português quis conferir ao correio eletrónico armazenado uma tutela superior aos demais documentos corpóreos, também eles, armazenados.[90]

Todavia, nas palavras do autor, *uma leitura integrada e coerente que acentue as inevitáveis semelhanças com os escritos tradicionais e as suas necessidades de tutela* superará o elemento gramatical da lei. Uma vez terminado o processo de transmissão com a chegada da mensagem à esfera do destinatário, a comunicação já não está *sujeita às falhas de reserva do operador ou à curiosidade estadual* – conforme desenvolvido por Manuel da

[89] ANDRADE, Manuel da Costa, *Bruscamente no Verão passado, cit.*, p. 156-160.
[90] O autor não entende como, na prática, ao não diferenciar o correio eletrónico recebido e lido do restante, a lei permite ao MP apreender uma carta que se encontre guardada num cofre, mas não um e-mail ou outra comunicação que se encontre guardada num sistema informático.

Costa Andrade – e, como tal, não deverá usufruir do regime da apreensão de correspondência, cujos apertados requisitos encontram justificação no facto de a comunicação se encontrar ainda em trânsito e, por isso, exposta a um maior risco de intromissão de terceiros.

Não fazendo sentido favorecer o correio eletrónico já recebido e lido, que deve ser considerado um mero documento escrito e, portanto, sujeito às garantias do mesmo, é suficiente um controlo judicial posterior feito nos termos dos n.os 1 e 3 do art. 16.º da LC (que consagra o regime de apreensão de dados informáticos): basta a intervenção do MP e, caso o conteúdo dos documentos apreendidos seja suscetível de revelar dados pessoais ou íntimos que possam pôr em causa a privacidade do titular ou de terceiro, um controlo judicial posterior. Assim, há somente lugar à aplicação do regime do art. 17.º da LC se a mensagem ainda não tiver sido lida pelo destinatário.[91/92]

Porém, para além da leitura do art. 17.º não nos permitir, só por si, fazer esta distinção, também tecnicamente, distinguir entre uma mensagem de correio eletrónico lida e uma não lida, não faz sentido.

Para começar, é importante ter presentes duas ideias, sendo a primeira a noção do gigante que é hoje em dia o mercado de software para correio eletrónico, onde empresas de peso como a Microsoft, a Google ou a Apple Inc. têm, cada uma, os seus próprios programas informáticos para correio eletrónico e uma série de outras empresas comercializam programas de correio eletrónico para diferentes sistemas operativos, como é o caso do Windows, entre outros que, por sua vez, vão sendo atualizados em novas versões ao longo do tempo – diferentes programas informáticos significam diferentes características técnicas e representações gráficas; e a segunda, o facto de presumirmos que o destinatário recebeu o correio eletrónico e tomou conhecimento do seu conteúdo (passando à frente a impossibilidade de ter a certeza absoluta que um e-mail foi efetivamente lido e não apenas aberto), somente através de uma sinalética normalmente presente no programa informático que geralmente se traduz numa imagem de um envelope fechado, envelope este que

[91] CORREIA, João Conde, *ob. cit.*, p. 40 e 41. A exigência de um despacho judicial prévio será tratada no próximo capítulo.

[92] Na mesma linha de pensamento, Paulo Dá Mesquita defende que o art. 17.º da LC, ao determinar a aplicação do art. 179.º do CPP, exclui da tutela especial as mensagens de correio eletrónico já acedidas pelo destinatário (Cfr. MESQUITA, Paulo Dá, *ob. cit.*, p. 118).

desaparece ou se transforma num envelope aberto, assim que o e-mail é acedido (e não necessariamente lido) voluntariamente pelo utilizador.[93]

Ora, alguns prestadores de serviço de correio eletrónico não têm este regime e, mesmo que o tenham, os seus utilizadores podem, rápida e facilmente, consoante os seus critérios, alterar o sinal de lido para não lido, ou melhor dizendo, de aberto para não aberto, e vice-versa (ao contrário do que acontece com o correio tradicional), a qualquer momento e por um número infinito de vezes. O correio eletrónico indicado como fechado não tem a finalidade de proteger o conteúdo do e-mail como os envelopes corpóreos protegem o conteúdo do correio tradicional. Estes sinais que por norma acompanham os e-mails, acabam por funcionar como meros filtros para o destinatário localizar e gerir o correio eletrónico recebido, pelo que assumir que a mensagem já foi lida, ou não, consoante a sinalética que a acompanha, fragilíssimo indicador de leitura, é errado.

Ademais, da mesma forma que o utilizador através de um clique muda o estado do e-mail para aberto ou não aberto, também o pode guardar no seu sistema informático sem o ter lido ou como mensagem enviada ou a enviar. Como distingui-los?

Para além do exposto, uma vez que o regime em apreço não se aplica somente ao correio eletrónico, mas igualmente a "registos de comunicações de natureza semelhante", que dirão os autores que defendem regimes diferentes para correio eletrónico lido e não lido, baseando-se apenas naquela nada fiável sinalética, do tratamento que se deve dar a mensagens como SMS, MMS ou mensagens instantâneas que chegam ao sistema informático do destinatário, cujos programas não têm sequer o filtro *lido/não lido?*

A isto soma-se o facto de muitas vezes as comunicações eletrónicas através de correio eletrónico ou semelhantes estarem a ocorrer simultaneamente em diferentes aparelhos informáticos, desde o computador, ao tablet, ao telemóvel do destinatário, onde as mensagens podem aparecer lidas num dos sistemas informáticos e não lidas noutro consoante as definições possíveis ou escolhidas pelo destinatário.[94]

Relativamente ao tratamento a dar aos e-mails e registos semelhantes já abertos, também a nossa jurisprudência não tem sido absolutamente unânime. Por um lado, podemos encontrar decisões onde é acolhida a tese de diferenciação entre mensagens lidas e não lidas,

---

[93] BRAVO, Rogério, "Da não equiparação do correio eletrónico ao conceito tradicional de correspondência por carta", Revista Polícia e Justiça, Jan/Jun, 2006 – III Série, N.º 7, Coimbra Editora, 2006, p. 7 e 8. Disponível em https://www.academia.edu/2049081 [acedido a 13 de janeiro de 2020].

[94] Neste sentido, CARDOSO, Rui, *ob. cit.,* p. 185-187; e também FIDALGO, Sónia, *ob. cit.*, p. 69 e 70.

como é o caso do Acórdão da Tribunal da Relação de Évora de 07.04.2015[95] onde se lê: "A mensagem recebida em telemóvel, atenta a natureza e finalidade do aparelho e o seu porte pelo arguido no momento das revistas e apreensões efetuadas, é de presumir que, uma vez recebida, foi lida pelo seu destinatário. *Na sua essência, a mensagem mantida em suporte digital depois de recebida e lida terá a mesma proteção da carta em papel que tenha sido recebida pelo correio e que foi aberta e guardada em arquivo pessoal*. Sendo meros documentos escritos, *estas mensagens não gozam da aplicação do regime de proteção da reserva da correspondência e das comunicações*". [96] Por outro lado, o Acórdão do Tribunal da Relação do Porto de 12.09.2012[97] dispõe que em nada releva se as SMS foram ou não abertas e lidas pelo destinatário, uma vez que a lei não faz esta distinção, invocando-se o princípio *ubi lex non distinguit nec nos distinguere debemus.* [98]

Sustentando-me na crítica feita por Manuel da Costa Andrade, não considero que uma mensagem que já se encontre armazenada no aparelho informático do destinatário mereça uma tutela idêntica à que é dada à correspondência corpórea que se encontre em trânsito que, por sua vez, usufrui de um regime mais garantístico em nome do princípio da inviolabilidade da comunicações, princípio este cujo momento que tem como objetivo salvaguardar, no caso de mensagens já armazenadas no computador do destinatário, cessou.

Questão diferente, sendo aqui que me afasto da linha de pensamento do autor e me aproximo da de Rui Cardoso, é a solução avançada para colmatar esta lacuna: conferir à apreensão de e-mails e semelhantes regimes jurídicos com diferentes níveis de tutela conforme se tratem de mensagens assinaladas como *lidas* ou como *não lidas.*

Tal solução, apesar de facilitadora à investigação, parece-me incomportável. Não só por a lei em nenhum momento discriminar mensagens lidas de não lidas, mas essencialmente por, na prática, esta destrinça ser, no fundo, uma ilusão, já que a diferença entre uma mensagem lida de uma não lida está literalmente à distância de um clique.

---

[95] Disponível em http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/ad8068a8c8f9b3c080257e2e00356d33 [acedido a 17 de fevereiro de 2020].
[96] No mesmo sentido, também os Acórdãos do TRL de 02.03.2011 e de 24.09.2013 e do TRP de 20.01.2016. Disponíveis em www.dgsi.pt [acedidos a 17 de fevereiro de 2020].
[97] Disponível em http://www.dgsi.pt/jtrp.nsf/c3fb530030ea1c61802568d9005cd5bb/877e0322acde18d080257a8300393cc6 [acedido a 18 de fevereiro de 2020].
[98] Neste sentido, *vd.* os Acórdãos do TRL de 07.03.2018 e do TRG de 29.03.2011. Ambos disponíveis em www.dgsi.pt [acedidos a 18 de fevereiro de 2020].

