Tiago Leonel dos Santos Aguiar

O Correio Eletrónico

A Apreensão e a Interceção no Processo Penal Português

Dissertação apresentada à Faculdade de Direito da Universidade de Coimbra
no âmbito do 2.º Ciclo de Estudos em Direito (conducente ao grau de Mestre),
na Área de Especialização em Ciências Jurídico - Criminais, sob Orientação
do Professor Doutor Nuno Fernando da Rocha Almeida Brandão.

Coimbra
2017

· U C ·

Universidade de Coimbra

• U C •

FDUC FACULDADE DE DIREITO
UNIVERSIDADE DE COIMBRA

Tiago Leonel dos Santos Aguiar

O Correio Eletrónico

A Apreensão e a Interceção no Processo Penal Português

The Electronic Mail

The Seizure and Interception in the Portuguese Criminal Procedure

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

Orientador: Professor Doutor Nuno Fernando da Rocha Almeida Brandão.

Coimbra, 2017

Dedicatória

Ao Salvador e ao Santiago, por me permitirem tão grande privilégio de os chamar de Filhos.

"Considerada por alguns como um objecto perigoso para a nossa sociedade e sendo por outros considerada como a «salvação», a informática constitui uma nova fonte de problemas jurídicos."*

Helena Moniz

---

*MONIZ, Helena, *Notas sobre a proteção de dados pessoais perante a informática (o caso especial dos dados pessoais relativos à saúde),* Separata da Revista Portuguesa de Ciência Criminal, Ano 7, Fasc. 2.º, Coimbra Editora, Abril – Junho 1997, p. 231-232.

Agradecimentos

Como em qualquer ciência, todo o começo é difícil. A velha máxima de Marx, refletida no culminar do presente trabalho, tem trazido à memória do Autor destas linhas os duros trilhos e sulcos que calcorreou para atingir o cume da montanha. Por se ter tratado de uma extraordinária caminhada de descoberta, provações, angústias, encantos e desencantos, num reiterado e intenso exercício de questionamento sísmico da ciência, é chegada a altura de deixar palavras de profunda gratidão a quem, com uma tremenda generosidade, tornou possível o sonho de realizar esta viagem.

A primeira palavra de agradecimento não poderá deixar de ser dirigida ao Ex.mo Senhor Professor Doutor Nuno Fernando da Rocha Almeida Brandão, verdadeiro timoneiro deste trabalho de investigação científico, não apenas pelo constante apoio e disponibilidade com que sempre me presenteou, como também os caminhos certeiros que apontou e me desafiou a percorrer, deveras inspiradores para alcançar a(s) meta(s) desejada(s). Endosso, pois, uma palavra de puro e sincero reconhecimento, quer pela transmissão de conhecimentos, quer pela sua notável dedicação pessoal, sabendo que as palavras de agradecimento nunca serão excessivas para retribuir o imensurável contributo que, de forma sempre presente, concedeu à proficuidade desta dissertação.

De igual modo, em momento algum poderei esquecer a Instituição de ensino a que me orgulho de pertencer. Assim, uma especial palavra de apreço a Todos os que, sem exceção, integram o Corpo Docente da Faculdade de Direito da Universidade de Coimbra, por me demonstrarem que, mais do que uma escola de Direito e veículo que transporta o nome da cidade aos quatro cantos do mundo, esta emblemática Instituição é uma verdadeira escola onde se cultivam princípios e valores. Agradeço, ainda aqui, a todos os Ex.mos Senhores Funcionários das várias salas de leitura e dos espaços bibliotecários da Faculdade que, muitas vezes emprestando-me o seu tempo para lá do seu horário de expediente, me concederam uma colaboração preciosa na pesquisa de obras científicas, sem as quais, estou certo, este trabalho ficaria mais pobre.

Para lá da Porta Férrea, uma especial palavra de gratidão ao Escritório que, há precisamente uma década, me deu a oportunidade de dar os primeiros passos na Advocacia, ensinando-me que os fios que tecem a toga são feitos a partir de uma inquebrável estrutura de princípios e solidariedade, cozidos a um ponto de linha que se

chama sabedoria. A todos, sem exceção, obrigado por me terem incentivado a voltar aos bancos da Faculdade, proporcionando-me todas as condições que permitissem dedicar-me, sob intenso afinco, ao labor da investigação científica.

Palavras de gratidão são ainda devidas ao Senhor Engenheiro de Informática Marco Estanqueiro, pela valiosíssima ajuda na compreensão de conceitos e procedimentos informáticos que se viriam a revelar indispensáveis à temática. De igual modo, uma palavra de agradecimento às diversas pessoas anónimas que trabalham nas mais variadas bibliotecas que frequentei para efetuar pesquisas.

Nos domínios da intimidade, ao meu Pai, por, desde muito cedo, me incutir a lição que a única fórmula para obter o sucesso é a partir do trabalho; à minha Mãe, modelo de humildade e altruísmo; à minha Irmã, por nunca me largar a mão, seja qual for a circunstância. O vosso incentivo, companheirismo, ânimo e confiança nas minhas capacidades, sempre foram fatores determinantes na subida da escadaria dos meus estudos académicos.

Falta o derradeiro agradecimento. Aquele que, sendo feito aos últimos, é dirigido aos que ocupam os lugares cimeiros. Os que são a razão do meu viver, os meus pilares e estrutura, pertencendo ao antes, ao durante e ao depois de tudo. À Filipa, por ser a melhor Mãe e a melhor Esposa do mundo, sem a qual, verdadeiramente, nada disto seria possível. Aos meus Filhos, Salvador e Santiago, sempre aos meus Filhos, por terem transformado a minha vida, por serem a maior motivação que vai em todas as linhas deste trabalho, assim como, nunca o poderei esquecer, o mais precioso oásis que encontrei nas horas em que a travessia se revelava mais árdua.

Resumo

O aparecimento da Internet, aliada à rápida expansão das tecnologias de informação e de comunicação, permitiu que o correio eletrónico revolucionasse a forma como comunicamos, tornando-se, no seio da nova sociedade da informação, um veículo privilegiado de comunicação.

Na era digital, as comunicações eletrónicas, trazendo benefícios inegáveis, expõem-nos, no reverso da moeda, a novos e diversificados perigos, catapultando a criminalidade informática para níveis tecnicamente evoluídos. Reconhecendo-se a natureza instável, dispersa e imaterial que caracteriza a prova digital, tornar-se-ia imperioso adaptar as leis penais às novas e evoluídas condutas desviantes perpetradas por meios informáticos, desafiando-se o legislador a apetrechar a investigação criminal de novos meios de obtenção de prova digital adaptados ao ambiente "eletrónico digital", de forma a garantir a integridade e força probatória desta prova.

No ordenamento jurídico português a prova digital está hoje regulada em três diplomas legais: O Código de Processo Penal, a Lei n.º 32/2008, de 17/07, e a Lei n.º 109/2009, de 15/09. Ao invés de assegurar a centralidade normativa do Código de Processo Penal, com a vigência destas leis extravagantes, o legislador português submeteu a prova digital, particularmente, o correio eletrónico, sob um labirinto jurídico, dada a aparente contraditoriedade entre diplomas.

Debruçando-nos sobre as questões processuais respeitantes à admissibilidade da apreensão e interceção das mensagens de correio eletrónico, procuramos com este estudo analisar as disposições processuais vigentes no ordenamento jurídico português que regulamentam a obtenção desta específica prova digital, questionando a conciliação dos novos mecanismos dispostos na Lei do Cibercrime com as várias disposições processuais relativas à obtenção da prova digital consagradas no Código de Processo Penal e na Lei 32/2008, de 17/07, de forma a aferir se estamos perante um conflito de disposições processuais na obtenção da prova digital, ou se, pelo contrário, estamos perante normas processuais que se complementam entre si.

Palavras-Chave: Internet, Cibercrime, Prova Digital, Correio Eletrónico, Direitos Fundamentais.

Abstract

The emergence of the Internet, coupled with the fast expansion of information and communication technologies, allowed the electronic mail to revolutionize the way in which we communicate, becoming, within the new information society, a privileged vehicle of communication.

In the digital age, the electronic communications, bringing undeniable benefits, expose us, on the other side of the coin, to new and diverse dangers, catapulting computer-related crimes to technically advanced levels. By recognizing the unstable, dispersed and immaterial nature which characterizes digital proof, it would become essential to adapt the penal laws to the new and advanced deviant behaviors perpetrated by electronic resources, challenging the legislator to equip the criminal investigation with new ways of obtaining digital proof adapted to the "electronic digital environment", to ensure the integrity and its probative force.

In the Portuguese legal system the digital proof is now regulated in three legal acts: The Code of Criminal Procedure, Law no. 32/2008, of 17/07, and Law no. 109/2009, of 15/09. Instead of ensuring the normative centrality of the Code of Criminal Procedure, with the enforcement of these extravagant laws, the Portuguese legislator submitted the digital proof, particularly the electronic mail, under a legal labyrinth, given the apparent contradiction between legal laws.

Dealing with procedural issues regarding the admissibility of the seizure and the interception of electronic mail, the aim of this study is to analyze the procedural provisions in the current Portuguese legal system which regulate the obtainment of this specific digital evidence, questioning the conciliation of the new available mechanisms in the Cybercrime Law with the various procedural provisions regarding the obtainment of the digital evidence established in the Code of Criminal Procedure and in Law 32/2008, of 17/07, in order to access if we are facing a conflict of procedural provisions in obtaining the digital proof, or whether, on the contrary, we are facing procedural provisions that complement each other.

Keywords: Internet, Cybercrime, Digital Proof, Electronic mail, Fundamental Rights.

Lista de Siglas e Abreviaturas

A.C. – Antes de Cristo
AA. VV. – Autores Vários
AAFDL – Associação Académica da Faculdade de Direito de Lisboa
Ac. – Acórdão
Al. – Alínea
ARPA – Advanced Research Projects Agency
Art.º – Artigo
BFDUC – Boletim da Faculdade de Direito da Universidade de Coimbra
BVferG – Bundesverfassungsgericht (Tribunal Constitucional Federal da Alemanha)
CC – Código Civil
CCiber – Convenção do Cibercrime
CD – Compact Disc
CEDH – Convenção Europeia dos Direitos do Homem
Cfr. – Conforme
Cit. – Citação
CNPD – Comissão Nacional de Proteção de Dados
CP – Código Penal
CPP – Código de Processo Penal
CRP – Constituição da República Portuguesa
DL – Decreto - Lei
DNS – Domain Name System
DUDH – Declaração Universal dos Direitos Humanos
DVD – Digital Versatile Disc
EUA – Estados Unidos da América
EUROPOL – Serviço Europeu de Polícia
Ex. – Exemplo
FBI – Federal Bureau of Investigation
GC – Gabinete do Cibercrime
GG – Grundgesetz (Constituição Federal da Alemanha)
IBAN – International Bank Account Number
ICP-ANACOM – Autoridade Nacional de Comunicações
IMAP – Internet Mail Acess Protocol
IMEI – International Mobile Equipment Identity
IMSI – International Mobile Subscriber Identity
IP – Internet Protocol
ISP – Internet Service Provider
ISSN – International Standard Serial Number
JIC – Juiz de Instrução Criminal
LC – Lei do Cibercrime

LECrim – Ley de Enjuiciamiento Criminal
MDA – Mail Delivery Agent
MP – Ministério Público
MTA – Mail Transfer Agent
MUA – Mail User Agent
N.º – Número
OPC – Órgão de Polícia Criminal
P. – Página
PGR – Procuradoria Geral da República
PJ – Polícia Judiciária
POP – Post Office Protocol
Q.I. – Quociente de Inteligência
RGPD – Regulamento Geral de Proteção de Dados
RIR – Regional Internet Registry
RMP – Revista Ministério Público
SMTP – Simple Mail Transfer Protocol
StPO – Strafprozeßordnung (Código de Processo Penal)
TC – Tribunal Constitucional
TCP – Transmission Control Protocol
TFUE – Tratado sobre o Funcionamento da União Europeia
TJUE – Tribunal de Justiça da União Europeia
TRC – Tribunal da Relação de Coimbra
TRE – Tribunal da Relação de Évora
TRG – Tribunal da Relação de Guimarães
TRL – Tribunal da Relação de Lisboa
TRP – Tribunal da Relação de Porto
UE – União Europeia
V.g. – Abreviatura de *verbi gratia* (significa por exemplo)
VoIP – Voice Over Internet Protocol

Índice

Introdução 12
1. O Nascimento da Sociedade da Informação 15
2. A Criminalidade Informática 19
2.1. As Categorias do Cibercrime 19
2.2. Os Sujeitos do Cibercrime 21
2.2.1. O Sujeito/Agente Ativo 21
2.2.2. O Sujeito Passivo – A Vítima. 24
3. A Prova Digital nos Fluxos Comunicacionais 26
3.1. O Ato Comunicacional 26
3.2. Do Correio Tradicional ao Correio Eletrónico 27
3.3. Da Comunicação entre Máquinas – "O Diálogo Protocolar" 31
3.4. Os Dados Informáticos nas Comunicações Eletrónicas 35
3.4.1. Os Dados de Base, Tráfego e Conteúdo 35
3.4.2. O Internet Protocol (IP) – Um Dado de Tráfego, Base ou Localização? 37
3.5. As Dificuldades Colocadas pela Prova Digital 39
4. A Reserva da Intimidade da Vida Privada nas Modernas Tecnologias de Informação e Comunicação 44
4.1. O Direito à Inviolabilidade das Comunicações Eletrónicas 44
4.2. A Proteção dos Dados Pessoais Informatizados e o Direito à Autodeterminação Informacional nas Comunicações Eletrónicas 50
5. O Regime Jurídico Aplicável ao Correio Eletrónico no Código de Processo Penal 58
5.1. Do CPP de 1987 até à Reforma de 2007 58
5.2. Da (In)Submissão do Correio Eletrónico ao Regime das Escutas Telefónicas 64
5.2.1. A Palavra Falada e a Palavra Escrita 66
5.2.2. A Encruzilhada Conceptual do art.º 189.º do CPP 72
6. A Lei n.º 32/2008, de 17 de Julho 80
7. A Lei 109/2009, de 15 de Setembro – A Lei do Cibercrime 84
8. O Art.º 17.º da LC - A Apreensão do Correio Eletrónico 91
8.1. A Apreensão das Mensagens de Correio Eletrónico e a Cláusula de Extensão Operada pelo Art.º 11.º da LC 91

8.2. O Correio Eletrónico Armazenado e a sua (não) Equiparação à Correspondência Tradicional 94
8.3. A Importância da Pesquisa Informática na Apreensão das Mensagens de Correio Eletrónico 104
8.4. A Exigência Prévia de Despacho Judicial para a Apreensão de Correio Eletrónico 109
9. O Art.º 18.º da LC – A Interceção do Correio Eletrónico 120
9.1. A Interceção dos Dados Informáticos em "Trânsito" 120
9.2. O Art.º 18.º da LC e a (In)Adequação à Cláusula de Extensão Prevista no Art.º 189º do CPP 123
9.3. As Buscas *Online* 134
Conclusão 137
Bibliografia 141
Jurisprudência, Pareceres e Outros Recursos Bibliográficos 154

Introdução

A expansão das modernas tecnologias de informação e comunicação, servindo de alavanca de transição da sociedade industrial para a sociedade da informação, permitiu, progressivamente, que a criminalidade informática se desenvolvesse tentacularmente no ciberespaço, catapultando-a para níveis altamente evoluídos, colocando a descoberto as fragilidades que a máquina estatal tem sentido ao lidar com tal flagelo.

Neste esteio, cedo se percebeu que atendendo ao complexo mundo do cibercrime, assim como aos constrangimentos da recolha e preservação da prova digital, peculiarmente por se tratar de prova *"fragmentária, dispersa, frágil, volátil, alterável, instável, apagável, manipulável, invisível e espacialmente dispersa"*[1], tornar-se-ia premente obter um novo modelo de ciência forense que orientasse e adaptasse a investigação criminal ao ambiente "eletrónico digital", garantindo-se que tal prova, à luz da ponderação constitucional, se mantivesse plenamente válida e processualmente admissível.

A questão da admissibilidade, designadamente, das condições processuais de admissibilidade da apreensão e intercepção de dados informáticos de comunicações eletrónicas, ou de elementos com origem em comunicações eletrónicas, assume importância fulcral para o processo penal, constituindo, pela sua natureza, prova vital na prossecução, identificação e punição dos meliantes dos delitos. Dentro dos novos meios de comunicação eletrónicos, assume primordial e particular destaque o correio eletrónico.

Conhecedor desta realidade, entre nós, o legislador cedo iniciou a repressão à criminalidade informática através da Lei n.º 109/91, de 17/8, também denominada de "Lei da Criminalidade Informática". Ora, o facto é que, não tendo o legislador contemplado neste diploma legal um regime jurídico específico de recolha da prova digital, remeteu a sua obtenção para o complexo meio de obtenção de prova ínsito no art.º 187.º e seguintes do Código de Processo Penal – relativo às escutas telefónicas – circunstância que, processualmente, obstaculizava e colocava em causa a investigação criminal, atendendo ao conjunto de enigmas que, por via deste específico meio de obtenção de prova, a prova digital se vê mergulhada.

[1] RODRIGUES, Benjamim Silva, *Da Prova Penal – Tomo IV, Da Prova - Electrónico - Digital e da Criminalidade Informático – Digital*, Rei dos Livros, Lisboa, 2011, ISBN 9789898305183, p. 29.