Concluindo, pese embora a apreensão de correio eletrónico e registos semelhantes e a apreensão de correspondência não afetem exatamente os mesmos direitos fundamentais, as diferenças substanciais entre uma carta e um e-mail impossibilitam que a este último se empregue a mesma lógica de aberto/fechado como se de um envelope se tratasse.

4.5. A Exigência de despacho judicial prévio e juiz como primeira pessoa a ter conhecimento do conteúdo das mensagens

No art. 17.º da LC consta que, quando encontradas mensagens de correio eletrónico e comunicações semelhantes, *"(…) o juiz pode autorizar ou ordenar, por despacho, aqueles que se afigurem ser de grande interesse para a descoberta da verdade ou para a prova (…)".* Será que, com isto, o legislador faz imperativamente depender a apreensão de correio eletrónico e comunicações semelhantes de um despacho judicial prévio, mesmo durante a fase de inquérito? Este aspeto processual, a par da questão de se saber se o juiz deve ser a primeira pessoa a tomar conhecimento do conteúdo das mensagens, são dois quesitos processuais intimamente ligados, que mais têm desafiado a doutrina e jurisprudência.

Na doutrina, destaco a tese de Pedro Verdelho nos termos da qual a aplicação do regime de apreensão de correspondência à apreensão de e-mails e registos de comunicações semelhantes seja feita *mutatis mutandis*: enquanto na primeira diligência processual é necessária uma prévia autorização judicial e é exigido que o juiz seja a primeira pessoa a tomar conhecimento do conteúdo da correspondência; na segunda, apesar de as mensagens de correio eletrónico e registos semelhantes não poderem ser usadas como prova num processo sem que haja despacho de um juiz nesse sentido, não sendo a lei *expressa*, é *clara*, na medida em que permite uma *apreensão cautelar* do correio eletrónico e registos semelhantes sem que haja uma decisão judicial prévia, sendo que a única exigência legal para a apreensão ocorrer é a forma de acesso ao suporte informático em que as mensagens se encontram armazenadas ser legítima.

Esta parece-me ser a solução que melhor se coaduna com a prática processual no inquérito, já que normalmente as mensagens de correio eletrónico e análogas são detetadas no decurso de uma pesquisa a um sistema informático, em regra, no decorrer de uma busca. Antes de se realizar uma busca, não se sabe se se encontrará um sistema informático e se, caso se encontre, o mesmo conterá mensagens de correio eletrónico e semelhantes, tão-

pouco se podendo prever se as mesmas serão de grande interesse para a descoberta da verdade. Consequentemente, um despacho judicial prévio à busca, de forma a acautelar a eventualidade de os OPC se depararem com e-mails e registos semelhantes, traduzir-se-ia numa carta em branco à investigação, frustrando a ponderação de valores que o preceito exige. [99]

Não nos olvidemos que, em regra, a menos que o juiz esteja presente na pesquisa, perícia ou acesso permitido ao sistema informático, que, na prática, só acontecerá no decurso de uma busca por ele presidida, as comunicações eletrónicas, antes de chegarem ao domínio do juiz para as apreender formalmente, já sofreram uma apreensão material através da apreensão do sistema informático ou de uma cópia das mensagens.[100]

Entende igualmente Pedro Verdelho que a apreensão provisória de e-mails e semelhantes pressupõe que quem procede à pesquisa toma conhecimento do conteúdo das mensagens, pois só assim está em posição de encaminhar para o juiz mensagens concretas que sejam relevantes para o caso. Sendo que, do ponto de vista operacional, entendo que a solução que dita que o juiz tem de ser a primeira pessoa a tomar conhecimento do teor de todos os e-mails e comunicações semelhantes em todos os sistemas informáticos encontrados durante uma busca, só depois autorizando a sua apreensão, pode revelar-se exacerbadamente penosa não só pela quantidade de aparelhos informáticos apreendidos mas também pela quantidade de comunicações armazenadas nos mesmos.

Seguindo, então, o raciocínio do autor, a apreensão, no âmbito de uma pesquisa informática, poderia ser autorizada pelo MP, sendo depois as mensagens apreendidas apresentadas a um juiz que decidiria ordenar, ou não, a efetiva apreensão das comunicações e sua consequente junção ao processo e, caso decidisse pela não apreensão, o suporte das mensagens deveria ser devolvido ou a cópia destruída – daí o autor apelidar a apreensão de *provisória.*[101]

No que toca à restituição a quem de direito da correspondência que se conclui irrelevante para a prova por força do disposto no n.º 3 do art. 179.º do CPP, alerto para a inadequação do termo "restituição", pois ao contrário do que acontece com a correspondência física, normalmente não há uma verdadeira restituição das mensagens

---

[99] Cfr. CASTRO, Henrique de Antas e, AA.VV., *Meios de obtenção de prova e medidas cautelares e de polícia, ob. cit.,* p. 60 e 61. *Ebook* disponível em http://www.cej.mj.pt/cej/recursos/ebooks/penal/eb_MeiosProva.pdf [acedido a 10 de julho de 2020].
[100] Cfr. CARDOSO, Rui, *ob. cit.,* p. 179 e 180.
[101] VERDELHO, Pedro, "A nova Lei do Cibercrime", *cit., p.* 743-745.

eletrónicas visto que o dono do suporte informático apreendido ou da informação objeto de cópia, não deixa necessariamente de continuar a aceder às comunicações eletrónicas alvo de apreensão.

Na mesma linha de pensamento, Rui Cardoso avança quatro argumentos para sustentar a apreensão provisória, sendo eles: 1) a letra da lei; 2) a coerência do sistema de tutela de direitos; 3) as diferenças de natureza entre correio corpóreo e correio eletrónico ou semelhante; e 4) a imposição constitucional de respeito pela estrutura acusatória do nosso processo penal.

O argumento na letra da lei prende-se com o preceito "o juiz pode autorizar ou ordenar, por despacho" utilizado várias vezes no CPP no que diz respeito à competência do juiz de instrução no que toca a meios de prova ou de obtenção de prova. Em meios de obtenção de prova como interceções telefónicas (art. 187.º do CPP) e interceções de comunicações eletrónicas (art. 18.º da LC), somente admissíveis na fase de inquérito, o legislador deixa claro que o juiz de instrução tem apenas competência para autorizar e nunca para ordenar – na instrução compete ao juiz de instrução ordenar a apreensão e no inquérito apenas autorizá-la. Autorizar significa conceder licença para algo,[102] ficando subentendido que a iniciativa cabe a outra pessoa, no caso, ao Ministério Público. É ao MP que compete a seleção das mensagens cuja apreensão irá ser autorizada, ou não, pelo juiz de instrução, pois só se o MP conhecer das mensagens é que poderá requerer a apreensão das mesmas que se afigurem de grande interesse para a descoberta da verdade ou para a prova. Não conhecendo as mensagens, ao requerer a sua apreensão, Rui Cardoso fala numa *subversão de papéis* entre JIC e MP: depois do primeiro autorizar, o MP poderia concluir pela irrelevância de tais mensagens, não usando a autorização concedida pelo juiz, caso contrário o juiz de instrução estaria a impor ao MP a utilização de concretos meios de prova e tal solução não respeita a estrutura acusatória do nosso processo penal, como desenvolverei no quarto argumento.

Em segundo lugar, entender que na fase de inquérito o juiz de instrução tem de ser a primeira pessoa a conhecer do conteúdo das mensagens de correio eletrónico e semelhantes seria assumir a evidente incoerência por parte do legislador ao tutelar mais fortemente situações à partida menos lesivas dos direitos fundamentais: segundo o n.º 3 do art. 16.º da LC, na apreensão de dados informáticos (que podem abranger fotografias íntimas ou dados

[102] "Autorizar" em Dicionário Infopédia da Língua Portuguesa. Porto: Porto Editora, 2003-2018. https://www.infopedia.pt/dicionarios/lingua-portuguesa/autorizar [acedido a 20 de fevereiro de 2020].

bancários) quem toma primeiro conhecimento são os órgãos de polícia criminal e o MP – só depois de tomar conhecimento dos dados informáticos é que a autoridade judiciária competente pode decidir se aqueles dados são suscetíveis de *revelar dados pessoais ou íntimos, que possam pôr em causa a privacidade do respetivo titular ou de terceiro,* de forma a, se for esse o caso, apresentá-los ao juiz que decidirá pela sua junção, ou não, ao processo; e para a interceção de comunicações, que pode mesmo acontecer em tempo real, também são os OPC e o MP quem toma primeiro conhecimento do conteúdo – n.º 4 do art. 18.º da LC que nos remete para o disposto no art. 188.º do CPP. Se os dados sobre os quais os OPC ou MP tomaram conhecimento no âmbito de uma interceção de comunicações nos termos do art. 18.º da LC, assim que a comunicação cessa, podem ficar armazenados nos sistemas informáticos dos intervenientes e, portanto, apesar de serem os mesmos, estarem a partir dali acessíveis através da apreensão de e-mails e semelhantes, porque é que, numa altura em que o processo de comunicação ainda se encontra em trânsito, o juiz não tem de ser a primeira pessoa a tomar conhecimento e, assim que cessa, há essa obrigatoriedade? Porque é que, se uma intromissão estadual no primeiro momento, como vimos *supra*, afeta de forma mais grave o direito de privacidade do indivíduo, é o segundo momento que merece maior tutela?