A resposta a tal paradigma frutificou de uma evolução normativa inspirada pelos influentes contributos europeus, nomeadamente, a Convenção sobre o Cibercrime adotada em Budapeste, em 23 de Novembro de 2001, e a Decisão-Quadro 2005/222/JAI do Conselho, de 24 de Fevereiro de 2005, materializadas com a criação da Lei n.º 109/2009, de 15 de Setembro (Lei do Cibercrime), colmatando este diploma legal profundas lacunas que, até então, eram sobejamente conhecidas no sistema processual penal português, apetrechando a investigação criminal com novos instrumentos especificamente talhados para a recolha da prova digital.

Não obstante as inovações processuais consagradas pela Lei do Cibercrime, a opção legislativa acabaria por não contemplar a revogação do art.º 189.º, n.º1, do Código de Processo Penal, que determina a aplicação do regime das escutas telefónicas quer à interceção e registo das mensagens de correio eletrónico, quer propriamente à sua apreensão, ainda que tais mensagens permaneçam armazenadas em suporte digital, desconsiderando tal normativo os desequilíbrios de proteção constitucional a que tal meio de prova, por via dos seus dois momentos, pode estar submetido: o momento de transmissão, em que a mensagem reclama a proteção inerente ao estatuto de comunicação, e o outro, posterior ao cumprimento do ato de levar ao destinatário o teor comunicacional, elevado ao estatuto aproximado de um ficheiro digital armazenado.

De tal forma, com o meio de obtenção de prova previsto no art.º 17.º da LC, consagrou o legislador a possibilidade de apreensão de mensagens de correio eletrónico, bem como de registos de natureza semelhante, que se encontrem armazenadas, submetendo a regulamentação de tal diligência a partir do regime estatuído para a apreensão de correspondência previsto no art.º 179.º do CPP. Por seu turno, o art.º 18.º da LC veio contemplar um regime específico para a interceção e registo de comunicações eletrónicas, ali se determinando que, em tudo o que não lhe for contrariado, seja aplicado o regime da interceção e gravação de conversações ou comunicações telefónicas dos art.ºs 187.º, 188.º e 190.º do CPP.

Com a consagração na Lei do Cibercrime destes dois regimes específicos de obtenção de prova digital e a remissão para os meios clássicos previstos no CPP, o legislador colocou o intérprete numa difícil encruzilhada interpretativa, atendendo à quantidade de fontes normativas a mobilizar e conciliar, abrindo flanco para uma acesa discussão doutrinária e jurisprudencial relativamente à aplicação e aparente equiparação de

regimes que, na sua realidade, são bem diferentes. Com efeito, confronta-se hoje o pensamento jurídico com um conjunto de questões que estão longe de se tornar consensuais. Desde logo, a primeira, consiste em saber se fará sentido ou não considerar que a opção legislativa equiparou o correio eletrónico ao correio tradicional, assim como saber se a remissão ínsita no art.º 17.º da LC comporta, na íntegra, a aplicação em bloco das regras, formalidades e condicionantes dispostas no art.º 179.º do CPP. Doutro passo, atendendo que a LC não procedeu, expressamente, à efetiva revogação do art.º 189.º do CPP, revelar-se-á imperioso traçar o historial evolutivo desta cláusula de extensão, questionando-se a vigência e aplicação desta disposição legal no que toca a interceção de mensagens de correio eletrónico já armazenadas em suporte digital, bem como questionar o sentido e alcance prático da remissão do art.º 18.º da LC para o regime das escutas telefónicas.

Desta forma, sem descurar a exemplificação prática e os aspetos técnico - informáticos, sobre os quais não nos coibiremos de tecer breves considerações, ainda que comedidas, pois que apenas os caminhos do direito pretendemos trilhar, procuraremos com este estudo analisar a temática do correio eletrónico, particularmente, os meios de obtenção de prova a que está submetido no ordenamento jurídico processual penal português, questionando a sua conciliação, ou insana convivência, com as várias disposições processuais relativas à obtenção da prova digital consagradas no Código de Processo Penal, na Lei 32/2008, de 17 de Julho, e na Lei 109/2009, de 15 de Setembro, de forma a aferir se estamos perante um conflito de disposições processuais na obtenção da prova digital, ou se, pelo contrário, estamos perante disposições normativas processuais que se complementam entre si.

Assim, cientes que a relativa novidade da Lei em apreço acarreta consigo a necessidade de um estudo doutrinário e jurisprudencial aprofundado, porventura apenas alcançável com o decurso do tempo, procuraremos, paralelamente às posições doutrinárias e jurisprudenciais que traremos a palco, dar o nosso modesto contributo no que à temática diz respeito, designadamente, indagando sobre possíveis soluções processuais que permitam uma maior articulação entre disposições processuais.

1. O Nascimento da Sociedade da Informação

No proémio do segundo milénio, pressagiava BILL GATES que "*estamos nos anos iniciais de um tempo que chamo de "década digital" - uma era em que os computadores deixarão de ser meramente úteis para se tornar uma parte significativa e indispensável da nossa vida diária*"[2], anunciando o aparecimento de um encantador, mas também perigoso, mundo novo.

De facto, aquando da criação da Internet, em 1969, pelo governo norte – americano (com objetivos marcadamente militares[3]), não se atreveria o Homem a representar que se tinha acabado de dar início, após a imprensa escrita de *Gutemberg*, nos finais do Séc. XVII, a que se sucedeu a descoberta do telefone, por *Alexander Bell*, no início do Séc. XIX, e o engenho do computador[4], no Séc. XX, a uma das maiores invenções da história do mundo tecnológico, cujo impacto revelar-se-ia de tal forma astronómico acabando por metamorfosear os transversais veios da sociedade.

O aparecimento das modernas tecnologias de informação e de comunicação, permitiu, à escala planetária, que a Internet se desenvolvesse, derrubando fronteiras territoriais, sociais, económicas, culturais, etárias, linguísticas e raciais. A interligação mundial de computadores, redes e sistemas informáticos, alavancou e conquistou um espaço virtual comum. Se por um lado, é inquestionável, sobretudo nos países mais desenvolvidos, o papel fulcral da Internet ao nível de infraestruturas estratégicas e nevrálgicas do Estado, designadamente, em áreas como a economia, a educação, as redes de transportes, a justiça, a saúde e a segurança, não podemos olvidar que também o circuito

[2]Afirmação proferida em ocasião do *World Economic Forum,* realizado na cidade de Davos, em 23 de Janeiro de 2003. Disponível *online* no endereço https://www.microsoft.com/presspass/ofnote/01-03davos.mspx [acedido em 25 de Agosto de 2016].

[3] Na década de 1960, a União Soviética e os Estados Unidos, blocos ideológicos e politicamente opostos, disputavam entre si posições de poder e influência no mundo, ambicionando as duas superpotências o controlo absoluto dos meios de comunicação. Nesta medida, temendo o governo dos EUA um ataque russo às suas bases militares, o que ocasionaria que viesse a público informações sigilosas expondo as vulnerabilidades do país, tornar-se-ia necessário criar uma rede que descentralizasse informação. Nascia assim a ARPANet (*Advanced Research Projects Agency Network)* , criada pela ARPA.

[4] O primeiro computador eletromecânico programável foi construído, em 1936, por Konrad Zuse, engenheiro alemão, a partir de uma relês que executava os cálculos e dados lidos em fitas perfuradas. Destaque-se a particularidade de Zuse ter tentado vender o computador ao governo alemão que, porém, desprezou a oferta, atendendo que não lhe vislumbrava nenhuma utilidade para fins bélicos. Nas descobertas do mundo tecnológico, destaque-se os contributos de John Napier (1550-1617), criador dos logaritmos e dos "*ossos de Napier*" e de Blaise Pascal (1623-1662), criador da calculadora.

das relações privadas, sejam elas de domínio económico/financeiro, institucional, ou simplesmente as estabelecidas em domínio social e pessoal (que proliferam com o nascimento das redes sociais, blogues e fóruns), foram projetadas para a era digital, assumindo-se a Internet como um veículo privilegiado de informação[5]. A passos largos, num curto espaço de tempo, por força do trilho informático, fomos caminhando para uma "sociedade global", também apelidada de *"*sociedade da informação*"*[6] ou "sociedade digital*"*[7]*,* sedenta de informação, manietada a um mundo virtual, tendo rapidamente o nosso léxico sido enriquecido, a velocidade cruzeiro, com inúmeros termos cibernéticos que, até então, nos eram completamente alheios e os quais, por iliteracia informática, detemos extremas dificuldade em apreender.

É indiscutível que a popularidade da Internet advém da sua capacidade de proporcionar, a muito baixo custo, uma comunicação e circulação transnacional de informação, através de um conjunto de serviços e dados instantaneamente disponíveis. Esta fina malha de informação permitiu o desenvolvimento e perpetuação de novas formas de comunicação, fazendo sentido falar-se hoje do mundo como uma "aldeia global". Por intermédio da Internet podemos trazer ao cómodo do nosso lar, entre outros, as compras da mercearia, os produtos das nossas lojas favoritas, refeições, bilhetes de agências de entretenimento, viagens, bancos e notícias do mundo inteiro, tudo reduzido a polegadas de um pequeno ecrã e, conforme apregoado em milhões de campanhas publicitárias, à distância de "um click". Os recursos de interação e partilha de informação no ciberespaço são verdadeiramente inesgotáveis.

De tal modo, esta sociedade da informação a que hoje pertencemos, ano após ano, galga muralhas e multiplica-se no ciberespaço[8], conquistando inúmeros utilizadores. Pegando-se no estudo levado a cabo pela *Bareme Internet,* realizado em 2015*,* repare-se no

---

[5] DIAS, Vera Marques, *A Problemática da Investigação do Cibercrime*, Data Venia, Revista Jurídica Digital, Ano 1, n.º 1, Julho - Dezembro 2012, ISSN 2182-8242, p. 64-85.

[6] PINHEIRO, Alexandre Sousa, *Privacy e Protecção de Dados Pessoais: A Construção Dogmática do Direito à Identidade Informacional*, Associação Académica da Faculdade de Direito de Lisboa, AAFDL Editora, Janeiro, 2015, p. 94-107.

[7] ROVIRA DEL CANTO, Enrique, *Delincuencia Informática y Fraudes Informáticos*, Estúdios de Derecho Penal dirigidos por Carlos María Romeo Casabona, 33, Editorial Comares, Granada, 2002, p. 7-9.

[8] A génese do termo, remontando a 1984, foi popularizada por Willian Gibson que definiu o ciberespaço como sendo uma alucinação consensual experimentada diariamente por biliões de utilizadores. Nos anos subsequentes, foram surgindo outras definições que refletiam já uma perspetiva onde se cruzava a visão filosófica com a tecnológica. Por exemplo, em 1999, o filósofo Lévy considerou que o ciberespaço era definido como sendo o espaço de comunicação aberto pela interligação mundial dos computadores e das memórias dos computadores.

caso português, onde o número de utilizadores da Internet aumentou mais de 10 vezes nos últimos 18 anos, passando de uma percentagem de 6,3%, registada em 1997, para 65,4% no ano de 2015, correspondente a um número na ordem dos 5,6 milhões de utilizadores[9].

A interação dos cibernautas e a gradual utilização da Internet tornam a rede[10] extremamente poderosa, sendo uma fonte colossal de comunicação, circunstância que leva à afirmação de que, quem não está na *net,* está votado a uma condição de "ultrapassado", constituindo a Internet um verdadeiro portal de interconectividade entre o velho mundo, *"geográfica e temporalmente definido",* e o *"novo mundo da sociedade da informação",* inteligível, na sua grande maioria, apenas pelas novas gerações.[11]

Neste incrível mundo virtual, todavia, nem tudo são só vantagens. Se por um lado, a rede comporta, em si mesmo, os ideais de liberdade, oportunidade e acesso à informação, por outro lado, a Internet contempla uma dimensão obscura, consubstanciada numa enriquecida multiplicidade de oportunidades de cariz ilícito. Aceder à Internet é um pouco como abrir as janelas e as portas de nossa casa. Sem os devidos percalços, corremos sempre o risco de ter intrusos indesejados, podendo a navegação, que se esperaria serena e pacífica, revelar-se um autêntico naufrágio. Assim, com alguma ingenuidade e profundo desconhecimento de redes, aliada à carência ou inoperância de segurança dos nossos equipamentos informáticos, tornamo-nos alvos extremamente fáceis e vulneráveis face à forma como nos expomos quando acedemos remotamente à rede.

Ora, equivale isto dizer, muitos utilizadores, astuciosamente e mal-intencionados, descobriram na Internet a pólvora para atuações ilícitas e lesivas, servindo-se da rede para a prática, entre outros, de crimes de burla (repare-se nos exemplos da fraude no arrendamento de casas de férias ou na apropriação de dinheiro por via do acesso ilegítimo

---

[9] Informação extraída do estudo levado a cabo, em 2016, pela Bareme Internet (Grupo *Marktest*), disponível *online* no endereço http://www.marktest.com/wap/a/n/id~209b.aspx [acedido em 5 de Setembro de 2016].

[10] Segundo MANUEL CASTELLS, a rede é *"um conjunto de nós interligados. As redes são formas muito antigas da actividade humana, mas atualmente essas redes ganham uma nova vida, ao converterem-se em redes de informação, impulsionadas pela Internet. As redes têm enormes vantagens como ferramentas organizativas, graças à sua flexibilidade e adaptabilidade, caraterísticas fundamentais para sobreviver e prosperar num contexto de mudança permanente. (...) Contudo, atualmente a introdução de novas tecnologias de informação e de comunicação de base informática, e em especial da Internet, permite que as redes desdobrem a sua flexibilidade e adaptabilidade, afirmando a sua natureza evolutiva. Assim, essas tecnologias permitem a coordenação de tarefas e a gestão da complexidade (...) O que permite o desenvolvimento de uma forma organizacional superior da actividade humana".* CASTELLS, Manuel, *A Galáxia Internet, Reflexões sobre a Internet, Negócios e Sociedade, Serviço de Educação e Bolsas,* Fundação Calouste Gulbenkian, Lisboa, 2004, p. 15-16.

[11] SANTOS, Paulo, BESSA, Ricardo e PIMENTEL, Carlos, *Ciberwar – O Fenómeno, as Tecnologias e os Actores*, FCA – Editora de Informática, Janeiro 2008.

a credenciais de contas bancárias), devassa da vida privada, usurpação de identidade (por via, por exemplo, do acesso ilegítimo a contas de correio eletrónico, ou a redes sociais, como meio para obter proveitos materiais através de outros ilícitos como a ameaça, extorsão ou falsificação de documentos), acesso ilegítimo a servidores e computadores de particulares e dos Estados, sabotagem informática (por via da disseminação de *software* malicioso nos sistemas informáticos), enfim, toda uma panóplia de ilícitos que, de forma assombrosa e intimidante, expõe as densas vulnerabilidades dos sistemas informáticos.

Doutro passo, os sistemas de informação e comunicação, permitindo o anonimato, têm demonstrado que por baixo da *Surface Web,* isto é, onde estão alojados os conteúdos da Internet facilmente acessíveis e devidamente indexados, existe um submundo virtual, designado de *Deep Web*[12], não acessível a motores de busca, que é totalmente desconhecido da generalidade das pessoas que acedem à Internet, e onde acaba por estar "enterrada" a maioria dos conteúdos ilícitos associados, por exemplo, à pornografia infantil, ao terrorismo, ao mercado negro de tráfico de órgãos e armas. Recorrendo-se ao exemplo de MICHAEL BERGMAN, imagine-se um barco a arrastar uma rede de pesca na superfície do oceano. Ainda que se possa pescar um grande peixe, permanece, todavia, uma grande quantidade de informação que está em águas profundas e que não pode ser pescada.

Assim, com o aparecimento dos inúmeros equipamentos móveis munidos de tecnologia de ponta, que permitem o acesso à Internet em praticamente qualquer lugar, o amplo leque dos recursos e fontes abertas de informação, assim como a proliferação das chamadas redes sociais, o espaço cibernético tornou-se propício a uma multiplicidade de condutas lesivas e ilícitas, praticáveis e praticadas na Internet, ou por intermédio dela. De facto, foi descoberto campo fértil, vulnerável, de lucro fácil, com riscos físicos inexistentes e com uma grande probabilidade de impunidade, não só para o cometimento de novos crimes, como também para revisitar os crimes tradicionais, agora com a exponencial ajuda e cumplicidade da Internet.

---

[12] A expressão é da autoria de MICHAEL BERGMAN. *Vide* BERGMAN, Michael, *The Deep Web: Surfacing Hidden Value*, BrightPlanet, Volume 7, Issue 1: *Taking License*, August, 2001, disponível *online* no endereço http://quod.lib.umich.edu/j/jep/3336451.0007.104?view=text;rgn=main [acedido em 16 de Setembro de 2016]. Sobre esta matéria, *vide,* ainda, RAMALHO, David Silva, *A investigação criminal na Dark Web*, Revista da Concorrência e Regulação, Ano IV, n.º 14/15, Almedina, Abril/Setembro 2013, p. 385-391.

2. A Criminalidade Informática

2.1. As Categorias do Cibercrime

Conforme temos vindo a expor, a interconexão de computadores e sistemas, aliada às sistemáticas e perpetuadas falhas de segurança, converteram o mundo do ciberespaço num autêntico "*El Dorado*" para a chamada *"virtual criminal communities",* criando um verdadeiro mundo *"underground",* tornando a prática de crimes informáticos cada vez mais frequente, diversa, móvel, evoluída, internacional e perigosa[13].