Como terceiro argumento, Rui Cardoso aponta algumas diferenças entre o correio eletrónico e o correio tradicional que inviabilizam a aplicação, na sua totalidade, do regime de apreensão de correspondência à apreensão de e-mails e semelhantes, expondo situações da vida prática nas quais a exigência de despacho judicial prévio impediria, ou dificultaria excessivamente, a apreensão dos e-mails e semelhantes, o que, nas palavras do autor, *constituiria uma interpretação contra a CCiber e o âmbito de apreensão de dados que Portugal, como Estado-parte, deve assegurar na sua legislação*.

Em primeiro lugar, muitas vezes, para compreendermos se estamos perante uma mensagem de correio eletrónico ou registos de natureza semelhante é necessário que se conheça o conteúdo do documento em causa, uma vez que o destinatário pode guardar a mensagem como se de uma imagem, de uma página web, ou de um documento de texto se tratasse, tendo apenas de lhe atribuir a extensão correspondente (.jpeg, .html, .docx, etc.);

Pode dar-se o caso de ser crucial, sob pena de se perderem dados importantes assim que o aparelho for desligado, realizar-se uma perícia imediata no decorrer da busca, de forma, por exemplo, a saber se o sistema informático em questão foi *hackeado* ou está a ser

naquele momento controlado externamente de alguma maneira que permita que sejam aí colocadas mensagens não recebidas pelo destinatário;

Além disso, se durante uma pesquisa informática forem descobertas comunicações em serviços como o *instant messenger* ou *chats online*, uma vez que nos primeiros as mensagens podem apagar-se automaticamente após um curto espaço de tempo e nos segundos, a janela de chat, caso o aparelho seja desligado, desaparece, desaparecendo igualmente com ela as comunicações encontradas, é essencial para a investigação que estas mensagens sejam apreendidas no momento da pesquisa e como tal, o seu conteúdo seja conhecido, mesmo que não na sua totalidade.

Finalmente, o autor expõe o que no meu ponto de vista é o argumento preponderante contra a exigência de despacho judicial prévio: o respeito pela estrutura acusatória da investigação criminal.

No nosso sistema penal vigora o princípio do acusatório, consagrado no n.º 5 do art. 32.º da Lei Fundamental, que impõe que a entidade que acusa seja diferente da entidade que julga. Em Portugal tal significa que é ao Ministério Público que cabe dirigir a investigação criminal, sendo que o juiz que atua nesta fase é o juiz de instrução funcionando somente como um juiz de garantias, controlando a atividade do MP e dos OPC na estrita medida do necessário para assegurar os direitos de quem está a ser alvo da investigação, não podendo tomar qualquer tipo de iniciativa no que à investigação diz respeito, impulsionando-a, delimitando o seu objeto ou dominando o seu resultado. Para que se respeitem os direitos fundamentais dos envolvidos e se faça verdadeiramente justiça, é crucial que quem investiga e acusa esteja distanciado de quem julga, pois o interesse do primeiro, o interesse público na repressão criminal, é conflituante com o interesse do segundo em exercer as suas funções como um terceiro imparcial.

Este princípio, apresentado por Gomes Canotilho e Vital Moreira como *garantia essencial do julgamento independente e imparcial*, implica: que o órgão de instrução seja diferente do órgão de acusação; que o órgão de acusação seja diferente do órgão julgador; que o órgão encarregue da instrução seja diverso do órgão ao qual compete a audiência de discussão e julgamento, e vice-versa.[103]

[103] CANOTILHO, José Gomes; MOREIRA, Vital, *Constituição da República Portuguesa Anotada, ob. cit.*, p. 522.

Transcrevendo um excerto do Ac. n.º 129/07, de 24.04.2007, do nosso TC[104], *a imparcialidade dos tribunais é uma exigência não apenas contida no art. 32.º da CRP mas uma decorrência do Estado de direito democrático (art. 2.º), na medida em que se inscreve na garantia universal de defesa dos direitos e interesses legalmente protegidos, através de um órgão de soberania com competência para administrar a justiça (n.º 1 do art. 202 da CRP).* Há assim uma *exigência de imparcialidade objetiva do tribunal,* decorrente da estrutura acusatória do processo penal*, que impede que o juiz do julgamento esteja envolvido na atividade instrutória, quer carreando para os autos elementos de prova suscetíveis de serem utilizados pela acusação, quer envolvendo-se em atos que possam significar dirigir a investigação,* justificando-se esta exigência pelas *garantias de defesa* e pela *necessidade de proporcionar ao juiz as condições de isenção requeridas pelo exercício das suas funções.*

É sabido que o processo de seleção das mensagens *de grande interesse para a descoberta da verdade e para a prova* pressupõe que se tome conhecimento do teor das mesmas. Ora, exigir que o juiz seja a primeira pessoa a tomar conhecimento das mensagens, determinando de seguida quais delas são relevantes para a investigação em curso, é permitir que seja o juiz, que na fase de inquérito deve apenas atuar como entidade que controla os DLG na estrita medida do necessário, a delimitar o objeto da investigação. Se assim for, o juiz não só investiga os factos como impõe ao MP os concretos meios de prova a utilizar, violando-se assim o princípio do acusatório. Portanto, por força do art. 204.º da CRP, segundo o qual os Tribunais devem decidir conforme a Constituição, a remissão que o art. 17.º faz para o regime de apreensão de correspondência tem de ser interpretada respeitando a estrutura acusatória do processo penal português, o que significa que não deve recair sobre o juiz de instrução a decisão de fazer juntar, ou não, ao processo o correio eletrónico e registos semelhantes apreendidos.[105]

Uma questão levantada por Rui Cardoso que não deixa de ser oportuna no presente capítulo, prende-se com o que é que o legislador tinha em vista proteger quando redigiu a parte do n.º 3 do art. 179.º do CPP que estipula que o juiz deve ser a primeira pessoa a tomar conhecimento do teor da correspondência. Para o autor, o que está em causa é *assegurar que o conteúdo da correspondência estava efetivamente nela contida.* Já que, se o objetivo fosse apenas evitar que outras pessoas, que não o JIC, conhecessem do teor da correspondência

[104] Disponível em https://dre.pt/home/-/dre/2296802/details [acedido a 6 de fevereiro de 2020].
[105] CARDOSO, Rui, *ob. cit.*, p. 195-211.

caso esta não relevasse para a prova, a decisão por parte do juiz seria irrecorrível. Acontece que nem o art. 179.º nem o art. 400.º do CPP (que enumera uma série de decisões em que não é admitido recurso) o ditam. Sendo a decisão recorrível, o MP tem necessariamente de conhecer do conteúdo das mensagens cujo interesse para a descoberta da verdade ou para a prova deve fundamentar quando recorre da decisão do juiz, respeitando as exigências do art. 412.º.[106]

Em sentido diverso, Rita Castanheira Neves entende decorrer da lei a necessidade de um despacho judicial prévio, porém, quanto à exigência do juiz como primeira pessoa a tomar conhecimento do conteúdo das mensagens para que posteriormente as selecione, não deixa de mencionar a dificuldade que tal exigência acarretaria na prática, dada a grande quantidade de e-mails e mensagens semelhantes que podem estar armazenados, acrescentando que a resposta a esta dificuldade não passa pela não exigência do juiz como primeira pessoa a tomar conhecimento do conteúdo das mensagens, mas sim pela implementação de critérios estritos para que se apreendam somente os e-mails essenciais à prova.[107]

No que toca à posição tomada pela nossa Jurisprudência, tem-se entendido que o art. 17.º da LC, ao remeter para o regime de apreensão de correspondência plasmado no art. 179.º do Código de Processo Penal, impõe a aplicação deste regime na sua totalidade, tendo vindo a decidir o TRL que o despacho judicial prévio é um requisito legal para a apreensão de correio eletrónico e registos semelhantes e que juiz que autoriza e ordena a apreensão deve ser a primeira pessoa a tomar conhecimento do teor das mensagens.[108]

Não obstante ser este o sentido para o qual a Jurisprudência nacional tem vindo a tender, no Acórdão do TRG de 29.03.2011[109] considerou-se que o art. 17.º da LC deve ser aplicado à apreensão de uma SMS, podendo o MP aceder ao conteúdo das mesmas antes da decisão de apreensão formal por parte do juiz de instrução: *Sublinhando que no sistema legal da LC não poderá nunca haver mensagens de correio eletrónico apreendidas para serem utilizadas como prova num determinado processo sem que haja despacho de um juiz nesse*

---

[106] CARDOSO, Rui, *ob. cit.*, p. 202 e 203.
[107] NEVES, Rita Castanheira, *ob. cit.*, p. 275.
[108] Veja-se, a título de exemplo, os Acórdãos do TRL de 11.01.2011, de 06.02.2018, de 07.03.2018 e de 04.02.2020. Disponíveis em www.dgsi.pt [acedidos a 18 de fevereiro de 2020].
[109] Disponível em http://www.dgsi.pt/jtrg.nsf/86c25a698e4e7cb7802579ec004d3832/6aa96edf91e899b2802578a00054631f [acedido a 18 de fevereiro de 2020].

sentido, defendendo, contudo, *nem sempre ser exigível a existência de uma prévia decisão judicial para a respetiva apreensão, que pode revestir a natureza provisória – v.g. quando surgida no decurso de uma pesquisa realizada com a autorização do MP*.