Neste domínio, no início da década de 70, com o aparecimento da criminalidade informática, o pensamento jurídico internacional foi confrontado com duas questões fundamentais que geraram controvérsia: a primeira, relacionada com a delimitação do universo das condutas ofensivas praticadas contra os meios informáticos, ou através deles, que deveriam catalogar-se de "crime informático"; a segunda, respeitante ao específico *nomen juris* a adotar para os crimes que lesassem os bens jurídicos relativos à propriedade, ao uso, à segurança, à funcionalidade dos computadores e conjunto de equipamentos periféricos (vulgo *hardware*), e ao funcionamento das redes e sistemas de computadores e telecomunicações que neles é possível correr (vulgo *software*).

De facto, ainda que não exista consenso doutrinal e jurisprudencial quanto à delimitação do conceito de "*criminalidade informática*", ou "*crimes informáticos*"[14], julgamos fazer sentido, como o vem fazendo a legislação internacional e nacional (as quais oportunamente nos pronunciaremos), utilizarmos a designação de "*cibercrime*" (sem prejuízo de utilizarmos outros termos conexos), para catalogar, ampla e abstratamente, todos os crimes relacionados com uma área tão complexa como é a informática, e em que o meio informático seja penalmente relevante.

Neste conspecto, a Comissão Europeia inclui no cibercrime três categorias de atividade criminosa: os crimes tradicionais, cometidos com o auxílio do computador e redes informáticas; os crimes de publicação de conteúdos ilícitos, designadamente, crimes relacionados com a publicação de conteúdos ilícitos que incitam ao terrorismo, à violência, ao racismo e xenofobia ou ao abuso sexual de menores; e os crimes exclusivos das redes

[13] SALOM CLOTET, Juan, *Delito Informático y su Investigación*, Cuadernos de Derecho Judicial, III, Consejo General Del Poder Judicial, Centro de Documentación Judicial, 2006, p. 106.

[14] A prática de crimes na internet assume várias denominações, entre elas: crime digital, crime informático, crime informático-digital, "*high technology crime*" ou mesmo "*computer related crime*".

eletrónicas, que são cometidos exclusivamente por meio informático, tratando-se de crimes novos e desconhecidos na era pré-Internet.[15]

Entre nós, GARCIA MARQUES e LOURENÇO MARTINS consideram frequente encarar a criminalidade informática como "*todo o acto em que o computador serve de meio para atingir um objectivo criminoso, (…) em que o computador é o alvo simbólico desse acto ou em que o computador é objecto do crime*"[16]. Por seu turno, BENJAMIM SILVA RODRIGUES insere o crime informático em categorias diferentes: o crime informático digital próprio/puro, em que "*o sistema informático ou o fluxo informacional ou comunicacional que nele se encontra armazenado é o objecto da conduta criminosa*", e o crime digital impróprio/impuro, em que o "*sistema informático é um meio para a prática de crimes informáticos*"[17]. Também PEDRO VENÂNCIO, a este propósito, faz a divisa da criminalidade informática em sentido amplo, englobando "*toda a panóplia de actividade criminosa que pode ser levada a cabo pelos meios informáticos, ainda que estes não sejam mais do que um instrumento para a sua prática, mas que não integra o seu tipo legal, pelo que o mesmo crime poderá ser praticado por recurso a outros meios"*, da criminalidade informática em sentido estrito, abarcando *"aqueles crimes em que o elemento digital surge como parte integrador do tipo legal ou mesmo como seu objecto de proteção"*[18], enquanto RUTE SANTOS, por sua vez, alude a uma catalogação tripartida assente nos "*crimes tipicamente informáticos"* (os crimes ligados eminentemente à informática), nos "crimes *essencialmente informáticos"* (onde o bem jurídico ofendido é de natureza informática), e nos crimes "*acidentalmente informáticos"* (em que o computador é apenas instrumento, não contendendo com o preenchimento do tipo legal de crime)[19].

Doutro compasso, a maioria da doutrina portuguesa, seguindo de perto OLIVEIRA ASCENSÃO[20], diferentemente, delimita a atividade criminosa associada ao

---

[15]Conteúdo disponível *online* no endereço http://eur-lex.europa.eu/legal-content/PT/TXT/?uri= URISERV: l14560 [acedido em 25 de Setembro de 2016].
[16] MARQUES, Garcia e MARTINS, Lourenço, *Direito da Informática*, 2ª Edição, Almedina, Coimbra, 2006, p. 639 e ss.
[17] RODRIGUES, Benjamim Silva, *Direito Penal Especial, Direito Penal Informático – Digital*, Coimbra Editora, 2009, p. 147, 279 e ss. e 351 e ss.
[18] VENÂNCIO, Pedro Dias, *Lei do Cibercrime – Anotada e Comentada*, Coimbra Editora, Janeiro 2011, p. 11 e ss.
[19] SANTOS, Rita Coelho, *O Tratamento Jurídico-Penal da Transferência de Fundos Monetários Através da Manipulação Ilícita dos Sistemas Informáticos*, Coimbra Editora, 2005, p. 32 e ss.
[20] ASCENSÃO, José de Oliveira, *Estudos sobre Direito da Internet e da Sociedade da Informação*, Livraria Almedina, Coimbra, 2001, ISBN 163116/01, p. 261-262. No mesmo sentido, *vide* VERDELHO, Pedro,

cibercrime nos seguintes domínios: os crimes que *"recorrem a meios informáticos",* não alterando o tipo penal comum (como são exemplo a devassa por meio de informática - art.º 193º do CP - e o crime de burla informática nas telecomunicações - art.º 221.º do CP); os crimes *"relativos à protecção de dados pessoais ou da privacidade"* (Lei nº 67/98, de 26/10, e a Lei nº 69/98, de 28/10); os crimes *"informáticos propriamente ditos"*, sendo o bem ou o meio informático o elemento típico autonomamente relevante (v.g. os crimes previstos na Lei nº 109/2009, de 15/09) e os crimes *"relacionados com o conteúdo"*, onde se destacam a pedofilia, o terrorismo, a violação do direito de autor, a difusão de pornografia infantil (art.º 172.º, n.º 3, alínea d), do CP) ou a discriminação racial ou religiosa (art.º 240.º, n.º 1, al. a), do CP), na "*medida em que a reação repressiva se tenha de especializar por força do meio utilizado*".

2.2. Os Sujeitos do Cibercrime

2.2.1. O Sujeito/Agente Ativo

O fenómeno da globalização cibernética, que já aqui retratamos, trouxe consigo o nascimento de distintos sujeitos criminosos, com diferentes modos de atuação e com diversas motivações, demonstrando que o perfil do criminoso informático não obedece a um padrão uniformizador[21], podendo, inclusive, aparecer sob a veste de pessoa coletiva.

No mundo virtual do crime, destacamos o *Hacker*[22] como o sujeito mais popular na prática de crimes informáticos. Fundamentalmente, podemos definir o *hacker* como um indivíduo que, sem autorização do seu legítimo titular, acede a computadores, sistemas e redes informáticas ou telemáticas alheias, com intuito de conhecer e modificar os aspetos mais internos de dispositivos, programas e redes de computadores. Devido aos seus conhecimentos informáticos, *o hacker* consegue contornar os limites do funcionamento

---

Cibercrime, in AA. VV., *Direito da Sociedade da Informação*, APDI (Associação Portuguesa de Direito Intelectual), Volume IV, Coimbra Editora, 2003, p. 347.

[21] ROVIRA DEL CANTO, Enrique, *Delincuencia Informática*…, p. 108. GARCIA MARQUES e LOURENÇO MARTINS ordenam a tipologia dos delinquentes informáticos entre amadores, perturbados, membros do crime organizado, quebra sistemas e extremistas idealistas. MARQUES, Garcia e MARTINS, Lourenço, *Direito da Informática*, Lições de Direito da Comunicação, Almedina, 2000, p. 500.

[22] Etimologicamente é um termo anglo – saxónico que deriva do verbo "*to hack"*, que significa "cortar grosseiramente", por exemplo, com uma catana.

"normal" dos sistemas, rompendo as barreiras de segurança que, supostamente, deveriam impedir o controlo dos sistemas e acesso a específicos dados[23]. Globalmente, é visto como um indivíduo aceite e não censurado pela sociedade, sendo, depois de condenado, contratado por grandes grupos económicos para ocupar cargos de relevo, com a finalidade de colaborar nos fins estratégicos e conexos à eliminação das falhas de segurança dos sistemas informáticos[24]. Por tal motivo, é alguém descrito como um verdadeiro génio e perito na área da informática, experiente e exímio no manuseamento de computadores e programação, homem com Q.I. acima da média, introvertido, antissocial, e com um frenético desejo em expor as falhas dos sistemas almejando notoriedade. Não será, pois, de estranhar que, na sua génese, a figura do *hacker* esteja associada ao *Hactivism*[25], devido ao facto da prática do crime estar instrumentalizada para a difusão de causas e mensagens, principalmente, contra Estados e Organizações. Entre os *hackers* mais famosos do mundo destacamos os nomes de Kevin David Mitnick[26], Gary McKinnon[27] e Julian Paul Assange[28].

Gradualmente, o mundo do cibercrime vai ganhando novas dinâmicas e contornos, tornando-se cada vez mais acessível para a chamada delinquência embriagada pelo *animus lucrandi*. O objetivo já não é criar ou alterar sistemas, mas sim extrair

---

[23] No seio do mundo do cibercrime é sagrada a distinção entre *hacker*s e *crackers*, distinção que assenta no facto dos *crackers* terem como objetivo a corrupção e quebra dos programas e sistemas informáticos, tornando-os inoperativos e inutilizáveis.

[24] BLASCO, Andrés, *Qué Es Internet?*, Principios de Derecho de Internet, Prainter, Tirant lo Blanch, Valencia, 2002, p. 52.

[25] O *Hactivism* é a mistura do "*hacking*" com o "*activism*". O ativista usa técnicas de *hacking* para promover as suas ideias e convicções, de modo a poder influenciar a tomada de decisões (ex. o grupo *Anonymous*). *Vide* SANTOS, Paulo, BESSA, Ricardo e PIMENTEL, Carlos, *Ciberwar – O Fenómeno, …*, p. 75-84.

[26] Mitnick cometeu os primeiros crimes em 1990, após ter acesso a número incalculável de computadores, operadoras de telecomunicações, empresas de tecnologia e servidores da Internet. É conhecido por ser um verdadeiro génio informático. Utiliza o nickname "*Condor*", tendo servido de inspiração para a criação do filme "*Os três dias do Condor*". O seu exuberante golpe informático, por via do acesso às redes do FBI e a redes militares, teve como consequência uma pena de prisão em 1995, tendo sido libertado em 2000. Trabalha atualmente como consultor de segurança na *Web*.

[27] McKinnon é um *hacker* escocês, tendo sido condenado, em 2008, à extradição para os EUA, após ter tido acesso e danificado, entre fevereiro de 2001 e março de 2002, mais de 57.000 computadores do exército americano.

[28] Assange estudou matemática e física, antes de se tornar porta-voz e editor-chefe do *WikiLeaks*. Fundou o *WikiLeaks* em 2006, ganhando vários prémios pela a atividade aí desenvolvida (com destaque para o "*Sam Adams Award*" e o "*Index on Censorship"* do *"The Economist*", em 2008), além de ter sido considerado o "homem do ano" pelo jornal francês "*Le Monde"* em 2010. Neste mesmo ano, trouxe a público um vasto conjunto de documentos sobre possíveis crimes de guerra, cometidos pelo exército dos EUA na guerra do Afeganistão e na guerra do Iraque. Em 2011 foi incluído na lista da revista "*Times*" como uma das 100 personalidades mais influentes do planeta. Assange encontra-se, desde junho de 2012, enclausurado na embaixada do Equador, em Londres, sob asilo político.

informação e usá-la ou vendê-la, concluindo a EUROPOL, num estudo por si publicado, que o "*cibercrime é mais rentável do que muitos outros crimes como o tráfico de droga*"[29], atendendo ao facto do lucro ser extremamente fácil de obter, privilegiando o anonimato e a não envolvência física entre o autor e a vítima, tornando a ação mais aliciante, moralmente tolerável, e com menos riscos para o autor do crime. Por seu turno, não podemos olvidar que, em si mesma, a própria Internet, através de um vasto conjunto de *sites*, vídeos demonstrativos, e propriamente as redes sociais, ensina, com algum detalhe, o "*modus operandi*" para a prática destes crimes por parte do chamado criminoso de oportunidade[30], nomeadamente, disponibilizando *softwares e hardwares* que permitem facilitar e contornar as falhas de segurança, quebrando assim a resistência que o comum delinquente, no mundo real, teria para a prática da conduta criminosa.

Um outro grupo conhecido do mundo cibernético são os chamados "cibercriminosos de colarinho branco" (conhecidos também por *insiders*). De modo geral, são funcionários altamente qualificados e colaboradores de magna confiança da entidade patronal que, tendo permissão para aceder aos sistemas informáticos, e aliando o seu *know-how* informático ao conhecimento interino da unidade empresarial, exploram as suas debilidades, aí praticando atividades ilícitas, como alterações informáticas, eliminação de dados, sabotagem de sistemas ou serviços e venda de informações confidenciais a concorrentes.[31]

Na catalogação dos sujeitos cibercriminosos é inevitável, atendendo à dimensão que os conflitos têm gerado e por serem os delinquentes mais temidos, falar-se nas organizações criminosas e nos ciberterroristas. O cenário do ciberterrorismo é algo que, depois das tragédias de 11.09.2001, nos EUA, de 11.03.2004, em Espanha, de 07.07.2005, no Reino Unido (novamente fustigado no ano de 2017), e, mais recentemente, em França (13.11.2015) e Bélgica (22.03.2016), ganhou pesado contorno na segurança dos estados,

---

[29] EUROPOL, *High Tech Crimes Within The EU: Old Crimes New Tools, New Crimes New Tools, Threat Assessment*, High Tech Crime Centre, 2007, p. 4 e 54. Conteúdo disponível *online* no endereço https://www.enisa.europa.eu/topics/nationalcsirtnetwork/files/eventfiles/ENISA_Europol_threat_assessment_2007_Dileone.pdf [acedido em 25 de Setembro de 2016].

[30] NETO, João Monteiro, *Crimes informáticos uma abordagem dinâmica ao direito penal informático*, Pensar Fortaleza, vol. 8, n.º 8, Fevereiro, 2003, p. 41 a 43, Conteúdo disponível *online* no endereço http://periodicos.unifor.br/rpen/article/view/736/1598 [acedido em 27 de Setembro de 2016].

[31] As motivações da delinquência podem aqui ser de variada ordem, destacando-se o descontentamento, a revolta contra a entidade empregadora, a resolução de problemas financeiros, a ganância, a vingança, a ascensão profissional ou simplesmente a falta de ética e de deontologia profissional. SANTOS, Paulo, BESSA, Ricardo e PIMENTEL, Carlos, *Ciberwar – O Fenómeno*…, p. 69-73.

podendo, inclusivamente, dizer-se que é um "dossier" de interesse mundial. A maioria das organizações criminosas usa a Internet, tanto para coordenar os membros, como para blanquear – *cyber laundering* – e dissimular as suas condutas ilícitas, recrutando ou contratando técnicos altamente especializados, usando também o cibercrime como forma de financiamento. Sendo a Internet um veículo rápido, barato, anónimo, remoto e global para divulgar informações e propagandas terroristas, assim como para recrutar novos membros de todas as nacionalidades e treiná-los, sem necessidade da presença física, é latente a preocupação com que hoje, na sua globalidade, todos os Estados se mostram preocupados com a sua segurança interna, nomeadamente, a devastação que um ataque terrorista pode provocar na rede eletrónica de sistemas de dados e na economia global, concretamente, paralisando sistemas e serviços, provocando o verdadeiro caos.

2.2.2. O Sujeito Passivo – A Vítima.

O estudo da vítima e a relação com o cibercriminoso, no âmbito do cibercrime, tem-se revelado solo fértil e propício para a identificação do agente, bem como o seu relacionamento e raio de ação no ciberespaço. No fundo, no campo da análise da vitimologia, é possível avaliar se estamos perante uma vítima – alvo, sendo a sua escolha intencional e criteriosamente selecionada[32], ou se, pelo contrário, estamos perante uma vítima colateral (também designada de vítima simbólica[33]), resultante de um ilícito que não a visava especificamente, eventualmente, resultado de um ataque informático em massa.

Por via de regra, as vítimas singulares são utilizadores incautos, com um conhecimento dos sistemas informáticos de nível básico, ou puramente inexistente, não atribuindo particular importância às questões de segurança informática, permitindo que, sob manifesta negligência, facilmente se introduzam no seu equipamento programas maliciosos. Na generalidade dos casos, a vítima fornece *passwords* e dados pessoais *online* (como sucede no caso do *phishing*[34]), sem verificar a sua fidedignidade, ingenuidade esta

[32] Casos em que existiu entre o agente e a vítima um elo de ligação, por via de um relacionamento amoroso, ou um vínculo contratual, ajudam a compreender a motivação do agente na prática do crime.
[33] CASEY, Eoghan, *Digital Evidence and Computer Crime, Forensic Science, Computers and the Internet*, Academic Press, 2000, p. 164-175.
[34] Fraude eletrónica em que o agente, utilizando ferramentas ou aplicações, se faz passar por uma pessoa ou empresa no intuito de adquirir dados pessoais de diversos tipos: senhas de contas, dados financeiros, números de cartões de crédito, entre outros dados. O *modus operandi* do crime, usualmente, consiste em remeter um *e-mail* à vitima como engodo para o fornecimento dos seus dados pessoais.

que origina a prática de uma multiplicidade de crimes informáticos[35]. Ainda assim, diga-se em abono da verdade, mesmo que o utilizador utilize medidas preventivas ou de proteção, estas não são infalíveis, sendo quase impossível, mesmo para um *expert* em informática, navegar na Internet sem ser alvo de um vírus informático ou de um *site* comprometedor.