Recentemente, o TRL, na Decisão Sumária de 06.02.2019,[110] veio defender que o conhecimento pelo JIC, em primeira mão, do conteúdo das mensagens, viola a autonomia, a estrutura acusatória do processo penal, e o direito de investigação do MP. Num caso em que o JIC determinou que a pesquisa ao conteúdo se fizesse através de um perito apenas com base nas palavras-chave indicadas por si, decidiu este Tribunal que a seleção de conteúdos, de modo a avaliar a sua relevância probatória, é da competência do titular da ação penal, o MP, estando vedada ao JIC qualquer intervenção conformadora do destino do processo à revelia do poder decisório do MP. Se o JIC limitar esta seleção atenta contra o art. 32.º da CRP e viola o disposto nos artigos 262.º e 263.º do CPP. Assim, o MP deve proceder previamente à análise do teor dos e-mails, estando obrigado a apresentar os mesmos ao JIC que, num momento posterior, decidirá o que se deve anexar aos autos e o que se deve eliminar, apenas de modo a assegurar a fiscalização jurisdicional dos DLG.

A meu ver, se por um lado a letra da lei é inequívoca no que toca à exigência de despacho judicial, retirando-se a mesma diretamente do art. 17.º da LC que dispõe "*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",* por outro, não especifica se esse despacho deve, ou não, ser *prévio*. No entanto, ainda que o legislador não o explicite, o facto de se ter limitado a reescrever o preceito que já constava do art. 179.º do CPP ("o juiz pode autorizar ou ordenar") no art. 17.º da LC, leva-me a considerar que a sua intenção foi a de atribuir a este preceito o mesmo sentido que lhe é dado em sede de apreensão de correspondência, ou seja, exigir a autorização prévia do juiz.

Apesar de entender estarmos perante um requisito legal deste meio de obtenção de prova (sendo que a triagem a cabo do JIC das mensagens relevantes tem como pressuposto que seja ele o primeiro a tomar conhecimento das mesmas) e, como qualquer requisito legal, o mesmo tem de ser respeitado até nova mudança legislativa, considero que se deve ter em consideração não só os inconvenientes práticos que Pedro Verdelho e Rui Cardoso mencionam, com a consequente frustração da investigação criminal que um tal requisito

[110] Disponível em http://www.pgdlisboa.pt/jurel/jur_mostra_doc.php?nid=5594 [acedido a 15 de julho de 2020].

pode significar, como também por ir diretamente contra um dos princípios basilares do nosso sistema penal que dita ser o MP o *dominus* da fase inquérito. Logo, compreendo o aplicador que interprete a remissão do artigo 17.º de forma engenhosa, com vista a aligeirar os efeitos nocivos desta opção legislativa.

O que me leva a defender que as características da realidade que se pretende regular exigem a criação de um regime de apreensão de e-mails e registos semelhantes autónomo, onde se repartam explicitamente as competências entre o MP e o JIC e se clarifique definitivamente se a autorização judicial é uma exigência prévia ou posterior, evitando que a dúvida se arraste nos nossos Tribunais.

Sublinho, no entanto, que alguns dos problemas expostos, nomeadamente os que se relacionam com a necessidade de uma atuação célere e assertiva por parte dos OPC quando se deparam com prova digital, dada a sua fragilidade, podem ser significativamente atenuados, através do mecanismo do n.^{os} 2 e 3 do art. 252.º do CPP, onde se prevê a apreensão da correspondência sem autorização prévia do juiz (sendo depois convalidada por ele no prazo de 48h) e a possibilidade do juiz autorizar a abertura da mesma de imediato (ou seja, pelos OPC), caso haja *periculum in mora.*

4.6. A possibilidade de aproveitamento em processo penal das mensagens apreendidas à ordem de outro processo

Uma questão interessante que merece a minha abordagem é a de saber se a prova obtida mediante apreensão de correio eletrónico poderá ser posteriormente utilizada em processo diferente daquele à ordem do qual se realizou a apreensão.

No dia 11 de julho de 2019, o TRL considerou que o aproveitamento *extraprocessual* de correio eletrónico se insere no n.º 7 do art. 187.º do CPP que regula o regime das escutas telefónicas, estando dependente de autorização judicial, cuja competência recai sobre o JIC do processo *no qual se visa obter tais meios de prova.* Ou seja, a junção ao processo dos meios de prova que contêm os conhecimentos fortuitos não está dependente da autorização judicial do juiz de instrução do "segundo" processo, mas sim do juiz de instrução

do "primeiro" processo que foi quem decidiu sobre a legalidade de tais meios de prova, bem como a verificação dos requisitos legais consagrados no n.º 7 do art. 187.º do CPP.[111]

Segundo Sónia Fidalgo,[112] e na mesma linha de pensamento de Jorge de Figueiredo Dias e Nuno Brandão,[113] há que diferenciar duas situações:

Um problema é o dos conhecimentos fortuitos obtidos no decorrer da apreensão de correio eletrónico. Manuel da Costa Andrade define conhecimentos fortuitos no âmbito das escutas telefónicas como *o aproveitamento dos dados na investigação de outros crimes e no contexto de outro processo criminal, distinto daquele em que se produziram as escutas*.[114] Problemática cujo estudo é sem dúvida pertinente, *dada a frequência da sua ocorrência, associada à impossibilidade fáctica de limitar a escuta aos conhecimentos ou factos que, à partida, determinam a sua validade* [115] – situação a que a apreensão de correio eletrónico se encontra, de igual forma, suscetível.

Estão aqui em causa elementos de prova, no caso, mensagens de correio eletrónico já apreendidas e individualizadas, do conhecimento das autoridades judiciárias e valoradas pelas mesmas, sendo que é a partir desta mesma apreciação que se encontram dados que podem ser relevantes para a investigação de outros crimes e no contexto de outro processo penal.

Nestas condições, não é por a lei não consagrar expressamente a transmissão de conhecimentos fortuitos decorrentes da apreensão de correio eletrónico de um processo penal para outro que tal transmissão é proibida. Entende-se, sim, que aqui tem lugar a aplicação do regime geral dos conhecimentos fortuitos adquiridos no âmbito de escutas telefónicas, consagrado somente em 2007 no n.º 7 do artigo 187.º do CPP, segundo o qual as conversações só poderão ser utilizadas noutro processo se nele se encontrarem igualmente verificadas as exigências legais que legitimaram a realização da escuta telefónica, nomeadamente: se tiver resultado de uma comunicação feita por algum dos sujeitos do n.º 4

---

[111] Acórdão do TRL de 11.07.2019 disponível em http://www.gde.mj.pt/jtrl.nsf/33182fc732316039802565fa00497eec/1bc410315a7483298025843b004c1e71 [acedido a 29 de dezembro de 2019].
[112] FIDALGO, Sónia, *ob. cit.*, p. 70 e ss.
[113] DIAS, Jorge de Figueiredo; BRANDÃO, Nuno, Parecer junto ao processo criminal n.º 184/12.5TELSB, não publicado, n.º 18 (*apud* FIDALGO, Sónia, *ob. cit.*, p. 70).
[114] ANDRADE, Manuel da Costa, *Bruscamente no Verão passado, cit.*, p. 174.
[115] ANDRADE, Manuel da Costa, *Sobre as Proibições de prova em Processo Penal, cit.*, p. 304.

do mesmo artigo; se for indispensável à prova do crime; e se este crime for um dos crimes de catálogo elencados no n.º 1.

Como tal, fazendo aplicar o regime dos conhecimentos fortuitos no decorrer das escutas telefónicas aos conhecimentos fortuitos decorrentes da apreensão de correio eletrónico e registos semelhantes, os dados obtidos através de uma apreensão de correio eletrónico só poderão ser valorados como prova noutro processo penal se neste processo se puder decretar a apreensão de correio eletrónico, isto é, se no processo para onde se pretende "exportar" os dados estiverem verificados os requisitos legais que permitem a utilização deste meio de obtenção de prova.[116]

Diz-nos o n.º 8 do art. 187.º que, no que diz respeito aos conhecimentos fortuitos no âmbito das escutas telefónicas, *os suportes técnicos das conversações ou comunicações e os despachos que fundamentaram as respetivas interceções são juntos, mediante despacho do juiz, ao processo em que devam ser utilizados como meio de prova (…)*. Impõe-nos, assim, a distinção dos poderes que competem ao juiz de instrução onde as escutas telefónicas foram realizadas e os que, por sua vez, caem na esfera de poderes do juiz do processo onde se pretendem "aproveitar" as escutas.