Frequentemente, apesar de não ser do conhecimento público, em parte devido ao descrédito e desconfiança que poderia originar tal facto, e outra parte atendendo ao enorme prejuízo que daí poderia advir (por força da perda de reputação e confiança junto do mercado e clientes), as vítimas são muitas vezes empresas, como bancos, seguradoras e entidades financeiras. Tais ataques informáticos, por uma questão de estratégia, são normalmente silenciados, sendo preferível a resolução do problema internamente, em detrimento da apresentação de queixa junto das autoridades. Outros dos estigmas do silêncio prendem-se com o facto do desconhecimento ou da ignorância do sujeito passivo, de que se foi alvo de um ataque, ou simplesmente a descrença na investigação policial e o sentimento de impunidade destes crimes.

O problema coloca-se quando não se alcança a amplitude do ataque informático, nomeadamente, nos casos em que, por força do acesso ao sistema informático por parte do cibercriminoso, a confidencialidade dos dados foi quebrada. É inegável que a não cooperação e colaboração da vítima impede uma melhor avaliação das imperfeições e riscos dos sistemas informáticos, bem como o aumento do *know - how* das autoridades, originando que a qualidade das medidas de segurança e dos meios de deteção do cibercrime, bem como propriamente de obtenção da prova digital, sejam postos em causa.

De tal forma, desde que ligada a um sistema ou rede informática, a vítima do cibercrime poderá ser qualquer pessoa, física ou jurídica, individual ou coletiva, pública ou privada.

Feita esta genérica contextualização dos meandros do cibercrime, deveras essencial para perceber a sua abrangência e a sua íntima relação e dependência com as comunicações eletrónicas, é hora de nos debruçarmos, em definitivo, sobre as questões jurídicas relacionadas com o correio eletrónico.

[35] CABO, Ana Isabel, *Nova lei facilita investigação da Criminalidade Informática*, Boletim da Ordem dos Advogados, n.º 65, Abril 2010, p. 31.

3. A Prova Digital nos Fluxos Comunicacionais

3.1. O Ato Comunicacional

Afirmava Aristóteles que "*o Homem é um ser eminentemente social. Para viver isolado, só se for um bruto ou um Deus*", pretendendo sobrelevar a circunstância de que o Homem tem absoluta necessidade de unir-se a seus pares, não apenas para realizar os fins que deseja, mas também para desenvolver em pleno as suas capacidades. O Homem está, pois, destinado à Pólis e dela é parte integrante[36].

Na nossa vida pessoal e profissional, a comunicação constitui-se como um elemento de extrema importância para que possamos transmitir a outrem informações, factos, ideias, ou mesmo desejos, tornando-se intuitivo e expectável que, em virtude de tal comunicação, as informações produzidas e transmitidas pelo emissor causem um impacto na vida do recetor, cujas consequências se podem fazem sentir de variadas formas e maneiras, desde a mais positiva até à mais negativa. Na verdade, todos nós precisamos de nos fazer entender e entendermos os outros.

Ao desenvolver a linguagem, seja ela gestual ou verbal, a espécie humana permitiu, desde os primórdios dos tempos, dar a conhecer os perigos que o mundo oferecia e, dessa forma, alertar a restante prole para o seu efeito. Comunicar, seja num ato comunicacional de presença física, seja à distância, faz assim parte da vida humana, sendo através deste processo, tão natural e instintivo, que partilhamos o que somos e a forma como gostaríamos de vir a ser. De tal forma, na esteira de FARIA COSTA, alumiando à destrinça conceptual entre informação e comunicação, podemos afirmar que "*o acto comunicacional é, por conseguinte, afirmação e descoberta do `outro´. A esta natureza de alteridade em que a comunicação se efectiva, contrapõe-se a informação como realidade objectivável e, por isso, independente da captação subjectiva e dialógica do homem*".[37]

Neste exercício de dialética, logo numa primeira nota, é importante considerar que, para que exista reciprocidade entre emissor e recetor, antes de tudo, dever-se-á ter presente que o ato comunicacional se inicia a partir do momento em que o emissor dirigiu, a concreto recetor, determinada mensagem, tornando-se a comunicação perfeita no

[36] LÉVY, André, CASANOVA, Catarina, GASPAR, Augusto e VIEIRA, António Bracinha, *Homem: Origem e evolução*, 2.ª edição, Edição Glaciar, Maio de 2015, ISBN: 978-989-8776-21-1.
[37] COSTA, José de Faria, *O direito penal, a informática e a reserva da vida privada, Direito Penal da Comunicação – Alguns escritos*, Coimbra, Coimbra Editora, 1998, p.66.

momento em que este último toma conhecimento do seu teor. Nas comunicações à distância, ao contrário do que ocorre entre presentes, o emissor recorre a terceiros confiando-lhes a tarefa de levarem a mensagem até ao destinatário. Neste cômputo, a comunicação já não se opera num único momento, deixando de depender apenas do emissor, perdendo a forma e natureza de uma comunicação direta e imediata, convertendo-se o ato comunicacional, como alude PEDRO GONÇALVES[38], numa relação triangular entre o emissor, o agente que transporta a comunicação e o recetor.

Assim, antes de avançarmos na exposição e nos curvarmos mais incisivamente na natureza jurídica do correio eletrónico, importa, desde já, ter presente que as questões relacionadas com a ponderação da comunicação fechada, por oposição à comunicação aberta[39], levam-nos à basilar premissa de considerar que o ato comunicacional fechado, pressupõe que a informação que viaja na comunicação tenha um recetor pré-determinado pelo emissor, independentemente de ocorrer sob a forma escrita ou oral, gerando-se a legítima e tutelada expetativa que a comunicação ocorra "*dentro de um certo e preciso número de intervenientes",* que esperam que o terceiro leve a cabo, *"de maneira eficaz, a protecção desse fechamento ou clausura*"[40].

3.2. Do Correio Tradicional ao Correio Eletrónico

Não obstante as dúvidas existentes quanto a etimologia da palavra correio, fontes históricas remontam o nascimento do vocábulo à Antiga Grécia, cerca de 190 anos a.C., provinda do ato de correr. Conta-se que um general grego, para fazer anunciar a vitória que tinha alcançado em Maratona contra os Persas, enviou Fidípides, um dos seus soldados, a Atenas para anunciar tal feito. Desgraçadamente, após correr até à cidade Grega, o soldado terá proferido a palavra "vitória", jazendo no solo devido ao cansaço[41]. Conceptualmente,

[38] GONÇALVES, Pedro, *Direito das Telecomunicações,* Almedina, Coimbra, 1999, p.11. A este propósito, fala-nos COSTA ANDRADE de uma "*relação triádica*", referindo-se a relação comunicacional que é estabelecida entre o emitente e o destinatário, interpondo-se o mediador que oferece o serviço da transmissão. ANDRADE, Manuel da Costa, *Comentário Conimbricense do Código Penal: parte especial*, Dir. Jorge de Figueiredo Dias, Américo Taipa de Carvalho, 2ª ed., Coimbra, Coimbra Editora, 2012, ISBN 9789723220612, p. 1095.

[39] A comunicação aberta contempla um universo de recetores, não previamente determinados, sendo reproduzível e percetível em vários tempos e lugares (v.g. imprensa, rádio e televisão).

[40] COSTA, José de Faria, *O direito penal, a informática*…, p.87.

[41] RAMOS, Armando Dias, *A Prova Digital em Processo Penal*, Chiado Editora, 1.º ed., Novembro 2014, p. 24.

com a evolução dos povos e transformações societárias, o termo foi ganhando significado, associando-se, hoje, os "correios" aos postos de envio, receção e distribuição de correspondência postal e mercadorias[42].

Nos marcos históricos da evolução dos meios de comunicação, à semelhança do que *Bell* tinha feito com o seu telefone,[43] inscreveu Ray Tomlinson o seu nome junto a uma das mais brilhantes descobertas do mundo dos engenhos tecnológicos: o correio eletrónico. Com efeito, decorria o ano de 1971, quando Tomlinson, programador informático norte – americano, conseguiu a proeza de enviar a primeira mensagem eletrónica, entre computadores, por via da rede ARPANet. De tal modo, após descobrir que o símbolo "@"[44] não se encontrava associado a nenhum nome próprio, deslindou que este sinal seria o ideal para separar o *user* (nome da pessoa) e o *host* (servidor) que iria hospedar a mensagem. Ora o facto é que, embora se tivesse tratado de um pequeno passo para o Homem, o contributo de Ray Tomlinson acabaria por se tornar num gigantesco passo para a humanidade, abrindo um capítulo extraordinário na era das telecomunicações[45], revolucionando o processo comunicacional. Com os sucessivos *booms*

---

[42] Os correios estão hoje apetrechados com um amplo leque de serviços, inclusive, na área da banca e soluções empresariais.

[43] As primeiras linhas telefónicas instaladas em Portugal, foram construídas nas cidades de Lisboa e Porto, no início de 1880, sob a alçada da *Edison Gower Bell Telephone Company of Europe Limited*, acabando, no início do séc. XIX, os CTT, Correios e Telégrafos, por se expandir à rede telefónica. Sobre a matéria *vide* MADUREIRA, Raquel Castro, DUARTE, A. Manuel e FONSECA, Raquel Matias, *133 anos de Histórias das Comunicações em Portugal*, Electrónica e Telecomunicações, Revista da Universidade de Aveiro, vol. 5, n.º 3, Junho 2011.

[44] Vulgarmente designado de arroba, tem o seu significado em inglês de "*at*" (em tal lugar). Inúmeras são as teorias quanto à origem do símbolo "@", sendo que, na mais antiga, aparece associado a fins mercantilistas para abreviar o custo unitário de determinado bem "*cada uma a*".

[45] O conceito de "telecomunicação" foi o primeiro a ser utilizado tanto na legislação penal, como pelas Leis de Bases de Telecomunicações (Leis n.ºs 88/89, de 11/09, e 91/97, de 1/08 – contemplando este último diploma, no art.º 2.º, n.º1, uma definição do termo). Com a revogação da Lei 91/97, de 01/08, pela Lei 5/2004, de 10/02, o conceito de telecomunicação, segundo COSTA ANDRADE, "*perdeu o seu lugar central – passando a ser objecto de remissões e referências mais ou menos indiretas – parecendo substituído pelo conceito de comunicações eletrónicas"*. De tal forma, e não obstante a "*obstinada teimosia*" do legislador, conforme alude BENJAMIM SILVA RODRIGUES, fruto da não atualização de diplomas, alguns Autores vêm a realçar a importância da terminologia da palavra "telecomunicação" firmando o facto do CP e da CRP (v.g. art.ºs 194.º e 384.º do CP) se encontrarem desatualizados, pois que, fruto da evolução tecnológica, as telecomunicações deram lugar às comunicações eletrónicas, apoiando-se, entre outros, no facto do termo ser já utilizado em diversos diplomas dispersos pela legislação nacional (ex. art.º 2, n.º 1, al. a) da Lei n.º 41/2004, de 18/08 e art.º 3, al. cc), da Lei n.º 5/2004 de 10/02). Não obstante, e porque nos encontramos confinados à letra da Lei mãe, conforme COSTA ANDRADE, o conceito "*continua a deter consistência e autonomia*" cobrindo a salvaguarda das "*intromissões nas comunicações eletrónicas*". 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, p. 157. RODRIGUES, Benjamim Silva, *Da Prova Penal – Tomo II, Bruscamente…A(s) Face(s) Oculta(s) dos Métodos Ocultos de Investigação Criminal*, 1.ª Edição, Editora Rei dos Livros, Abril, 2010, p. 341-344. COSTA, José de Faria, *As telecomunicações e a privacidade: o olhar (in)discreto de um penalista*, As Telecomunicações e o Direito

da tecnologia, o modo de envio de mensagens foi aperfeiçoado, começando a surgir o aparecimento de novos protocolos[46] de transmissão/receção de mensagens, bem como o surgimento de servidores de *Webmail*[47], como o *Hotmail, Gmail, Yahoo, entre outros.*

O correio eletrónico, ou *e-mail*[48] como é vulgarmente conhecido, ganhou assim uma grande dimensão nas nossas vidas, tanto mais que, devido às suas características, fundamentalmente, a celeridade e os baixos custos, tornou-se num privilegiado veículo de informação de envio e receção de correspondência, extremamente acessível a partir de dispositivos fixos, como computadores, ou dispositivos móveis, como *smartphones, PDA`s, Tablets*, entre outros. Estamos, assim, conforme nos demonstram IRENE ALBARRÁN LOZANO, CARMEN DE PABLOS HEREDERO E ANTONIO MONTERO NAVARRO[49], perante um meio de comunicação que é: "*Eletrónico"*, porque utiliza meios eletrónicos de gestão e de transporte; "*Assíncrono"*, atendendo que não existe necessidade de sincronia entre envio e receção; "*Ubíquo"*, dada que permite o seu acesso em locais diferentes; "*Digital"*, pois apenas utiliza a informação digitalizada e "*Informático"*, porque relacionado com as tecnologias da informação.

Não tenhamos dúvidas, dentro da era das comunicações eletrónicas, o correio eletrónico projetou-nos para uma nova realidade na forma de comunicar, não tendo sido com estranheza que o legislador, de modo a possibilitar a identificação de condutas desviantes, sentiu necessidade de adaptar as leis penais a este moderno meio de comunicação.

De forma incompreendida, não obstante a dispersa legislação extravagante que o nosso ordenamento jurídico dispõe em matéria de regulação informática, e sobre a qual, ao

---

na Sociedade da Informação, Instituto Jurídico da Comunicação, Faculdade de Direito da Universidade de Coimbra, Coimbra, 1999, p. 65.

[46] Designa-se por protocolo um conjunto de regras que definem o modo como a informação é formatada – os pacotes – e como os sistemas que constituem a Internet interagem de modo a garantir o fluxo coerente e eficiente de informação na Internet. COMER, Douglas, *Internetworking with TCP/IP*, Volume 1: Principles, Protocols, and Architectures, Fourth Edition, Prentice Hall PTR, Upper Saddle River, NJ, 2000, *apud* PORTELA, Irene, *A intercepção legal de comunicações em redes IP,* Revista de Estudos Politécnicos, Vol VI, nº 9, 2008, ISSN: 1645-9911, p. 4.

[47] *Webmail* é um interface que permite, a partir de um *browser* de acesso à Internet, consultar e enviar mensagens de correio eletrónico, sem necessitar de ter instalado no seu equipamento um programa específico para a leitura ou envio de correio eletrónico, sendo apenas necessário um computador ou outro dispositivo móvel ligado à Internet.

[48] Deriva do verbo inglês "*to mail"*, que significa mandar, enviar. O termo está associado a *electronic mail.*

[49] ALBARRÁN LOZANO, Irene, PABLOS HEREDERO, Carmen e MONTERO NAVARRO, Antonio, *Uso del correo electrónico: un análisis empírico en la Universidad Complutense de Madrid,* Documentos de Trabajo de la Facultad de Ciencias Económicas y Empresariales, nº 09, 1999, ISSN: 2255-5471. Conteúdo disponível online no endereço http://eprints.sim.ucm.es/6676/1/9909.pdf [acedido em 15 de Novembro de 2016].

longo deste trabalho, faremos a devida análise, somente com a Lei n.º 46/2012, de 29 de Agosto[50], tratou o legislador luso, no seu art.º 2.º, n.º1, al. b), de definir o correio eletrónico como "*qualquer mensagem textual, vocal, sonora ou gráfica enviada através de uma rede pública de comunicações que possa ser armazenada na rede ou no equipamento terminal do destinatário até que este a recolha*", entendendo-se por comunicação, nos termos da al. a), "*qualquer informação trocada ou enviada entre um número finito de partes mediante a utilização de um serviço de comunicações eletrónicas acessível ao público"*.

Até então, eramos forçados a recorrer à al. h), do art.º 2.º, da Diretiva 2002/58/CE[51], para obtermos um enquadramento legal que nos permitisse obter um conceito jurídico de correio eletrónico, sem prejuízo das definições que iam sendo alavancadas pela própria doutrina, de que é exemplo ROMEO CASABONA, para quem o correio eletrónico era uma *"modalidade de comunicação, em geral de caráter pessoal, que incorpora texto, som e imagem e que se serve das redes telemáticas como tecnologia de transmissão e dos sistemas informáticos (computadores e o software ou sistema lógico correspondente) como instrumentos de emissão e recepção entre dois ou mais comunicantes e nesse caso de armazenamento de mensagens*"[52], ou mesmo BENJAMIM SILVA RODRIGUES, definindo-o como "*qualquer mensagem textual, vocal sonora ou gráfica, combinada ou não, enviada através de um terminal de um ponto de uma rede pública de comunicações electrónicas para outro terminal conexionado a tal rede, podendo ser, temporária ou definitivamente armazenada na rede ou equipamento terminal do destinatário até que proceda à sua recolha, mediante "carregamento" e correspectivo "descarregamento", em equipamento informático que torna a mensagem humana perceptível (ou lisível) pelos vários sentidos (visão ou audição)"*[53]. De resto, de acordo com este mesmo Autor, o legislador utiliza a designação de "correio eletrónico" como uma

[50] O diploma veio alterar a Lei n.º 41/2004, de 18/08 (Lei do Tratamento dos Dados Pessoais e Privacidade nas Telecomunicações).