Paulo Pinto de Albuquerque considera que ao primeiro cabe decidir sobre a legalidade das escutas, bem como a verificação dos pressupostos legais plasmados no n.º 7 do art. 187.º, sendo que, se os mesmos se verificarem, ele determina a remessa para o outro processo de *cópia da totalidade das gravações referentes ao alvo ou alvos em questão, dos relatórios referentes às ditas gravações e dos despachos atinentes à autorização, manutenção e cessação de escuta telefónica;* ao juiz do "segundo" processo, caberá apenas a possibilidade de *ordenar a destruição das cópias das gravações e dos relatórios*, mas somente depois de os interessados neste processo terem a possibilidade de tomar conhecimento de tais documentos na sua íntegra, de modo a que seja salvaguardada a garantia constitucional de defesa do arguido.[117]

Parece-me ser esta a solução que melhor se harmoniza com a prática processual, uma vez que, não obstante ser o juiz do processo originário quem profere o despacho, é lógico que não é ele quem se encontra no melhor lugar para avaliar a "indispensabilidade" para a prova do processo de destino do conhecimento fortuito, pois, a não ser que também

[116] ANDRADE, Manuel da Costa, *Bruscamente no Verão passado, cit.,* p. 173; FIDALGO, Sónia, *ob. cit.,* p. 71.
[117] ALBUQUERQUE, Paulo Pinto de, *ob. cit.,* p. 528.

ele seja o juiz natural deste processo, não o conhece, *reconduzindo-se tal aferição a uma análise perfunctória, isolada e descontextualizada dos autos para que se remete.*[118] Só posteriormente, remetidos os suportes técnicos ou cópia dos mesmos para o segundo processo, é que as entidades processuais que se encontram responsáveis por este último poderão avaliar e selecionar as partes que considerarem relevantes para a prova.

Situação diferente é aquela em que o MP, aquando da fase de inquérito de um processo a decorrer, solicita ao juiz de instrução a realização de uma pesquisa em caixas de correio eletrónico que já se encontram apreendidas, mas à ordem de outro processo, ou seja, não se pretende "importar" para o segundo processo as mensagens de correio eletrónico de conteúdo conhecido, mas sim realizar uma nova busca ao sistema informático onde se encontram as mensagens que são elementos probatórios de um primeiro processo, mas que, para todos os efeitos, ainda são de conteúdo desconhecido no segundo processo, com o intuito de apreender os e-mails que se revelem relevantes para a prova deste último.

Em princípio, esta segunda busca é permitida e, por vezes, inevitável. Imaginemos o caso em que as mensagens de correio eletrónico se encontram apenas armazenadas num único computador e imaginemos agora que esse computador já foi apreendido, mas com o objetivo de ser alvo de uma busca informática no âmbito de outro processo.

Perante uma segunda pesquisa nestes termos, entendo que o MP deve dirigir a sua solicitação para a apreensão das mensagens de correio eletrónico ao juiz de instrução deste segundo processo, pois só o juiz que exerce funções no processo para o qual se pretende realizar a nova pesquisa (onde, volto a frisar, se encontram dados desconhecidos neste segundo processo) está apto a avaliar se os pressupostos de que a mesma depende se verificam, nomeadamente o "grande interesse para a descoberta da verdade e para a prova" (art. 17.º da LC). É este juiz, e não o do segundo processo, que deve proferir despacho a autorizar a apreensão e também deverá ser ele, como vimos, o primeiro a ter conhecimento do teor das mensagens apreendidas.

Caso contrário, se a realização da nova apreensão acontecesse mediante autorização do juiz do processo originário, estaríamos perante uma violação das regras de competência do tribunal que, segundo a al. *e)* do art. 119.º do CPP, significaria uma nulidade insanável

[118] CARLOS ADÉRITO TEIXEIRA, "Escutas Telefónicas: a mudança de paradigma e os velhos e os novos problemas", *Revista CEJ*, 1.º Semestre 2008, Número 9 (Especial) – Jornadas sobre a revisão do Código de Processo Penal, p. 279 e 280.

dos atos praticados por esse juiz. O que, por sua vez, leva a que a prova alvo de apreensão por força de autorização do juiz incompetente não possa ser valorada.[119]

5. Tratamento do correio eletrónico e registos de comunicações de natureza semelhante no ordenamento jurídico Alemão

Dada a universalidade do problema em consideração, o meu estudo ficaria incompleto se não discorresse, ainda que brevemente, sobre o regime de apreensão de correio eletrónico e registos semelhantes no ordenamento jurídico que ainda hoje é fonte de inspiração para o nosso legislador e doutrina portuguesa.

Se a proliferação da Internet esteve na génese da aldeia global em que vivemos, cujos desafios de regulação preocupam o legislador português, é apenas natural que também os demais legisladores se dediquem à problemática da prova digital.

Com efeito, recentemente, Ministros da Justiça de oito Estados da Alemanha, no âmbito da Declaração de Kassel, adotada a 31 de julho de 2017, reconheceram a urgência de uma agenda digital que operasse mudanças legislativas a nível do direito penal e direito processual penal alemão, destacando alguns temas jurídicos que a próxima legislatura devia tratar, como a criminalização de publicidade a organizações terroristas em plataformas como o *Youtube* ou o *Twitter* ou a clarificação das regras legais que serviços de telecomunicações como o *WhatsApp* ou o *Skype* devem respeitar.[120]

O Código Penal Alemão (*Strafgesetzbuch)* criminaliza a violação de correspondência tradicional no seu §202 onde se pode ler que *quem, sem autorização para tal, abrir carta selada ou outro documento selado que não lhe é dirigido; ou, sem o abrir, tomar conhecimento do conteúdo de tal documento utilizando meios técnicos, é punido com pena de prisão até um ano ou multa.*

Já no §202a, referente à espionagem de dados, o StGB pune com pena de prisão até 3 anos ou multa quem, sem autorização para tal, obtenha ou dê a terceiro acesso a dados que não lhe foram dirigidos e se encontravam protegidos contra acesso não autorizado,

[119] Precisamente neste sentido, FIDALGO, Sónia, *ob. cit.*, p. 71-73.
[120] Consultado em https://beck-online.beck.de/Dokument?vpath=bibdata%2Freddok%2Fbecklink%2F2007428.htm [acedido a 15 de setembro de 2020].

encontrando-se na subsecção 2 a definição de dados: *dados armazenados ou transmitidos eletrónica ou magneticamente ou de outra forma não imediatamente percetível.* [121]

Não obstante a recente tendência da lei alemã em dispersar em diplomas extravagantes várias formas de interceção de comunicações, o legislador alemão conseguiu compilar no StPO uma grande variedade de meios de obtenção de prova, incluindo meios ocultos de investigação. Esta tentativa de lhes dar guarida formal no StPO, erguendo, assim, um verdadeiro sistema (em oposição ao que aconteceu no ordenamento jurídico português), mereceu o elogio de Manuel da Costa Andrade.[122]

É no Capítulo VIII do Código de Processo Penal Alemão (*Strafprozeßordnung)* que se encontram regulados os meios de obtenção de prova, onde se incluem, no que ao meu estudo importa, a apreensão de objetos para fins probatórios (§94 e ss.), a apreensão de correspondência (§99 e §100),[123] a vigilância das telecomunicações (§100a) e a recolha de dados de tráfego (§100g).

O §100a trata da vigilância das comunicações, medida que consiste na monitorização e registo da palavra falada ou dos dados transmitidos através de uma infraestrutura de telecomunicações. Verificados determinados requisitos de admissibilidade, todos aqueles que fornecem ou colaboram na prestação de serviços de telecomunicações numa base comercial devem cooperar com o tribunal, o MP e os seus investigadores, fornecendo informações necessárias sem demora, como se pode ler na subsecção 5 do mesmo artigo e no §110 da Lei das Telecomunicações, Lei de 22.06.2004, (Telekommunikationsgesetz) e concedendo equipamento técnico para implementar o monitoramento de telecomunicações. Por se tratar de uma medida invasiva, nem sempre feita com o conhecimento do visado, em que o Estado penetra no processo comunicacional do cidadão, está subordinada a exigentes requisitos (*v.g.* reservada a infrações penais graves elencadas na subsecção 2; a investigação dos factos e localização do arguido ser infrutífera por outros meios; apenas pode ser ordenada pelo juiz mediante requerimento do MP, ou

[121] Ainda no StGB é tipificada a violação do segredo postal e das telecomunicações no §206, no entanto, as normas aqui estipuladas apenas dizem respeito a proprietário ou funcionário de uma empresa no ramo de prestação de serviços postais e de telecomunicações.
[122] ANDRADE, Manuel da Costa, *Bruscamente no Verão passado, cit.*, p. 23 e 24.
[123] Estipulada no §99, permite a apreensão de correspondência e telegramas dirigidos ao arguido, *que estejam sob custódia de pessoas ou empresas que prestem ou participem em serviços postais* ou de telecomunicações em atividade, dos quais possa ser deduzível dos factos disponíveis que foi enviada pelo arguido ou lhe é dirigida, desde que o seu conteúdo seja relevante para a investigação.