[51] Nos termos da diretiva, o correio eletrónico aparece definido como "*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.*".

[52] ROMEO CASABONA, Carlos María, *La protección penal de los mensajes de correo eletrónico y de outras comunicaciones de carácter personal a través de Internet*, Derecho y Conocimiento, Vol. 2, 2006, p. 129, também acessível *online* no endereço https://www.unifr.ch/ddp1/derechopenal/obrasportales/op_20080612_17.pdf [acedido em 23 de Novembro de 2016].

[53] RODRIGUES, Benjamim Silva, *Das Escutas Telefónicas à Obtenção da Prova [em ambiente digital]*, Tomo II, Coimbra, 2009, p. 500. A este propósito *vide* VEIGA, Armando e RODRIGUES, Benjamim Silva, *Escutas telefónicas, rumo à monitorização dos fluxos informacionais e comunicacionais digitais*, Coimbra Editora, 2ª Edição, 2007, p. 364.

espécie de "pedra angular" para se referir, em bloco, ao conjunto da multiplicidade de comunicações eletrónicas que estão englobadas neste conceito[54]. Tal ideia, porém, é contrariada por COSTA ANDRADE[55], na afirmação que o correio eletrónico é, em si mesmo, uma forma de telecomunicação, distinta de outras formas de comunicação eletrónica englobadas no conceito de telecomunicação, como é o caso das comunicações de voz realizadas através da Internet (*VoIP – Voice Over Internet Protocol*).

Mais recentemente, embora parecendo desabonar a pauta conceptual da Lei n.º 46/2012, de 29/08, quando afirma que a nível nacional não existe uma definição de correio eletrónico, ARMANDO DIAS RAMOS vem a definir esta forma de comunicação como se tratando de "*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 computador"*[56].

Com o devido respeito, não nos podemos ater a tais conceitos e, muito embora não se pretenda discorrer numa área tão específica e técnica como a da informática (não sendo de resto esta a sede própria para tal), em prol de uma melhor (de)composição do procedimento técnico informático do *iter* da mensagem de correio eletrónico, temos de "*meter a foice em seara alheia"* para explicar alguns conceitos que, ainda que de forma simples e reconhecidamente lacunosa, estão inerentes a esta forma de comunicação.

3.3. Da Comunicação entre Máquinas – "O Diálogo Protocolar"

Conforme avançamos, genericamente, a Internet é concebida por se tratar de uma rede global, por sua vez constituída por milhões de redes de computadores e outros sistemas, sejam eles privados ou públicos, ligados entre si através de tecnologias de rede diversas. Tal como o Homem necessita das letras para formar palavras, para que, por sua vez, consiga comunicar, também os computadores e outros dispositivos informáticos, através da Internet, e por via dos impulsos eletrónicos dos *bits e bytes*, necessitam recorrer aos protolocos existentes de forma a estabelecer uma comunicação entre si.

[54] RODRIGUES, Benjamim Silva, *Da Prova Penal – Tomo II, Bruscamente…* p. 381.
[55] ANDRADE, Manuel da Costa, *Bruscamente no verão passado*…, p. 163-164.
[56] RAMOS, Armando Dias, *A Prova Digital em Processo Penal*, Chiado Editora, 2.º ed., Fevereiro de 2017, ISBN: 978-989-51-2383-4, p. 31.

Fundamentalmente, os protocolos estruturais da Internet são dois: o IP[57] (*Internet Protocol*) e o TCP[58] (*Transmission Control Protocol*), habitualmente agregados e designados de protocolo modelar TCP/IP[59]. Este protocolo, padrão de comunicação, é utilizado nos sistemas internos da Internet e também nos computadores e outros sistemas que pretendemos ligar à Internet (por exemplo, um computador, um *smartphone*, um tablet, um *smartwatch*, ou qualquer outro tipo de *gadget* que permita ligação à rede). Como ensinam EDMUNDO MONTEIRO e FERNANDO BOAVIDA, sobre a camada de ligação do modelo TCP/IP, por sua vez, existem vários protocolos, com diferentes funções, destacando-se, no que ao envio/receção de *e-mails* diz respeito, três tipos de protocolos: o SMTP[60] (*Simple Mail Transfer Protocol*) – que se caracteriza por se tratar de um protocolo standart que permite enviar as mensagens eletrónicas de um servidor para outro – o POP3[61] *(Post Office Protocol)* – que permite recuperar mensagens de correio eletrónico de distintos servidores - e o IMAP[62] *(Internet Mail Acess Protocol)* – que, sendo um protocolo alternativo ao POP3, caracteriza-se pelo facto de permitir que as mensagens de *e-mail* se mantenham guardadas e disponíveis no servidor (ao contrário do POP3, os *e-mails* no

[57] O Protocolo IP é responsável pela comunicação entre *hosts* em redes TCP/IP. Ele é responsável pela comunicação entre cada elemento da rede, permitindo o transporte de uma mensagem de um *host* de origem, até a um *host* de destino.

[58] O TCP é um protocolo da camada de transporte, que garante que os dados são integralmente transmitidos para os corretos *hosts* de destino. Entre outros, *vide*, COMER, Douglas, *Internetworking with TCP/IP*, Volume 1: Principles, Protocols, and Architectures, Fourth Edition, Prentice Hall PTR, Upper Saddle River, NJ, 2000, *apud* PORTELA, Irene, Revista de Estudos Politécnicos, 2008, Vol VI, nº 9, p. 4.

[59] O TCP/IP representa um conjunto de protocolos que, operando entre si, permitem que diversos equipamentos que constituem uma rede possam transportar as comunicações. Trata-se de um protocolo estruturado por 5 camadas (aplicação, transporte, camada IP, acesso à rede e físico) na qual cada camada utiliza e presta serviços às camadas adjacentes, apenas tratando das informações que correspondem à sua função.

[60] O SMTP, contrariamente ao HTTP, não tem capacidade para transportar mensagens multimédia que incluam imagens, sons ou vídeos, sendo que, somente os protocolos POP ou IMAP, permitem ao utilizador aceder ao seu conteúdo. MONTEIRO, Edmundo e BOAVIDA, Fernando, Engenharias de Redes Informáticas, FCA, 7.ª edição, Agosto de 2000, p. 330-343.

[61] O POP3 transfere as mensagens do servidor para a caixa de correio onde o programa de *e-mail* está instalado, removendo-as do servidor. Tem a desvantagem dos *e-mails* deixarem de estar disponíveis através do *webmail* ou programa de *e-mail*. Assim, um novo acesso realizado a partir de outro cliente POP3, não informará o utilizador que tem uma nova mensagem, atendendo que esta já foi lida.

[62] O IMAP permite aceder ao correio eletrónico em modo "*online*", "*offline*" e "*disconnected*", tendo como vantagem o facto de permitir a criação e manipulação de múltiplas caixas de correio, quer no desktop, quer no servidor. Outra particularidade deste protocolo, considerado como de alta segurança, reside no facto de permitir a criação de filtros que facilitam a transferência de *e-mails* recebidos/enviados para outras caixas de correio, estejam elas no servidor ou em outro dispositivo de acesso, assim como, caso se pretenda mudar de programa de *e-mail*, ou mesmo mudar de computador, permite não correr o risco dos dados se perderem, possibilitando o acesso a toda a correspondência, bastando para tanto apenas a sincronização com o servidor de *e-mail*.

IMAP não são automaticamente eliminados) até que o utilizador as elimine, permitindo a gestão da caixa de correio a partir de múltiplos dispositivos.

Assim, para melhor assimilação prática, podemos estabelecer uma analogia entre números de telefone e endereços IP. Quando se telefona para alguém, antes de mais, é necessário saber o seu número de telefone. De forma semelhante, quando um computador ligado à Internet precisa de enviar dados para outro, precisa conhecer o endereço de IP do destinatário. Se desconhecemos o número de telefone para onde queremos telefonar, recorremos à lista telefónica para obter o número. De forma semelhante, os computadores recorrem a um serviço de diretório denominado DNS (Domain Name System) para traduzir os nomes em endereços IP.

Dando seguimento à analogia entre números de telefone, para que uma comunicação seja bem-sucedida deve ser corretamente interpretada pelo destinatário da chamada. Para isso, é necessário decidir a linguagem que será falada e o nível de vocabulário que será usado. Transpondo tal analogia para o processo de envio de uma mensagem de correio eletrónico, a ligação entre a origem e o destino apenas é possível, antes de mais, por via dos *Mail User Agent* (MUA), que, tratando-se da parte visível ao utilizador, mais não são senão os programas que permitem ao emissor e recetor comporem e recolherem a mensagem eletrónica, com recurso aos servidores de correio eletrónico. Entre os MUA mais comuns podem referir-se o *Mozilla Thunderbird*, o *Microsoft Outlook* e o *Mac OS Mail*. Em alternativa aos MUA, surgem as chamadas contas de correio eletrónico criadas e geridas por via de *Webmail´s* (v.g. *Gmail, o Sapo, o Hotmail, Yahoo*[63]), com a reconhecida vantagem de se tratar de um sistema que permite ao utilizador aceder às mensagens utilizando apenas um navegador de Internet (ex. *Internet Explorer, Mozilla Firefox, Chrome*), sem que seja necessário instalar-se e configurar-se programas específicos, tornando-se acessível a partir de qualquer dispositivo eletrónico.

Em qualquer caso, é na parte invisível ao emissor e destinatário, que se processa o diálogo protocolar que, como vimos, mais não é senão uma verdadeira comunicação entre máquinas, por via dos servidores e com recurso aos diferentes protocolos, com vista a transportar as mensagens de correio eletrónico do endereço de origem (do *host* emissor) até

[63] É ampla e gradual a oferta de programas de receção e envio de mensagens eletrónicas por via de *webmail*. *Vide*, a título de exemplo, a lista disponível em https://en.wikipedia.org/wiki/Comparison_of_email_clients. [acedido em 29 de Novembro de 2016].

ao endereço de destino (*host* recetor), sendo aqui os routers importantes ativos de rede. Neste procedimento, as mensagens de correio eletrónico, desfragmentando-se, viajam em datagramas sob a forma de pacotes[64], que apenas são unificados quando todos chegam ao seu destino, tornando a mensagem de correio eletrónico legível, agora sob a forma de cabeçalho (que permite identificar o percurso da mensagem desde o servidor de envio ao servidor final) e corpo (referente ao texto, imagens, sons ou ficheiros que a mensagem comporte[65]).

Porque uma imagem, por vezes, valerá mil palavras, remetemos, *infra*, para um *paper* da autoria de PEDRO MARQUES[66], que nos auxilia a ter uma noção do procedimento informático inerente ao envio/receção de uma mensagem de correio eletrónico, esperançados que nos permita, em abono da nossa superficial explicação, ter uma abrangente perceção do circuito das etapas do "diálogo protocolar".

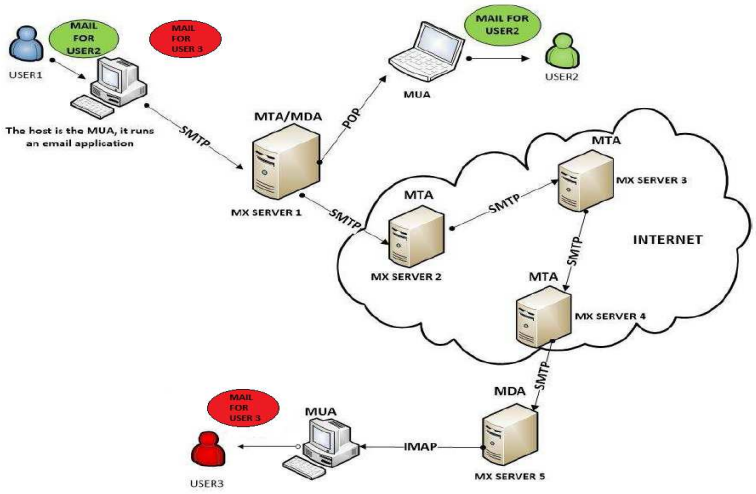

Fig.1 – Ilustra o processo de envio/receção de uma mensagem de correio eletrónico utilizando os protocolos SMTP, POP3 e IMAP.

[64] Como já vimos, uma transmissão de dados entre computadores consiste no envio e receção de sinais elétricos, os quais codificam *bits*. Normalmente, os *bits* são agrupados em conjunto ou sequências, que podem ir desde um simples *byte* (codificando um caráter) até um pacote de milhares de *bits* ou *bytes*. Na comunicação de dados entre computadores fala-se em pacotes (*packets*), ou em *frames*, como sendo agrupamentos ou sequências de *bits* ou *bytes,* com determinada estrutura que os computadores ou interfaces de rede têm de codificar e descodificar. Normalmente, uma mensagem ou comunicação de um computador para outro é fragmentada em pacotes. Um pacote de dados tem uma estrutura típica que inclui: um cabeçalho, a parte dos dados propriamente dita e um segmento terminal que costuma efetuar o controlo de eventuais erros que ocorram ao longo do percurso do pacote.

[65] Protocolos como o HTTP (*HyperText Transfer Protocol*) e o FTP (*File Transfer Protocol*), são utilizados para transferir ficheiros.

[66] MARQUES, Pedro P. Leitão da Costa, *Informática Forense - Recolha e Preservação da Prova Digital*, Dissertação de mestrado em Segurança em Sistemas de Informação, Universidade Católica Portuguesa Faculdade de Engenharia, Maio, 2013, p. 81.

3.4. Os Dados Informáticos nas Comunicações Eletrónicas

3.4.1. Os Dados de Base, Tráfego e Conteúdo

Em sede de investigação de criminalidade informática, a célere obtenção das informações constantes das comunicações eletrónicas, pode revelar-se uma autêntica chave mestra no apuramento dos factos e identificação da autoria do crime, dela dependendo o culminar do êxito de toda uma investigação. Assim, na análise das mensagens de correio eletrónico, reveste especial importância a recolha e preservação dos chamados dados informáticos, que, de forma automática, vão sendo apostos nos cabeçalhos das mensagens eletrónicas.

No mundo informático, em termos simplistas, os dados são expressões gerais que descrevem características das entidades sobre as quais operam os algoritmos. No fundo, estamos a falar de informação digital codificada. Atendendo à imprecisão conceptual, aos espaços vazios na Lei, bem como à complexa regulamentação e articulação entre diplomas, até à criação da Lei do Cibercrime, a questão dos dados informáticos sempre foi matéria escorregadia. A dificuldade de apreensão de conceitos informáticos por parte do aparelho judicial, fruto da incensurável falta de formação específica do mundo cibernético, a que não ficou alheia a clareza e lucidez normativa, redundou em diversos acórdãos dos Tribunais superiores onde a confusão de conceitos de dados informáticos era evidente. À giza de exemplo, *vide* Acórdão do Tribunal da Relação de Guimarães, de 10 de Janeiro de 2005, proferido sob o processo n.º 2013/04-1, onde se consignou que "*não faz sentido, em nosso modesto entendimento, fazer-se a distinção que a Jurisprudência fazia entre dados de base, de tráfego e de conteúdo, pois que tudo se trata de comunicações, a merecer o mesmo tratamento jurídico*"[67]. Tais decisões desconsideravam, inclusivamente, a existência do parecer n.º 21/2000[68], de 16/06, do Conselho Consultivo da PGR, que

[67] O acórdão encontra-se disponível *online* no endereço: http://www.dgsi.pt/jtrg.nsf/86c25a698e4e7cb7802579ec004d3832/0acea33f67fe0e2980256fe3003d53b8?OpenDocument [acedido em 28 de Novembro de 2016].

[68] Tal parecer surge na sequência de um pedido feito pela fornecedora de telecomunicações *TMN – Telecomunicações Móveis Nacionais*, questionando os termos da sua colaboração com as autoridades de investigação, a propósito dos pedidos de informação sigilosa formulados por magistrados do Ministério Público, assim como dos Tribunais, de dados pessoais dos seus clientes. Acessível *online* no endereço http://www.dgsi.pt/pgrp.nsf/7fc0bd52c6f5cd5a802568c0003fb410/58101f7b2b6fb7818025689e00501437?OpenDocument&Highlight=0,P000212000 [acedido em 3 de Dezembro de 2016]. De resto, tal parecer vem consolidar o que se mostrada já consignado no Parecer n.º 16/94/complementar, disponível em www.dgsi.pt.

reconhecia a destrinça entre três tipos de dados informáticos: *"os dados de base, necessários ao acesso à rede, designadamente através da ligação individual e para utilização própria do respectivo serviço* (…) *Os elementos ou dados funcionais (de tráfego), necessários ou produzidos pelo estabelecimento da ligação da qual uma comunicação concreta, com determinado conteúdo, é operada ou transmitida, (…) e os elementos de conteúdo – dados relativos ao próprio conteúdo da mensagem, da correspondência enviada através da utilização da rede"*.