diretamente por este último, em caso de *periculum em mora,* carecendo a ordem, sob pena de ineficácia, de confirmação por parte do juiz dentro de 3 dias úteis).[124]

Segundo o BverfG, o sigilo postal, de correspondência e das telecomunicações, estipulado no n.º 1 do §10 da Constituição Alemã (*Grundgesetz), assegura o direito ao livre desenvolvimento da personalidade, garantindo a troca de informações privada, subtraída à esfera pública e, por conseguinte, protege também a dignidade do ser humano,* radicando a sua razão de ser na proteção da comunicação privada, independentemente da forma de transmissão (por cabo, analógico, digital, etc.) e a forma de expressão (língua, imagem, som, entre outros), num momento em que os interlocutores, devido à distância física que os separa, dependem da transmissão de outrem (serviços de telecomunicações) estando a comunicação, como tal, especialmente vulnerável ao acesso de terceiros.[125]

Este princípio fundamental não abrange apenas o conteúdo das mensagens, mas também os dados de tráfego: *o direito fundamental protege também a confidencialidade sobre as circunstâncias do processo de comunicação. O que compreende especialmente o se, o quando, o como, entre que pessoas ou entre que aparelhos a comunicação teve lugar ou foi tentada* pois tendo *um grande conteúdo de expressividade (…) podem, em concreto, permitir conclusões decisivas sobre a comunicação e movimentação.*[126]

Quanto ao âmbito de extensão deste segredo, o BVerfG defende que a tutela da inviolabilidade das comunicações termina assim que os dados atingem a esfera de domínio do destinatário, momento este em que os dados de conteúdo e os dados de ligação deixam de se distinguir dos dados produzidos pelo próprio, como sejam os documentos elaborados e gravados num sistema eletrónico do visado de uma busca e apreensão, pois passa a poder impedir o acesso de terceiros e decide se os guarda ou elimina, ainda que o fator decisivo da proteção do sigilo das comunicações não seja *a possibilidade de eliminação de forma segura, mas sim a sua comparabilidade com quaisquer outros dados armazenados na esfera privada do indivíduo.* Posto isto, findo o processo de comunicação, os dados de ligação armazenados no dispositivo do interlocutor não são protegidos pelo §10 da GG, mas sim

---

[124] §100e do StPO que estipula as regras processuais do §100a. (Cfr. ROGALL, Klaus, "Nova regulação da vigilância das telecomunicações na Alemanha", *2.º Congresso de Investigação Criminal,* Trad. Vânia Costa Ramos, Almedina, 2010, p. 124-128.

[125] BVerfG, 2 BvR 2099/04 de 02.03.2006 (*apud* RAMOS, Vânia, "Âmbito e Extensão do Segredo das Telecomunicações", *Revista do Ministério Público*, n.º 11, Out./Dez., 2007, p. 147).

[126] BVerfG 2 BvR 2099/04 de 02.03.2006 (*apud* ANDRADE, Manuel da Costa, *Bruscamente no Verão passado, cit.,* p. 161).

pelo direito à autodeterminação informacional estipulado no n.º 1, §2 conjugado com o n.º 1, §1 da GG e, eventualmente, pela inviolabilidade do domicílio consagrada no §13 da GG.[127]

Se, no entendimento do BVerfG, é verdade que diferentes momentos do processo comunicativo merecem diferentes níveis de tutela sob a asa de diferentes princípios, é natural que faça depender o regime a aplicar do momento em questão.

Como tal, a apreensão de dados cujo processo de transmissão ainda não foi concluído está adstrita aos rigorosos requisitos do §100a do StPO (vigilância das telecomunicações) por cair no âmbito de tutela da inviolabilidade das comunicações do §10 da GG, pensado para proteger o destinatário num momento em que está sujeito aos perigos típicos do processo de transmissão fora da sua influência. Assim que o processo de comunicação cessa, cessa com ele a necessidade de proteção da inviolabilidade das telecomunicações, passando os mesmos dados, agora armazenados no dispositivo, a estar abrangidos pela proteção subsidiária do direito à autodeterminação informacional, aplicando-se a partir deste momento as normas da apreensão de objetos consagradas no §94 e ss. do StPO.[128]

Esta distinção entre o momento em que a comunicação se encontra em trânsito e o momento em que ela já cessou tem consagração expressa no próprio StPO na subsecção 5 do seu §100g (recolha de dados de tráfego): "se a recolha de dados de tráfego não for efetuada pelo prestador de serviços de telecomunicações, será determinada *de acordo com as regras gerais* após o *fim do processo de comunicação"*.

Já em 2005, o mesmo tribunal de Karlsruhe, tinha decidido que os §94 e ss. do StPO permitem a apreensão de suportes de armazenamento de dados e dos dados neles armazenados como prova de processo penal, considerando que tais preceitos cumprem os requisitos constitucionais em relação à apreensão de suportes de dados e dos dados neles armazenados, satisfazendo, relativamente ao direito de autodeterminação informacional, *as exigências segundo as quais o legislador tem que determinar a finalidade do levantamento*

---

[127] BVerfG 2 BvR 2099/04 de 02.03.2006 (*apud* RAMOS, Vânia, *ob. cit.*, p. 148 e 149).

[128] STEPHAN LUDEWIG,"Proteger e avaliar o smartphone – Necessidade de adaptação da política criminal?", *Revista de Política Criminal* (Kriminalpolitische Zeitschrift) – Kripoz, 2019, que pode ser consultado em https://kripoz.de/2019/09/18/die-sicherstellung-und-auswertung-des-smartphones-kriminalpolitischer-anpassungsbedarf/ [acedido a 12 de setembro de 2020]; e PAOLA BENEDICT, "Mensagens de *WhatsApp* como prova", AA.VV., *Direito Penal na Idade da Digitalização*, *Kripoz-Jup*, *Revista de Política Criminal*, 2020, disponível para consulta em https://kripoz.de/wp-content/uploads/2020/06/kripoz-jup-sammelband-strafrecht-im-zeitalter-von-digitalisierung-und-datafizierung.pdf [acedido a 16 de outubro de 2020].

dos dados de forma precisa, específica para cada domínio e reconhecível para o visado. Mostrando-se ainda consciente da crescente relevância da prova digital no ponto 99 onde se pode ler que *embora os poderes de intervenção relevantes sejam originalmente adaptados a objetos físicos, o legislador histórico que criou as normas desatualizadas sobre a apreensão ainda não podia prever a possibilidade de os dados eletrónicos se tornarem significativos como informação não física para a apresentação de provas em processos penais. Contudo, o aditamento do §98 e ss. no StPO em 1992 já mostra que a nova legislatura assumiu que as bases de dados poderiam ser apreendidas.*[129/130]

Apurado que no ordenamento jurídico alemão não tem acolhimento a equiparação do correio eletrónico à correspondência corpórea e que, assim que a mensagem chega à esfera do destinatário, deixa de ter lugar a tutela da inviolabilidade das comunicações, passando a apreensão de e-mails e comunicações de natureza semelhante armazenadas num dispositivo a fazer-se segundo as regras gerais de apreensão de objetos, atrevo-me a fazer minhas as palavras de Armando Dias Ramos quando conclui que, já que a lei alemã é a fonte onde os nossos juristas e legislador vão muitas vezes beber, que lhe sigam as pisadas no que toca ao tratamento dos e-mails e registos semelhantes para fins probatórios.[131]

[129] Cfr. BVerfG, 2BvR 1027/02, de 12.04.2005 (*apud* RAMOS, Vânia, *ob. cit.*, p. 142).
[130] Não nos esqueçamos que também entre nós se procede à distinção do regime de interceção de e-mails e registos semelhantes em tempo real, do regime de apreensão de e-mails e registos semelhantes armazenados em suporte eletrónico (ver *supra* p. 25). O problema está no facto do legislador português, a estas últimas, atribuir um regime pensado para a correspondência corpórea ainda em trânsito.
[131] RAMOS, Armando Dias, *A Prova Digital em Processo Penal, cit.*, p. 89 e 90.

Conclusão

Ao se consagrarem na Lei do Cibercrime diligências processuais com vista à obtenção de prova no meio informático, atribuiu-se à prova digital uma certa regulação autónoma. Não tendo o legislador considerado a desaconselhável consagração de tais preceitos fora do nosso CPP, dada a atual e crescente relevância que a prova digital conquistará na investigação penal, também não revogou formalmente o art. 189.º do CPP que ainda hoje, onze anos após a entrada em vigor da LC, remete para o regime das escutas telefónicas.

Estou ciente da tremenda dificuldade da lei em acompanhar o contínuo e acelerado desenvolvimento tecnológico que torna o ciberambiente, de certo modo, resistente a tentativas de sistematização. Todavia, não se entende como em 2009 entrou em vigor a Lei do Cibercrime que, já em plena Era Digital, sujeitou os e-mails e registos semelhantes a uma interpretação extensiva de uma norma pensada para a correspondência corpórea fechada, sendo que até ao presente ano ainda não foi alvo de alterações, apesar da realidade que pretende regular estar em constante progresso.

Neste momento, enquanto a lei assim permanecer, à apreensão de e-mails, SMS e outras mensagens de *WhatsApp, Messenger*, etc., armazenadas no aparelho eletrónico do destinatário, independentemente de terem sido abertas e lidas, por força do art. 17.º da LC, aplica-se o regime da apreensão de correspondência previsto no art. 179.º do CPP, nos termos do qual a autorização judicial prévia é uma exigência, o JIC deve ser a primeira pessoa a tomar conhecimento do teor das mensagens que se pretendem apreender e o requerimento para uma nova apreensão deve ser dirigido ao juiz do processo em que se pretende aproveitar a prova. Apesar de ser da opinião que é este o entendimento que deve prevalecer segundo a atual redação da lei, considero que tal redação ficou aquém das necessidades de regulação que a prova digital invoca.

Comecei o meu estudo com o propósito de descortinar se a aplicação do regime de apreensão de correspondência ao art. 17.º da LC se deve fazer na sua íntegra ou deve ser objeto de uma interpretação restritiva, com as devidas adaptações à apreensão de prova digital. Entretanto, ao longo da minha investigação, tornou-se evidente que as especificidades do correio eletrónico justificam que o legislador lhes erija um regime completamente autónomo, que os livre de uma vez da sombra da correspondência corpórea.

Concluo a minha dissertação numa nota de apelo ao legislador para que se debruce com novos olhos para a complexidade técnica e jurídica da apreensão de comunicações eletrónicas, que reclama para si um regime autossuficiente, ajustado às suas particularidades únicas, que premeie pela agilidade do processo penal, nunca negligenciando a tutela dos direitos fundamentais aqui postos em causa.

Bibliografia

- ALBUQUERQUE, Paulo Pinto de, *Comentário do Código de Processo Penal: à luz da Constituição da República e da Convenção dos Direitos do Homem*, 4.ª Edição, Universidade Católica Editora, 2011;

- ANDRADE, Manuel da Costa, "Sobre o regime processual penal das escutas telefónicas", *Revista Portuguesa de Ciência Criminal*, Ano I, 3, Jul/Set, 1991, Aequitas, p. 369-408;

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

- ANDRADE, Manuel da Costa, *Sobre as proibições de prova em Processo Penal*, Reimpressão, Coimbra Editora, 2013;

- CANOTILHO, J. J. Gomes; MOREIRA, Vital, *Constituição da República Portuguesa anotada*, Vol. I, 4.ª Edição Revista, Coimbra Editora, 2014;

- CARDOSO, Rui, "Apreensão de correio electrónico e registos de comunicações de natureza semelhante – artigo 17.º da Lei n.º 109/2009, de 15.IX", *Revista do Ministério Público*, n.º 153, 2018, p. 167-214;

- CORREIA, João Conde, "Prova digital: as leis que temos e a lei que devíamos ter", *Revista do Ministério Público*, n.º 139, Jul/Set, 2014, p. 29-59;

- COSTA, José de Faria, "As telecomunicações e a privacidade: o olhar (in)discreto de um penalista", *Direito Penal da Comunicação – Alguns escritos*, Coimbra Editora, 1998, p. 47-78;

- CASTRO, Catarina Sarmento e, "O direito á autodeterminação informativa e os novos desafios gerados pelo direito à liberdade e à segurança no pós 11 de setembro", *Estudos de Homenagem ao Conselheiro José Manuel Cardoso da Costa*, Vol. II, Coimbra Editora, 2005, p. 65-95;

- DIAS, Jorge de Figueiredo, "Revisitação de algumas ideias-mestras da teoria das proibições de prova em processo penal (também à luz da jurisprudência constitucional portuguesa*)", Revista de Legislação e de Jurisprudência*, n.º 146, 2016, p. 3 a 16;

- FIDALGO, Sónia, "Apreensão de correio eletrónico e utilização noutro processo das mensagens apreendidas", *Revista Portuguesa de Ciência Criminal*, n.º 1, IDPEE, 2019, p. 59-74;

- MARTINS, A. G. Lourenço, *Criminalidade informática,* AA.VV., *Direito da Sociedade da Informação,* Vol. IV, Coimbra Editora, 2003, p. 9-41;

- MARTINS, A. G. Lourenço; MARQUES, J. A. Garcia; DIAS, Pedro Simões, *Cyberlaw em Portugal: O direito das tecnologias da informação e da comunicação*, Centro Atlântico, 2004;

- MESQUITA, Paulo Dá, "Prolegómenos sobre prova electrónica e intercepção de telecomunicações no Direito Processual Penal Português – o Código e a Lei do Cibercrime", *Processo Penal, Prova e Sistema Judiciário*, Coimbra Editora, 2010, p. 83-129;

- NEVES, Rita Castanheira, *As ingerências nas comunicações eletrónicas em processo penal, Natureza e respetivo regime jurídico do correio eletrónico enquanto meio de obtenção de prova,* Coimbra Editora, 2011;

- NUNES, Duarte Rodrigues, *Os meios de obtenção de prova previstos na Lei do Cibercrime*, Gestlegal, 2018;

- RAMALHO, David Silva, *Métodos ocultos de investigação criminal em ambiente digital*, Almedina, 2017;

- RAMOS, Vânia Costa, "Âmbito e Extensão do Segredo das Telecomunicações (Acórdão do Segundo Senado do Tribunal Constitucional Federal Alemão, 2 de março de 2006)", *Revista do Ministério Público*, n.º 11, Out./Dez., 2007, p. 141-159;

- RAMOS, Armando Dias, *A prova digital em processo penal: o correio eletrónico*, 2.ª Edição, Chiado Editora, 2017;

- RODRIGUES, Benjamim, *Das escutas telefónicas – À obtenção da prova [em ambiente] digital*, Tomo II, 2.ª Edição, Coimbra Editora, 2009;

- RODRIGUES, Benjamim, *Direito penal, Parte especial – Direito penal informático-digital*, Tomo I, Coimbra Editora, 2009;

- RODRIGUES, Benjamim, *Da prova penal, Da prova – eletrónico-digital e da criminalidade informático-digital*, Tomo IV, Rei Dos Livros, 2011;

- ROGALL, Klaus, "Nova regulação da vigilância das Telecomunicações na Alemanha", *2.º Congresso da Investigação Criminal*, Coordenação científica: Maria Fernanda Palma; Augusto Silva Dias; Paulo de Sousa Mendes, *Trad.* Vânia Costa Ramos, Almedina, 2010, p. 117-143;

- SANTIAGO, Rodrigo, "Considerações acerca do regime estatutário do segredo profissional dos advogados", *Revista da Ordem dos Advogados*, Ano 57, n.º 1, 1997, p. 229-247;

- SANTOS, Paulo; BESSA, Ricardo; PIMENTEL, Carlos, *Cyberwar – O fenómeno, as tecnologias e os atores*, FCA – Editora de Informática, 2008;

- TEIXEIRA, Carlos Adérito, "Escutas telefónicas: a mudança de paradigma e os velhos e os novos problemas", *Revista CEJ*, 1.º Semestre 2008, Número 9 (Especial) – Jornadas sobre a revisão do Código de Processo Penal, p. 243-295;

- VENÂNCIO, Pedro Dias, *Lei do cibercrime anotada e comentada*, Coimbra Editora, 2011;

- VERDELHO, Pedro, *Cibercrime*, AA.VV., *Direito da sociedade da informação*, Vol. IV, Coimbra Editora, 2003, p. 347-383;

- VERDELHO, Pedro, "A nova lei do cibercrime", *Scientia Iuridica*, Tomo LVIII, n.º 320, 2009, Universidade do Minho, p. 717-749;

- VERDELHO, Pedro; BRAVO, Rogério; E ROCHA, Manuel Lopes, *Leis do cibercrime*, Vol. I, Centro Atlântico, 2003.