Não obstante, caminhando-se sobre a pena da doutrina, e porque julgamos que privilegia a caracterização (pese embora discordarmos com os Autores quanto à concreta catalogação do IP), não deixamos de perfilhar, quanto à tipologia de dados informáticos, os ensinamentos de ARMANDO VEIGA e BENJAMIM SILVA RODRIGUES. Assim, segundo os Autores, *"os dados de base consistem nos elementos fornecidos pelo utilizador à empresa que fornece o acesso à rede e ou ao serviço de comunicações electrónicas, v.g., nome, morada, e os dados que aquela empresa fornece, em sentido inverso, ao utilizador para efeito de interligação à rede e ou ao serviço de comunicações electrónicas, v.g., número de acesso, nome de utilizador, password. Os dados de tráfego dizem respeito aos elementos funcionais da comunicação e permitem o envio da comunicação através de uma rede de comunicações electrónicas, v.g., data e hora do início da sessão (login) e do fim (logoff) da ligação ao serviço de acesso à Internet, endereço de IP atribuído pelo operador, volume de dados transmitidos, entre outros. Os dados de conteúdo baseiam-se no conteúdo da comunicação transmitida pela rede de comunicações electrónicas"*[69].

Com a entrada em vigor da LC, no seu art.º 2.º, al. b), os dados informáticos são definidos como sendo "*qualquer representação de factos, informações ou conceitos sob uma forma suscetível de processamento num sistema informático, incluindo os programas aptos a fazerem um sistema informático executar uma função"*, acabando este diploma, no art.º 2.º, al. c)[70], por dispor de uma definição rigorosa do que são dados de tráfego, delimitando-os aos elementos "*da origem da comunicação, o destino, o trajecto, a hora, a data, o tamanho, a duração ou o tipo do serviço subjacente*", sendo, porém, o diploma omisso quanto à definição dos dados de base e conteúdo. A este propósito, não podemos

[69] VEIGA, Armando e RODRIGUES, Benjamim, *A Monitorização de dados pessoais de tráfego nas comunicações electrónicas*, Revista Raízes Jurídicas, Curitiba, v. 3, n. 2, Jul./Dez. 2007, p. 73.
[70] O art.º 2.º, al. c), da LC, acaba por ser uma reprodução fiel da definição constante da al. d), do art. 1.º, da CCiber.

deixar de considerar que a LC, no que aos dados de tráfego diz respeito, representa um enorme avanço comparativamente à Lei n.º 41/2004, de 18 de Agosto[71], que os define, no seu art.º 2.º, al. d), ampla e desfasadamente, como "*quaisquer dados tratados para efeitos do envio de uma comunicação através de uma rede de comunicações eletrónicas ou para efeitos da faturação da mesma*", caindo o legislador no desacerto legislativo ao não fornecer uma pauta conceptual concisa e rigorosa. Imprudência esta que emergia já da Lei n.º 32/2008, relativa à conservação de dados gerados ou tratados no contexto oferta de serviços de comunicações eletrónicas, não se encontrando consagrada neste diploma uma definição de dados de tráfego.

3.4.2. O Internet Protocol (IP) – Um Dado de Tráfego, Base ou Localização?

Em termos genéricos, podemos definir o IP (*Internet Protocol*) como uma combinação numérica correspondente à identificação de um equipamento na Internet (por exemplo um computador, uma impressora ou router), não se confundindo, porém, com a identificação de uma pessoa. Até porque pode suceder que várias pessoas utilizem o mesmo equipamento. A análise ao cabeçalho técnico da mensagem de correio eletrónico revelará o endereço IP de origem da comunicação. De resto, recorrendo-se hoje a várias fontes abertas da Internet[72], como por exemplo as existentes nos endereços *www.centralops.net* e *www.dnsstuff.com*, poderá, a partir-se do endereço IP, obter-se facilmente a identificação da entidade fornecedora do serviço de Internet (ISP), a quem caberá, por sua vez, fornecer a identificação do cliente a quem foi atribuído esse IP.

Ora, como já se antevê, não será através da identificação do endereço IP que o investigador verá revelada a identidade do autor do crime, tanto mais que, conforme IRENE PORTELA, "*O fornecedor de serviços IP permite ao usuário a utilização do endereço em vários locais associados a endereços IP diferentes, por isso é muito difícil para o sistema de intercepção identificar um usuário alvo pelo endereço fictício,*

[71] Transpôs para a ordem jurídica nacional a Diretiva n.º 2002/58/CE, do Parlamento Europeu e do Conselho, de 12/07, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas.

[72] No fundo, são bases de dados dos denominados RIR (*Regional Internet Registry),* organizações que gerem a alocação e registo dos recursos de endereços da Internet numa particular região do mundo. Sobre a matéria *vide* MARQUES, Pedro P. Leitão da Costa, *Informática Forense*…, p. 50.

independentemente de sua localização e endereço IP."[73]. Com tal dado, apenas será possível ao investigador confirmar que determinada comunicação foi efetuada através daquele número técnico de acesso à Internet, estabelecendo a ligação entre uma comunicação já conhecida e a sua origem. O problema surge atendendo que não existe na Lei um estatuto do endereço IP. De igual modo, também não é expressamente determinado em nenhum texto legal se o endereço IP é, ou não, um dado de tráfego, circunstância que acaba por despoletar divergente entendimento jurisprudencial[74].

Qualificar o endereço IP como dado de tráfego condiciona a investigação, na medida que a sua obtenção apenas poderá ser autorizada, durante o inquérito, pelo JIC, exigindo-se que, *in casu*, se investiguem crimes graves. Por tal motivo, a fim de colocar um ponto de ordem na divergência jurisprudencial, uniformizando procedimentos e elucidando o aparelho judicial, a PGR, através do seu Gabinete do Cibercrime, por via da nota prática n.º1/2012[75], veio aclarar que *"A identificação de um determinado endereço IP, conjugada com a identidade de quem o utilizou num dado dia e hora, não revela informação sobre o percurso dessa comunicação nem sobre outro eventual tráfego comunicacional da pessoa em causa. Apenas comprova que essa mesma comunicação (e apenas essa) foi efectuada por via daquele número técnico de acesso à Internet. Portanto, com esta informação, apenas se estabelece a ligação entre uma determinada comunicação, que se conhece já, e a respectiva origem"*. Concordamos com tal orientação. De facto, como nos elucida COSTA ANDRADE[76], à semelhança dos procedimentos de

[73] PORTELA, Irene, *A intercepção legal de comunicações*…, p. 5. Por norma os IP's (IPv4) são dinâmicos, ou seja, modificam-se aleatoriamente. Existem também IP's fixos, mas apenas para grandes grupos económicos. Com a recente implementação dos novos IPv6 antevê-se que cada cliente da Internet tenha um IP fixo.

[74] No Acórdão do TRC, de 03.10.2012, sob o processo n.º 84/11.6JAGRD-A.C1, foi considerado que "*a informação relativa à identificação de determinado IP que realizou uma concreta comunicação em certo grupo data/hora, respeita a dados de tráfego*". No mesmo sentido o Acórdão do TRE, de 5/06/2012, sob o processo n.º 12/12.1YREVR. Por seu lado, no Acórdão do TRL, de 19/06/2014, sob o processo n.º 1695/09.5PJLSB.L1-9, foi considerado que "*a identificação de um determinado endereço de IP conjugada com a identidade de quem o utilizou num dado dia e hora não revela informação sobre o percurso da comunicação nem sobre outro eventual tráfego comunicacional da pessoa em causa"*. Acórdãos acessíveis *online* no endereço http://www.dgsi.pt [acedidos em 16 de Dezembro de 2016].

[75] Acessível *online* no endereço:
http://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/nota_pratica_1_pedido_de_ip.pdf [acedido em 18 de Dezembro de 2016].

[76] ANDRADE, Manuel Costa, *Bruscamente no verão passado*…, p. 162. Este é de resto o entendimento predominante do Tribunal Constitucional Alemão, assinalado na sua decisão de 22.8.2008. Em sentido inverso, defendendo que o acesso aos dados de IMEI e IMSI colocam em causa o direito à inviolabilidade do sigilo das comunicações *vide* RODRIGUES, Benjamim Silva, *Da Prova Penal, Tomo II, Bruscamente*... p. 355-356.

identificação do número de um aparelho de telemóvel (IMEI) ou do respetivo cartão (IMSI), cremos que o IP cai fora do regime da tutela da inviolabilidade das telecomunicações[77], podendo a sua obtenção ser solicitada pela autoridade judiciária competente, independentemente do tipo de crime que esteja em causa, desde que se torne necessário à descoberta da verdade. Este é, de resto, o entendimento acolhido por parte do Tribunal Constitucional alemão, na sua decisão de 22 de Agosto de 2006, na formulação de que os dados de localização não configuram uma comunicação eletrónica, mas sim uma mera "*comunicação técnica entre aparelhos*", não apresentando um "*especifico potencial perigo*" para a privacidade da comunicação, não gozando assim da tutela constitucional do art º 10.º da *Grundnorm.*

Doutro passo, por via da referência específica da al. b), do n.º 4, do art.º 14.º da Lei do Cibercrime, o endereço IP pertence ao conjunto de dados informáticos que podem ser solicitados por via de uma injunção para apresentação ou concessão de acesso a dados. Em todo o caso, não podemos deixar de realçar que, contrariamente ao que se impunha, devia o legislador ser mais claro sobre o estatuto do IP, definindo conceitos translúcidos, ao invés de ter deixado para o intérprete a árdua tarefa, sobretudo nesta matéria, de adivinhar os seus desígnios.

3.5. As Dificuldades Colocadas pela Prova Digital

O vertiginoso desenvolvimento das redes informáticas e das redes de comunicações[78], permitiram o desenvolvimento da palavra digital. A "revolução comunicacional", convertida na passagem do *átomo* ao *bit*, abonou o processo comunicacional, possibilitando a transmissão, já não apenas da voz, mas também da imagem, com o custo económico a depender, já não da natureza da comunicação, mas sim do "tamanho" dos pacotes transmitidos. Contrariamente aos tempos antigos, a "tinta da

[77] ANDRADE, Manuel Costa, *Bruscamente no verão passado*…, p. 162.

[78] A Lei nº 5/2004, de 10/02, no seu art.º 3.º, al. dd), define a rede de comunicações electrónicas como "*os sistemas de transmissão e, se for o caso, os equipamentos de comutação ou encaminhamento e os demais recursos, nomeadamente elementos de rede que não se encontrem activos, que permitem o envio de sinais por cabo, meios radioeléctricos, meios ópticos, ou por outros meios electromagnéticos, incluindo as redes de satélites, as redes terrestres fixas (com comutação de circuitos ou de pacotes, incluindo a Internet) e móveis, os sistemas de cabos de electricidade, na medida em que sejam utilizados para a transmissão de sinais, as redes de radiodifusão sonora e televisiva e as redes de televisão por cabo, independentemente do tipo de informação transmitida*".

caneta" ficou obsoleta face às palavras eletrónicas, agora transmitidas por via de cabos, fibra ótica, e mesmo sem fios, tornando o processo comunicacional extremamente acessível, espontâneo e cómodo.

Se é um facto que as comunicações estabelecidas, por meio da Internet, provocaram alterações profundas na forma como comunicamos, também é verdade que nos expuseram a novos perigos. De entre a vastíssima quantidade de informação de cariz pessoal que circula nas redes de informação e comunicação, facilmente acessíveis a um motor de busca, o endereço de correio eletrónico, pessoal ou profissional, tornou-se num veículo privilegiado para a atividade delituosa desenvolvida pelos senhores do crime. Basta imaginarmos o exemplo do envio de mensagens de correio eletrónico, intencionado para a disseminação de um vírus capaz de afetar as funcionalidades do sistema informático, com vista à espionagem pessoal ou empresarial, ou o caso do envio de *e-mails* fraudulentos concebidos para a obtenção das credenciais de acesso da vítima (como por exemplo dados *home banking*), que permitam ao cibercriminoso a realização de transações e saques, ou até mesmo o recurso a esta forma de comunicação com o intuito de proferir ameaças e difamações.

Nesta evolução, tornar-se-ia imperioso adaptar as leis penais à moderna sociedade da informação, criando-se novos tipos legais de crimes, adaptados às novas e evoluídas condutas desviantes cometidos por meios informáticos, preenchendo-se, assim, vazios legais que, até então, eram latentes no nosso ordenamento jurídico.

Paralelamente, só seria possível punir os criminosos, se a investigação criminal fosse apetrechada de novas regras processuais que imaculassem a validade da prova digital, com respeito pelo princípio da legalidade, plasmado no art.º 125.º do CPP, segundo o qual apenas serão admissíveis *"as provas que não forem proibidas por lei"*. De tal forma, divide-se a doutrina em torno da resposta que a dogmática penal deverá prosseguir perante tal flagelo, discutindo-se a pertinência do combate ao cibercrime ser abordado por via do "*Direito Penal do Risco*", como propõem ROVIRA DEL CANTO[79] e ULRICH SIEBER[80], atribuindo-se primazia a uma prevenção do crime, tipificando-se condutas de

[79] ROVIRA DEL CANTO, Enrique, *Delincuencia informática y frauds*…, p. 53-56 e 116-118.

[80] SIEBER, Ulrich, *Legal Aspects of Computer – Related Crime in the Information Society – Comcrime – Study*, 1998, p. 194, 195 e 201. Sobre o tema *vide* BACHMAIER WINTER, Lorena, *Investigación criminal y protección de la privacidad en la doctrina del Tribunal Europeo de Derechos Humanos*, AA.VV., 2.º Congresso de investigação criminal (org. por Maria Fernanda Palma /Augusto Silva Dias / Paulo de Sousa Mendes), Coimbra, Almedina, 2011, cit., p. 162; SANTOS; André Teixeira, *Os novos desafios do Direito*

perigo abstrato em nome da salvaguarda da tutela dos bens jurídicos supra – individuais, ou, pelo contrário, como aponta FARIA COSTA[81], não há que cair na tentação de diabolizar a informática, podendo continuar a ser objeto de estudo à luz dos instrumentos tradicionais do direito penal.

Em qualquer caso, razão parece assistir a ORIN KERR quando alude que as regras do processo penal estão talhadas para a procura e colheita da prova física, ficando destituída de sentido para a captura da prova digital que, no fundo, se circunscreve na linguagem binária de "*zeros*" e "*uns*", sob a forma de eletricidade[82]. De resto, também na *International Hi-Tech Crime and Forensic Conference*, realizada em Londres, em Outubro de 1999, avançou o *Scientific Working Group on Digital Evidence* com um conjunto de definições, standards e princípios, advertindo a comunidade forense internacional para a complexa natureza da prova digital e o caminho que a investigação necessitaria percorrer, de forma a garantir a sua força probatória[83].

Assim, como realça ARMANDO RAMOS, apresentando-se a prova digital como a "*informação passível de ser extraída de um dispositivo eletrónico (local, virtual ou remoto) ou de uma rede de comunicações*", impõe-se com particular equidade a questão das condições processuais de admissibilidade da recolha de dados das comunicações eletrónicas, não se podendo confiar, como adverte BENJAMIM SILVA RODRIGUES[84], ao agente policial das"ruas" ou das"secretárias" a realização de "buscas informáticas", sob pena de originar uma perda irreversível de dados imprescindíveis para a investigação forense digital.

As características ímpares da prova digital, particularmente o facto de ser temporal, frágil, dispersa, volátil, alterável e imaterial, tornam-na numa prova tecnicamente complexa e carente de interpretação especializada, afigurando-se, hoje, imprescindível falar-se da ciência forense digital, não apenas enquanto nova forma de

---

Penal no século XXI, Scientia Ivridica, n.º 316, 2008, p. 628 e ss.; AMBOS, Kai, *Derecho penal del enemigo,* trad. por Gómez Jara Díez e Miguel Lamadrid, Bogotá, Universidad Externato de Colombia, 2007, p. 23-28.

[81] COSTA, José de Faria, *Algumas Reflexões sobre o Estatuto Dogmático do Chamado ´Direito Penal Informático´*, Direito Penal da Comunicação, Coimbra Editora, 1998, p. 111, 112 e 115-119.

[82] KERR, Orin S., *Digital Evidence and the New Criminal Procedure*, Columbia Law Review 279, GWU Law School Public Law Research Paper No. 108, 2005. Acessível *online* no endereço https://papers.ssrn.com /sol3/Papers.cfm?abstract_id=594101 [acedido em 23 de Novembro de 2016].

[83]Informação disponível *online* em https://www.fbi.gov/about-us/lab/forensic-sciencecommunications/fsc/ april2000/swgde.htm/ [acedido em 23 de Novembro de 2016].

[84] RODRIGUES, Benjamim Silva, *Direito Penal - Parte Especial, Tomo I, Direito Penal Informático-Digital,* Coimbra, Coimbra Editora, 2009, p. 740-742.

investigação, mas sobretudo para que se estabeleçam importantes manuais de procedimentos, princípios e regras que mantenham a integridade, fiabilidade e inalterabilidade deste tipo de prova, assegurando-se a manutenção da "*chain of custody*", ou "cadeia de controlo", à luz do crivo dos preceitos da Lei mãe.

Como anota RITA SANTOS[85], as técnicas de recolha e produção da prova digital não se comprazem com as técnicas utilizadas na obtenção dos tradicionais meios de obtenção de prova. A enorme quantidade de informação digital que pode ser criada, modificada ou eliminada, numa fração de segundos, e em qualquer parte do mundo, aliada à constante evolução dos sistemas de informação, impõe que a investigação se especialize e se apetreche de ferramentas específicas que garantam a integridade da prova digital. A tal propósito, revelando a faceta mais débil da justiça e colocando a nu as fragilidades da investigação, atente-se nos modestos números apresentados pelo recente relatório anual de segurança interna[86], demonstrando que, no ano de 2016, somente 801 processos de inquérito foram levantados por crimes informáticos, sendo que, destes, apenas em 402 foram constituídos arguidos, recaindo sobre os crimes de burla informática e nas comunicações o maior número de ilícitos.

Os inexoráveis avanços tecnológicos, aliados à progressiva e inquietante impunidade da prática de ilícitos cometidos no ciberespaço, impuseram que o legislador engrenasse uma nova velocidade, regulamentando, no que à matéria da captura e recolha da prova digital diz respeito, diversas áreas onde o Direito, face à informática, era inexistente ou obsoleto. Ora o facto é que, *quiçá,* fruto de alguma distração, nem sempre se procedeu à melhor forma de regulamentação destas questões ligadas ao mundo da Informática e das redes de comunicações, verificando-se que a obtenção de certo tipo de prova digital, nomeadamente, no que ao correio eletrónico diz respeito, foi ocorrendo "*à custa do sacrifício da ponderação constitucional codificada em matéria de inviolabilidade do sigilo das comunicações*"[87], suprindo-se a velha máxima, como bem afirma ANTÓNIO HENRIQUES GASPAR, citando HENKEL e ROXIN, que "*o processo penal é, ou deve ser, em expressão semântica marcada, direito constitucional aplicado ou sismógrafo da*

[85] SANTOS, Rita Coelho, *O Tratamento Jurídico - Penal da Transferência de Fundos*..., p. 24.
[86] Acessível *online* no endereço: https://www.parlamento.pt/ActividadeParlamentar/Paginas/DetalheActividadeParlamentar.aspx?BID=104739&ACT_TP=RSI [acedido em 30 de Abril de 2017].
[87] RODRIGUES, Benjamim Silva, *Da Prova Penal – Tomo IV, Da Prova - Electrónico - Digital e da Criminalidade Informático – Digital*..., p. 20.

sua efectiva aplicação"[88], atendendo que "*o processo penal é por excelência o direito dos inocentes"*[89]*,* pelo que não pode comprometer os direitos, liberdades e garantias constitucionalmente consagrados dos cidadãos de um Estado Democrático.

Assim, ficaria prejudicado o nosso estudo se não fizéssemos uma breve incursão aos direitos constitucionalmente consagrados no âmbito das comunicações eletrónicas.

[88] GASPAR, António Henriques, *As exigências da investigação no processo penal durante a fase de instrução*, *in, Que futuro para o Direito Processual Penal? Simpósio em Homenagem a Jorge Figueiredo Dias por Ocasião dos 20 anos do Código Processo Penal Português*, Coord. Mário Ferreira Monte, Trad. Inês Fernandes Godinho, Coimbra Editora, 2009, p. 87. A este propósito, alude GERMANO MARQUES que o processo-crime é uma "*sequência de actos juridicamente pré-ordenados à decisão sobre se foi praticado algum crime e, em caso afirmativo, sobre as respectivas consequências jurídicas e a sua justa aplicação*" *in* SILVA, Germano Marques, *Curso de Processo Penal, I Volume – Noções Gerais, Elementos do Processo Penal*, 6.ª Edição, Lisboa, Verbo, 2010, p. 31.

[89] VALENTE, Manuel Guedes, *Escutas Telefónicas - Da Excepcionalidade à Vulgaridade*, 2.ª edição, Coimbra, Edições Almedina, 2008, p. 37.

4. A Reserva da Intimidade da Vida Privada nas Modernas Tecnologias de Informação e Comunicação

4.1. O Direito à Inviolabilidade das Comunicações Eletrónicas

A sociedade globalizada em que vivemos, sendo particularmente mediatizada, tornou-se "info-orientada", em que tudo, ou quase tudo o que acontece, é facilmente acessível ao conhecimento de todos, circunstância que cada vez mais tolhe o que na nossa vida há de privado ou familiar, acabando tal circunstância por comprimir os campos de liberdade onde nos podemos expressar e comportar sem quaisquer aparências e/ou amarras sociais, abstraídos de olhares indiscretos, livres de rótulos e refugiados num espaço de sossego.

A era digital trouxe avanços consideráveis para a vida em sociedade, em especial, a rapidez com que hoje alcançamos as mais variadas informações, e a facilidade que temos no armazenamento e portabilidade de dados, agora em quantidade de *Teras e Zettabytes*. A este propósito, discorrendo sobre os espaços de informação na Internet, alude GARCIA MARQUES que *"as potencialidades da informática proporcionaram a recolha, armazenamento, tratamento e pesquisa da informação, incluindo a informação pessoal, organizada e acessível em bancos ou bases de dados*"[90], vulgarmente designados de *datacenters*.

Neste mar de informação, facto é que, de forma inconsciente e incauta utilização, somos enviesadamente conduzidos a espaços virtuais permeáveis a intromissões na nossa vida privada. Um exemplo característico é o que gradualmente sucede nas redes sociais (v.g. *facebook, twitter, instagram*), onde as pessoas divulgam as suas preferências, os seus afazeres, os locais que frequentam, as suas qualidades, os seus defeitos, o seu próprio lar, enfim, as pessoas ficam obcecadas na exposição da sua vida pessoal (propriamente profissional), sem se darem conta que estão a divulgar um conjunto de informações íntimas, convidando à intrusão na sua vida privada, expondo ao risco o seu património e, mais importante que tudo, a sua própria vida.

De tal forma, há, pois, que preservar um espaço de liberdade e segurança do "nosso" e para os "nossos", reclamando-se do Estado a incumbência de erigir mecanismos

[90] MARQUES, Garcia e MARTINS, Lourenço, *Direito da Informática*…, p. 137.

de defesa face às novas, e por vezes ocultas, formas de intromissão na vida privada, protegendo o utilizador naquilo que de mais íntimo e pessoal lhe possa dizer respeito: a sua privacidade. Há, portanto, que encontrar um ponto de equilíbrio entre aquilo que é o interesse público e o privado, compatibilizando-se a promoção de um e a defesa do outro[91].

Historicamente, a reflexão acerca da proteção da reserva da intimidade da vida privada, convoca-nos a recuar ao ano de 1890, a um ensaio publicado na conceituada revista "*Harvard Law Review*", intitulado "*The right to privacy",* da autoria de SAMUEL WARREN e LOUIS BRANDEIS.[92] Substancialmente, questionaram estes dois advogados a compatibilização de interesses a propósito da liberdade de imprensa e a exposição que os jornais submetiam a classe burguesa com a divulgação da sua vida privada**.** Da publicação deste artigo, emancipou o conceito do direito à reserva da intimidade da vida privada, ganhando amplitude o reconhecimento do direito à privacidade. O conceito acabaria por influir na *Common Law* e propagar-se à generalidade dos sistemas jurídicos europeus.

Pese embora o contributo da aludida publicação, a verdade é que, no nosso ordenamento jurídico, o sentido do direito à privacidade, ou à reserva da vida privada, acabaria por não corresponder ao conceito anglo-saxónico do "*right to privacy*" enquanto "*right to be let alone*". Diríamos que o conceito de "*privacy*", na sua vasta extensão de direito ao isolamento e refúgio, perdeu parte do seu significado e do seu conteúdo. Ao contrário do "*right to privacy*", o direito à reserva da intimidade da vida privada surge na nossa ordem jurídica com um âmbito de aplicação concreto, por oposição a concretos direitos, transformando-se num direito que considera que a pessoa é, nas palavras de OLIVEIRA ASCENSÃO, "*convivência e solidariedade*"[93], parecendo claro que "*uma coisa é o direito à reserva, outro ao isolamento*".

Assim, a ordem jurídica portuguesa, bebendo das disposições consagradas em normas internacionais, designadamente, na Declaração Universal dos Direitos Humanos

---

[91] ANDRADE, José Carlos Vieira de, *Os direitos fundamentais na Constituição portuguesa de 1976*, 5. ed. Coimbra, Edições Almedina, 2012, p. 141.

[92] WARREN, Samuel, e BRANDEIS, Louis, *The right to privacy*, Harvard Law Review, Vol. IV, n.º 5, *December* 15, 1890, p. 193-220.

[93] ASCENSÃO, José de Oliveira, *Teoria Geral do Direito Civil*, Vol. I, Faculdade de Direito de Lisboa, Lisboa, 1996, p.118-121. Estabelecendo igualmente uma distinção entre o direito à reserva da intimidade da vida privada e o *right of privacy, vide* DRAY, Guilherme Machado, *Justa causa e esfera privada,* Estudos do Instituto de Direito do Trabalho, Vol. III, Justa Causa de Despedimento, Almedina, Coimbra, 2001, p. 35-91 e PINTO, Paulo Mota, *A limitação voluntária do direito à reserva sobre a intimidade da vida privada,* in Estudos em homenagem a Cunha Rodrigues, Vol. II, Coimbra Editora, Coimbra, 2001, p. 527-558.

(1948)[94], na Convenção Europeia dos Direitos do Homem (1950)[95] e no Pacto Internacional sobre Direitos Civis e Políticos (1966)[96], documentos que, conforme LUISA NETO[97], se revelaram essenciais para colocar a pessoa como "*fundamento da ordem social, política e jurídica, de acordo com uma revalorização resultante do aludido processo de internacionalização"*, acolheu o direito à reserva da intimidade da vida privada e familiar no seu manto constitucional, consagrando-o no art.º 26.°, n.º 1, da CRP, alocando-o no âmbito dos direitos, liberdades e garantias.

De acordo com esta disposição, assegura a Lei mãe que "*A todos são reconhecidos os direitos à identidade pessoal, ao desenvolvimento da personalidade, à capacidade civil, à cidadania, ao bom nome e reputação, à imagem, à palavra, à reserva da intimidade da vida privada e familiar e à protecção legal contra quaisquer formas de discriminação*". A propósito de uma anotação ao art.º 26.°, n.º 1, da CRP, GOMES CANOTILHO e VITAL MOREIRA aduzem que o direito à reserva da intimidade da vida privada e familiar inclui dois direitos menores*:" a) o direito a impedir o acesso de estranhos a informações sobre a vida privada e familiar e b) o direito a que ninguém divulgue as informações que tenha sobre a vida privada e familiar de outrem"*[98]. Neste lastro, concluem os Autores que o critério constitucional para a averiguação do conteúdo do referido direito deve ser extraído dos conceitos de "privacidade" e de "dignidade humana", consagrados no art.º 26.º da CRP, a fim de *"definir-se um conceito de esfera privada de cada pessoa, culturalmente adequado à vida contemporânea"*[99]. Ainda nesta matéria, ao indagar sobre a relevância da palavra "intimidade" indexada ao da "vida

[94] Trata-se de um diploma surgido após a II Grande Guerra, tendo consagrado um texto de direitos inalienáveis da condição e dignidade humana, estabelecendo, no seu art.º 12.º, que "*Ninguém será sujeito a interferência na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataques à sua honra e reputação*". A publicação da DUDH viria a ser publicada em Portugal em 1978.

[95] A CEDH foi adotada em Roma, pelo Conselho da Europa, em 4 de Novembro de 1950, tendo entrado em vigor em 3 de Setembro de 1953. No seu art.º 8.º, a Convenção viria a consagrar que qualquer pessoa tem direito ao respeito pela sua vida privada e familiar, respeito este extensível ao seu domicílio e correspondência. Portugal viria a assinar esta Convenção em 22 de Setembro de 1976, tendo procedido à sua ratificação por via da Lei n.º 65/78, de 13/10.

[96] Este Pacto entrou em vigor na ordem jurídica internacional em 23 de Março de 1976. Portugal assinou-o em 7 de Outubro deste mesmo ano, merecendo destaque o princípio postulado no art.º 17.º do Pacto, segundo o qual "*1. Ninguém será objecto de ingerências arbitrárias ou ilegais na sua vida privada, família, domicilio ou correspondência, nem de ataques ilegais à sua honra e reputação. 2. Toda a pessoa tem direito à proteção da lei contra essas ingerências ou esses ataques*".

[97] NETO, Luísa, *O Direito Fundamental à disposição sobre o próprio corpo (A relevância da vontade na configuração do seu regime),* Coimbra: Coimbra Editora, 2004, p. 116.

[98] CANOTILHO, Gomes e MOREIRA, Vital, *Constituição da República Portuguesa Anotada*, Coimbra Editora, 1993, p. 179-180.

[99] CANOTILHO, Gomes e MOREIRA, Vital, *Constituição da República Portuguesa Anotada*…, p. 196.

privada", enaltece PAULO MOTA PINTO que a expressão conceptual e delimitadora de "intimidade", não se sobrepõe, e muito menos contrapõe, ao da "vida privada", pois que o critério *"foi o de excluir aspectos como a vida profissional ou o chamado "segredo dos negócios" ("secret dês affaires") - aspectos, esses, que mesmo quando fizessem parte da vida privada, dificilmente poderiam ser considerados `íntimos´"*[100], fazendo assim o Autor referência que, para o que releva, é que há aspetos da "vida privada" que se têm afastados do núcleo e tutela da reserva da intimidade da vida privada e familiar[101], aludindo que o núcleo da vida privada de uma pessoa é composto por um vasto conjunto de informações tais como a sua identidade, filiação, residência, número de telefone, estado de saúde, vida amorosa, assim como as informações transmitidas por carta ou outros meios de comunicações. No contexto de dados pessoais, que melhor trataremos *infra*, à giza de PAULO MOTA PINTO, também HELENA MONIZ[102] reconhece as duas esferas da reserva da vida privada, utilizando o critério divisório entre os dados pessoais e os dados sensíveis (ou pessoalíssimos), para demarcar os diferentes âmbitos entre o direito à reserva da vida privada (dados pessoais) e o núcleo do direito sobre a intimidade da vida privada (dados sensíveis)[103].

Neste esteio, cedo se percebeu que não bastaria a mera consagração constitucional para resguardar o cidadão no seu direito à reserva da intimidade da vida privada, evidenciando-se que seria necessário rodear este direito de mecanismos de garantia de defesa, para que a prescrição constitucional não passasse de meras "letras mortas".

Face ao aparecimento das tecnologias da informação e comunicação (agora transmitidas em nanosegundos), o processo comunicativo foi exposto a intensificados perigos, provocados pela ingerência de terceiros, tornando-se intuitivo que as exigências tutelares que protegiam a privacidade teriam que sair reforçadas. Assim sendo, à

---

[100] PINTO, Paulo da Mota, *A limitação voluntária do direito à reserva sobre a intimidade da vida privada* …, p. 531-532.

[101] Tal entendimento é, de resto, partilhado por COSTA ANDRADE e ANDRÉ LAMAS LEITE, no reconhecimento de "*um núcleo muito restrito da pessoa humana*", dando como exemplo os relativos à sexualidade e estado de saúde. Cfr. LEITE, André Lamas, *Entre Péricles e Sísifo: o novo regime legal das escutas telefónicas*, Revista Portuguesa de Ciência Criminal, Ano 17, n.º4, Out.- Dez. 2007, p. 660.

[102] MONIZ, Helena, *Notas sobre a proteção de dados pessoais perante a informática (o caso especial dos dados pessoais relativos à saúde),* in Separata da Revista Portuguesa de Ciência Criminal, Ano 7, Fasc. 2.º, Coimbra Editora, Abril – Junho 1997, p. 231-241.

[103] A este propósito, defende OLIVEIRA ASCENSÃO que os dados sensíveis, como "a *filiação partidária, a saúde e vida sexual, os dados genéticos ou a fé religiosa*" constituem dados "*cujo tratamento é em geral proibido*". *Vide* ASCENSÃO, José de Oliveira, *Estudos sobre Direito da Internet e da Sociedade da Informação…,* p. 267.

semelhança de alguns tipos legais de crimes já existentes no nosso ordenamento, e que punem a perturbação e devassa da vida privada, quando posta em causa por meio dos telefones e da informática (v.g. art.ºs 190.º, n.º 2, 192.º, 193.º e 194.º do CP e art.ºs 6.º e 7.º da LC), não deverá o Estado deixar de erigir garantias e meios de defesa contra ataques ou violações do direito à reserva da intimidade da vida privada e familiar[104].

Por via da consagração do art.º 34.°, a nossa Lei Fundamental, à semelhança da sua congénere disposta no art.º 10.º da Constituição alemã, garante a inviolabilidade do domicílio e da correspondência, nomeadamente, assegurando que qualquer pessoa que estabeleça uma comunicação, seja pelas vias telemáticas ou demais meios de comunicação, tenha a legítima confiança que esta permaneça fechada no circuito dos sujeitos da relação comunicacional, proibindo-se todo o tipo de ingerências por parte de autoridades públicas ou entidades privadas, designadamente, a interceção, gravação e divulgação do seu teor. Assim, ao equiparar e projetar a privacidade do domicílio à correspondência, onde se incluem as comunicações eletrónicas (especificamente objeto do nosso estudo, o correio eletrónico), o Estado edificou uma barreira que protege o ato comunicacional estabelecido pelo cidadão.