Jurisprudência

- Acórdão do Tribunal Constitucional n.º 128/92, de 01.04.1992, disponível *online* em https://www.tribunalconstitucional.pt/tc/acordaos/19920128.html [acedido a 24 de abril de 2020];

- Acórdão do Tribunal Constitucional n.º 129/07, de 24.04.2007, disponível *online* em https://www.tribunalconstitucional.pt/tc/acordaos/20070129.html [acedido a 6 de fevereiro de 2020];

- Acórdão do Tribunal Constitucional n.º 403/2015, de 17.09.2015, disponível *online* em https://dre.pt/home//dre/70300353/details/maximized?p_auth=OsYd65lz [acedido a 24 de abril de 2020];

- Acórdão do Tribunal da Relação de Évora de 20.01.2015, proferido sob o processo n.º 648/14.6GCFAR-A.E1, disponível *online* em http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/2fbdd21285478f5f80257de10056ff7a?OpenDocument [acedido a 5 de fevereiro de 2020];

- Acórdão do Tribunal da Relação de Évora de 07.04.2015, proferido sob o processo n.º 13/15.8PAOLH-A, disponível *online* em http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/ad8068a8c8f9b3c080257e2e00356d33?OpenDocument [acedido a 17 de fevereiro de 2020];

- Acórdão do Tribunal da Relação de Guimarães de 29.03.2011, proferido sob o processo n.º 735/10.0GAPTL-A.G1, disponível *online* em http://www.dgsi.pt/jtrg.nsf/86c25a698e4e7cb7802579ec004d3832/6aa96edf91e899b2802578a00054631f?OpenDocument [acedido a 18 de fevereiro de 2020];

- Acórdão do Tribunal da Relação de Lisboa de 11.01.2011, proferido sob o processo n.º 5412/08.9TDLSB-A.L1-5, disponível *online* em http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/e5ed1936deb44eb180257824004ab09d?OpenDocument [acedido a 18 de fevereiro de 2020];

- Acórdão do Tribunal da Relação de Lisboa de 02.03.2011, proferido sob o processo n.º 463/07.3TAALM-A.L1-3, disponível *online* em http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/d10c400a16882e9e80257853005d65c1?OpenDocument [acedido a 17 de fevereiro de 2020];

- Acórdão do Tribunal da Relação de Lisboa de 29.03.2012, proferido sob o processo n.º 744/09-1S5LSB-A.L1-9, disponível *online* em http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/3fadd3f921c9d658802579e2004500c9?OpenDocument [acedido a 10 de julho de 2020];

- Acórdão do Tribunal da Relação de Lisboa de 24.09.2013, proferido sob o processo n.º 145/10.9GEALM.L2-5, disponível *online* em http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/c60dfe830c97cf8980257c0000368afa?OpenDocument [acedido a 17 de fevereiro de 2020];

- Acórdão do Tribunal da Relação de Lisboa de 06.02.2018, proferido sob o processo n.º 1950/17.0T9LSB-A.L1-5, disponível *online* em http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/a1b9fce5f23b342480258242004327a3?OpenDocument [acedido a 18 de fevereiro de 2020];

- Acórdão do Tribunal da Relação de Lisboa de 07.03.2018, proferido sob o processo n.º 184/12.5TELSB-A.L1), disponível *online* em http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/f46dd746a7530742802583850037249e?OpenDocument [acedido a 18 de fevereiro de 2020];

- Acórdão do Tribunal da Relação de Lisboa de 08.05.2018, proferido sob o processo n.º 6/16.8TELSB-C.L1-5, disponível *online* em

http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/e48d47e75466b9da802582b00053061e?OpenDocument [acedido a 6 de setembro de 2020];

- Acórdão do Tribunal da Relação de Lisboa de 21.02.2019, proferido sob o processo n.º 6/16.8TELSB-D.L1-9, disponível *online* em http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/a75d4805a5715595802583ad0030a8e0?OpenDocument [acedido a 12 de julho de 2020];

- Acórdão do Tribunal da Relação de Lisboa de 11.07.2019, proferido sob o processo n.º 184/12.5TELSB-B.L1-3, disponível *online* em http://www.gde.mj.pt/jtrl.nsf/33182fc732316039802565fa00497eec/1bc410315a7483298025843b004c1e71?OpenDocument [acedido a 29 de dezembro de 2019];

- Acórdão do Tribunal da Relação de Lisboa de 04.02.2020, proferido sob o processo n.º 1286/14.9IDLSB-A.L1-5, disponível *online* em http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/a411de057cfd2e1d80258507004c7e4e?OpenDocument [acedido a 18 de fevereiro de 2020];

- Acórdão do Tribunal da Relação do Porto de 12.09.2012, proferido sob o processo n.º 787/11.5PWPRT.P1, disponível *online* em http://www.dgsi.pt/jtrp.nsf/c3fb530030ea1c61802568d9005cd5bb/877e0322acde18d080257a8300393cc6?OpenDocument [acedido a 18 de fevereiro de 2020];

- Acórdão do Tribunal da Relação do Porto de 03.04.2013, proferido sob o processo n.º 856/11.1PASJM.P1, disponível *online* em http://www.dgsi.pt/jtrp.nsf/d1d5ce625d24df5380257583004ee7d7/d21c6752627b971780257b4f003caa5d?OpenDocument [acedido a 10 de julho de 2020];

- Acórdão do Tribunal da Relação do Porto de 20.01.2016, proferido sob o processo n.º 1145/08.4PBMTS.P1, disponível *online* em http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/54a82f139588437f80257f5a0033e764?OpenDocument [acedido a 10 de julho de 2020];

- Acórdão do Tribunal da Relação do Porto 13.04.2016, proferido sob o processo n.º 471/15.0T9AGD-A.P1, disponível *online* em http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/ef54d51d3972157d80257fa4002e2d75?OpenDocument&Highlight=0,109%2F2009 [acedido a 10 de julho de 2020];

- Decisão Sumária do Tribunal da Relação de Lisboa de 06.02.2019, proferida sob o processo n.º 152/16.8TELSB-B.L1, disponível *online* em http://www.pgdlisboa.pt/jurel/jur_mostra_doc.php?nid=5594&codarea=57& [acedido a 15 de julho de 2020];

- Acórdão do TJUE, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González.*, de 13.05.2014, disponível *online* em https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131 [acedido a 16 de julho de 2020].

Links Relevantes

- AA.VV., *Meios de obtenção de prova e medidas cautelares e de polícia,* Lisboa: Centro de Estudos Judiciários, 2019. *E-book* disponível em http://www.cej.mj.pt/cej/recursos/ebooks/penal/eb_MeiosProva.pdf [acedido a 10 de julho de 2020];

-Artigo sobre o interesse dos empregadores na "pegada digital" dos seus trabalhadores. Disponível em https://apnews.com/press-release/pr-businesswire/83451cf9ed6c49f094ef946975e7f772 [acedido a 3 de julho de 2020];

- Artigo sobre Ray Tomlinson, *Meet the man who put the @ in your e-mail*. Disponível em https://www.internethalloffame.org/blog/2012/07/30/meet-man-who-put-%E2%80%98%E2%80%99-your-e-mail [acedido a 24 de novembro de 2019];

- BRAVO, Rogério, "Da não equiparação do correio eletrónico ao conceito tradicional de correspondência por carta", *Revista Polícia e Justiça*, Jan/Jun, 2006, III Série, N.º 7, Coimbra Editora, 2006. Disponível em https://www.academia.edu/2049081/Da_n%C3%A3o_equipara%C3%A7%C3%A3o_do_correio_electr%C3%B3nico_ao_conceito_tradicional_de_correspond%C3%AAncia_por_carta [acedido a 13 de janeiro de 2020];

- Documento do CONSELHO DA EUROPA, *Electronic Evidence Guide – A basic guide for police officers, prosecutors and judges,* 2020. Disponível em https://rm.coe.int/c-proc-electronic-evidence-guide-2-1-en-june-2020-web2/16809ed4b4 [acedido a 7 de setembro de 2020];

- Documento do TRIBUNAL EUROPEU DOS DIREITOS HUMANOS, *Guide on Article 8 of the European Convention on Human Rights,* 2020. Disponível em https://www.echr.coe.int/documents/guide_art_8_eng.pdf [acedido a 28 de setembro de 2020];

- Informação sobre a Declaração de Kassel. Disponível em https://beck-online.beck.de/Dokument?vpath=bibdata%2Freddok%2Fbecklink%2F2007428.htm [acedido a 15 de setembro de 2020];

- BENEDICT, Paola, "Mensagens de *WhatsApp* como prova", AA.VV., "Direito Penal na Idade da Digitalização", *Kripoz-Jup, Revista de Política Criminal,* 2020, p. 74-82. Disponível em https://kripoz.de/wp-content/uploads/2020/06/kripoz-jup-sammelband-strafrecht-im-zeitalter-von-digitalisierung-und-datafizierung.pdf [acedido a 16 de outubro de 2020];

- BARLOW, Perry, "A declaration of independence of cyberspace". Disponível em https://www.eff.org/cyberspace-independence [acedido a 24 de novembro de 2019];

- RAMOS, Armando Dias, *A novíssima Diretiva sobre o Cibercrime,* Apresentação na Conferência na Universidade Autónoma de Lisboa, "Espaço de Liberdade, Segurança e Justiça", 2013. Disponível em https://www.academia.edu/8696174/A_Nov%C3%ADssima_Diretiva_sobre_o_Cibercrime [acedido a 27 de novembro de 2019];

- LUDEWIG, Stephan, "Proteger e avaliar o smartphone – Necessidade de adaptação da política criminal?", *Kripoz – Revista online de Política Criminal,* 2019. Disponível em https://kripoz.de/2019/09/18/die-sicherstellung-und-auswertung-des-smartphones-kriminalpolitischer-anpassungsbedarf/ [acedido a 12 de setembro de 2020];

- VLECK, Tom Van, "The history of electronic mail". Disponível em https://www.multicians.org/thvv/mail-history.html [acedido a 24 de novembro de 2019].