Por tal via, no nosso ordenamento jurídico, o direito ao sigilo das comunicações privadas consubstancia-se num direito que se integra nos "direitos, liberdades e garantias" fundamentais dos cidadãos, ínsitos no art.º 18.º da CRP, mais precisamente na proteção da "intimidade da vida privada"[105], garantindo assim que, num determinado ato comunicacional, ninguém possa interferir no circuito estabelecido entre o emissor e recetor. No entanto, a verdade é que tal direito, nos termos do n.º 4.º, do art.º 34.º da CRP, admite restrições. Nas palavras de VIEIRA DE ANDRADE[106], tal preceito contém uma

[104] Os art.ºs 176.° a 185.° do CP conferem uma proteção abrangente do direito à reserva da intimidade da vida privada, criminalizando um conjunto de condutas suscetíveis de lesar os bens jurídicos localizados no âmbito da esfera pessoal. A lei tutela ainda, paralelamente, o direito à reserva sobre a intimidade da vida privada no Código Civil, incluindo-o entre os chamados "direitos de personalidade" (artigos 70.º a 80.º do CC) dispondo o art.º 80.ºdo CC que "*1. Todos devem guardar reserva quanto à intimidade da vida privada de outrem; 2. A extensão da reserva é definida conforme a natureza do caso e a condição das pessoas*".

[105] A este respeito, alude GOMES CANOTILHO que os "*direitos fundamentais cumprem a função de direitos de defesa dos cidadãos sob uma dupla perspectiva: (1) constituem, num plano jurídico-objectivo, normas de competência negativa para os poderes públicos, proibindo fundamentalmente as ingerências destes na esfera jurídica individual; (2) implicam, num plano jurídico - subjectivo, o poder de exercer positivamente direitos fundamentais (liberdade positiva) e de exigir omissões dos poderes públicos, de forma a evitar agressões lesivas por parte dos mesmos*". Cfr. CANOTILHO, José J. Gomes, *Direito Constitucional e Teoria da Constituição*, 7. ed. Coimbra, Almedina, 2010, p. 407.

[106] ANDRADE, José Carlos Vieira de, *Os direitos fundamentais na Constituição portuguesa*…, p. 293.

"*reserva qualificada*" que permite a restrição do conteúdo deste direito "*para a salvaguarda dos direitos ou valores enunciados*". Assim, nos termos do art.º 34.º, n.º 4.º, da CRP, "*É proibida toda a ingerência das autoridades públicas na correspondência, nas telecomunicações e nos demais meios de comunicação, salvos os casos previstos na lei em matéria de processo criminal*", sendo que, a esta luz, nos termos do art.º 126.º, n.º 3, do CPP, são nulas as provas obtidas em desrespeito pela lei.

A dificuldade, já se antevê, está em saber quando é que a lesão no direito à reserva da intimidade da vida privada ainda é tolerada ao nível do processo penal, ou se, pelo contrário, já não estará o processo penal no âmbito de uma violação inadmissível do direito à privacidade da comunicação[107]. Nem sempre é fácil alcançar o ponto de equilíbrio entre valores, nomeadamente, definir o campo de admissibilidade dos meios de obtenção de prova. A este propósito, conforme desnudado em inúmeros processos judiciais, reflita-se acerca da utilização abusiva das escutas telefónicas e interceções de comunicações eletrónicas no nosso País, nem sempre se conciliando a salvaguarda da dignidade humana com a descoberta da verdade material. A sociedade do risco, de que fala o alemão ULRICH BECK[108], vê-se confrontada com o flagelo da criminalidade grave e organizada, de que é exemplo o terrorismo, impondo-se ao Estado a criação de soluções. Todavia, não pode valer tudo na obtenção da prova e descoberta da verdade material, impondo-se limites em nome da salvaguarda de outros, compreendidos nos direitos, liberdades e garantias do cidadão, e sempre no estrito respeito pelos princípios do excesso, da proporcionalidade e da legalidade. Assim, as restrições ao sigilo das comunicações eletrónicas, consagradas nos n.ºs 2 e 3, do art.º 18.º da CRP, para além dos limites positivados pela Lei constitucional, sempre haverão de passar pelo crivo do art.º 32.º, n.º 8, da CRP, que determina a nulidade de todas as provas obtidas com a intromissão abusiva na vida privada, no domicílio, na correspondência ou nas telecomunicações[109].

De tal modo, será sempre, desde logo, à lupa destes preceitos constitucionais que residirá a questão de se determinar se a prova obtida, ainda que no estrito cumprimento dos

---

[107] A este propósito, defende BENJAMIM SILVA RODRIGUES não ser possível sustentar a admissibilidade de uma lesão à integridade física para efeitos de obtenção da prova. RODRIGUES, Benjamim Silva, *Da Prova Penal*, Tomo II, *Bruscamente*... p. 201.

[108] DIAS, Jorge de Figueiredo, *Temas Básicos da Doutrina Penal – Sobre os Fundamentos da Doutrina Penal*, sobre a Doutrina Geral do Crime, Coimbra Editora, 2001, p. 158.

[109] Cfr. SANTOS, Cristina Máximo, *As novas tecnologias da informação e o sigilo das telecomunicações*, Revista do Ministério Público – Lisboa, Sindicato dos Magistrados do Ministério Público, A. 25, n.º 99, 2004, p. 93.

requisitos inerentes aos procedimentos do direito adjetivo, não colide com os direitos liberdades e garantias do cidadão, nomeadamente, se não viola a fina malha dos princípios plasmados na CRP, concebidos para a proteção da esfera da vida privada e reserva da intimidade do indivíduo.

4.2. A Proteção dos Dados Pessoais Informatizados e o Direito à Autodeterminação Informacional nas Comunicações Eletrónicas

O aumento exponencial das plataformas da Internet, abriu as portas a um extraordinário e selvático mercado de aplicações informáticas, assim como um vasto leque de oferta de serviços, tendencialmente gratuitos, permitindo aos privadas e às entidades públicas, no exercício das suas atividades, a utilização de dados pessoais numa escala sem precedentes[110].

Neste aliciante mundo virtual, os recursos e as fontes da rede são inesgotáveis, fruto da intensa atividade dos fluxos informacionais e comunicacionais. De facto, na interação com a rede, nem sempre as pessoas têm a perceção que, numa simples operação de comércio eletrónico, numa visita a uma página *Web*, na utilização das redes sociais[111], ou da simples utilização de armazenamento de dados em nuvem[112], disponibilizam informações pessoais a terceiros, gerando-se a expetativa que a rede e os sistemas de segurança informáticos sejam capazes de resistir a eventos acidentais, ou a ações ilícitas, que comprometam a disponibilidade, autenticidade, integridade e a confidencialidade dos dados pessoais, conservados ou transmitidos, sendo "*crucial criar uma cultura de segurança no ciberespaço*"[113].

Por outro lado, ainda que não exista "*menoridade tecnológica*", como refere OLIVEIRA ASCENSÃO, não deixa o utilizador de ficar numa situação de vulnerabilidade

[110] GARRIGA DOMÍNGUEZ, Ana, *Nuevos retos para la protección de datos personales: en la era del big data y de la computación ubicua*, Editorial Dykinson, 1ª ed., 2016, p. 25.

[111] A este propósito, assinala TIM WU, professor norte-americano da universidade de Columbia, que empresas como a *Google* e o *Facebook* geram elevados lucros a processar uma matéria-prima que obtêm gratuitamente: os nossos dados pessoais. De tal modo, deveriam pagar pela sua utilização. Acessível *online* no endereço http://www.newyorker.com/business/currency/facebook-should-pay-all-of-us [acedido em 05 de Janeiro de 2017].

[112] Sobre a computação em nuvem, *vide* RAMALHO, David Silva, *A Recolha de Prova Penal em Sistemas de Computação em Nuvem*, Revista de Direito Intelectual, n.º 2, 2014, p. 123-162.

[113] VEIGA, Pedro, *Direito a Pensar Tecnologicamente*, Revista Científica sobre *Cyberlaw* do Centro de Investigação Jurídica do Ciberespaço – CIJIC – da Faculdade de Direito da Universidade de Lisboa, Ed. n.º II, Junho de 2016, p. 8.

informática absoluta, sendo *"preciso uma fé piedosa na auto contenção dos órgãos públicos para não sentir que quase toda a vida dos destinatários está à mercê de uns tantos cliques"*[114]. Fenómenos como o *Phishing*, a burla informática, a devassa da vida privada, o *Hacking*, a espionagem empresarial ou comercial (*v.g.* furto de patentes e segredos de negócio), ou mesmo o diabólico *Ransomware*[115], têm colocado a nu as falhas de segurança das redes e dos sistemas, daí resultando graves lesões nos direitos fundamentais das pessoas. Exemplo sintomático, foi o que aconteceu em 2013 à "*iCloud*" da *Apple*, quando esta sofreu um ataque que poderia ter colocado em perigo milhões de utilizadores de *iPhone* e *iPad,* no acesso aos seus elementos pessoais, tais como contactos, agendas e números de cartões de crédito.

Com o avanço tecnológico e a capacidade para receber, transmitir e cruzar informação, de diversa natureza, foi despertada nos legisladores onde a realidade informática se encontrava mais desenvolvida, a necessidade de aprovar legislação dotando as autoridades de meios para combater os abusos que pudessem ser provocados pelos poderes públicos, assim como privados, no tratamento de dados informáticos. Doutro passo, conforme demonstra MIGUEL PUPO CORREIA, é uma "*realidade incontornável, que os dados – ou parte deles - relativos às comunicações electrónicas, que ficam ou podem ficar ao alcance das empresas prestadoras dos respectivos serviços, constituem um meio de prova directo, forte e muitas vezes único dos factos que as autoridades de investigação criminal e os tribunais carecem de apurar"*[116].

O ordenamento jurídico português, designadamente, pela garantia constitucional consagrada no art.º 35.º da CRP, no texto de 1976, sob a epígrafe "*Utilização da informática*", albergou de forma pioneira o direito à proteção dos dados pessoais informatizados[117]. Neste conspecto, de acordo com o disposto no seu n.º 3, "*A informática não pode ser utilizada para tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo*

---

[114] ASCENSÃO, José Oliveira, *Direito da Sociedade da Informação*, Vol. VIII, Coimbra Editora, Julho 2009, ISBN 978-972-32-1710-0. p. 125.

[115] O *Ransomware* é um tipo de vírus malicioso concebido para contaminar e restringir o acesso a um determinado sistema informático infetado, coagindo a vítima a pagar um "resgaste" ao cibercriminoso a fim do mesmo poder fornecer o(s) código(s) que possibilitem desencriptar os arquivos que ficaram "sequestrados" por via do golpe.

[116] CORREIA, Miguel Pupo, *Retenção de dados de comunicações*, Universidade Lusíada de Lisboa, n.º 7, 2010, p. 171.

[117] CASTRO, Catarina Sarmento, *Direito da Informática, Privacidade e Dados pessoais*, Coimbra, Edições Almedina, 2005, ISBN: 9789724024240, p. 32.

mediante consentimento expresso do titular, autorização prevista por lei com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis".

Neste âmbito, sendo os dados recolhidos com estrita observância dos princípios da proporcionalidade e finalidade, o n.º 1, do art.º 35.º da CRP, garante ao titular dos dados o direito de conhecer os propósitos a que se destina a sua recolha, devendo o processamento de recolha dos mesmos observar o cumprimento de três regras essenciais: o dever de informação, o dever de adequação e o dever de obtenção de consentimento prévio e esclarecido do interessado. Assim, tornando-se cada vez mais importante a existência de garantias contra o tratamento e a utilização abusiva de dados pessoais informatizados[118], e a sua compatibilização com vários direitos, liberdades e garantias, o direito à autodeterminação informacional, consagrado no artigo 35.º da CRP, surge assim como o direito que cada pessoa tem de controlar a informação disponível a seu respeito nas etapas de recolha, armazenamento, utilização e transmissão dos seus dados pessoais.[119]

Pese embora esta consagração percursora na CRP, somente em 1991, com a Lei n.º 10/91, de 27 de abril (a primeira Lei da Proteção de Dados Pessoais face à Informática), veio o legislador regular esta matéria, introduzindo os princípios da timoneira Convenção n.º 108, adotada pelo Conselho da Europa em 28 de janeiro de 1981, protegendo os dados informatizados pessoais das pessoas singulares. O objetivo desta Convenção era tutelar a intimidade e garantir o funcionamento do mercado interior e a livre circulação de dados pessoais entre os Estados-membros da União.

Em 24 de Outubro de 1995, através da Diretiva 95/46/CE, do Parlamento Europeu e do Conselho, os princípios fundamentais da proteção de dados, que constavam da Convenção 108 do Conselho da Europa, passariam a ser integrados nesta Diretiva. Substancialmente, visou a Diretiva conciliar o direito sobre a informação com o direito à circulação da informação, tendo influenciado o panorama do direito interno de todos os

---

[118] PÉREZ LUÑO, Antonio Enrique, *Manual de Informática y Derecho*, Ariel Derecho, Barcelona, 1996, p.43-44. Igualmente sobre a matéria, *vide* EIRAS, Agostinho, *Segredo de Justiça e Controlo de Dados Pessoais Informatizados*, Coimbra Editora, Col. Argumentum, 4, 1992, p. 9 e 65 e ss.

[119] A este propósito, HELENA MONIZ refere que se encontram englobados por este direito: o direito de acesso aos dados e conhecimento de que os dados estão integrados numa certa base, o direito ao esclarecimento, o direito de retificação dos dados inseridos na base, o direito de atualização dos dados e o direito de eliminação de informações incorretas. MONIZ, Helena, *Notas sobre a proteção de dados*…, p. 253. Ainda nesta matéria, *vide* MARTINS, Lourenço, MARQUES, Garcia e DIAS, Pedro, *Ciberlaw em Portugal – O direito das tecnologias da informação e comunicação*, Centro Atlântico, 1.ª Edição, Setembro de 2004, p. 367-421.

países da União Europeia, obrigando à adoção de legislação interna em matéria de proteção de dados pessoais, estimulando a uniformização do nível de proteção concedido por todos os Estados membros, visando alcançar um patamar de segurança comum[120].

No nosso ordenamento jurídico a matéria da proteção de dados é assegurada e regulamentada pela ainda vigente Lei n.º 67/98, de 26/10, denominada de Lei da Proteção de Dados Pessoais, que, substituindo a Lei n.º 10/91, de 27/04, transpôs para o direito interno a Diretiva n.º 95/46/CE. Em consonância com o previsto na Diretiva n.º 95/46/CE, de 24/10, a Lei n.º 67/98 de 26/10, prevê o conceito de dados pessoais, no art.º 3.º, al. a), definindo-o *como "qualquer informação, de qualquer natureza e independentemente do respectivo suporte, incluindo som e imagem, relativa a uma pessoa singular identificada ou identificável ('titular dos dados');é considerada identificável a pessoa que possa ser identificada directa ou indirectamente, designadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social"*. Neste sentido, são considerados dados pessoais, entre outros, o nome, morada, residência, local de trabalho, endereço do correio eletrónico, o nº de telefone, n.º de cartão de cidadão, o n.º fiscal, o tipo sanguíneo, o IBAN da conta bancária, bem como demais elementos que, por estarem associados a uma pessoa, permitam identificá-la.

De acordo com o previsto no art.º 4.º, n.º 3, a Lei n.º 67/98, de 26/10, será aplicável "*a) No âmbito das actividades de estabelecimento do responsável do tratamento situado em território português"*, "*b) Fora do território nacional, em local onde a legislação portuguesa seja aplicável por força do direito internacional"* e "*c) Por responsável que, não estando estabelecido no território da União Europeia, recorra, para tratamento de dados pessoais, a meios, automatizados ou não, situados no território português, salvo se esses meios só forem utilizados para trânsito através do território da União Europeia",* cabendo, nos termos do art.º 22.º e 23.º deste diploma, à Comissão Nacional de Proteção de Dados controlar e fiscalizar o cumprimento das disposições legais e regulamentares em matéria de proteção de dados pessoais.

[120] CRATO, Nuno Teixeira, *The Walking Virtually Dead: Entre uma Algoritmocracia Jus Constituendum e um Homem Virtual Transparente, Existe Espaço para o Direito a uma Identidade Informacional?,* Dissertação de Mestrado em Segurança da Informação e Direito no Ciberespaço, Universidade de Lisboa, Out. 2016, p. 34 e ss.

Ainda em matéria de comunicações eletrónicas, reveste importância a Lei n.º 41/2004[121], de 18/08, que transpôs para a ordem jurídica nacional a Diretiva n.º 2002/58/CE, do Parlamento Europeu e do Conselho, de 12/07, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas, regulamentando, assim, o tratamento de dados pessoais no contexto das redes e serviços de comunicação eletrónicas acessíveis ao público, especificando e complementando as disposições da Lei n.º 67/98, de 26 de outubro[122]. Denote-se que as operadoras de telecomunicações guardam informação respeitante à identificação dos seus clientes, e respeitante às comunicações por si efetuadas. Com efeito, a Lei 41/2004, de 18/08, estabelece regulamentação especial, designadamente, em matéria de tratamento de dados de base, localização, tráfego e conteúdo, sujeitando-os, consoante o seu tipo, a diferentes procedimentos de tratamento, visando zelar pela privacidade tanto dos assinantes – que contrataram com uma empresa a prestação de serviços de comunicações eletrónicas – como dos utilizadores desses serviços. Neste conspecto, nos termos do art. 4º, n.º1, da Lei nº 41/2004, salvo consentimento prévio do utilizador e exceção dos casos previstos na lei, estão as empresas fornecedoras de redes e serviços vinculadas a garantir a inviolabilidade de comunicações e dos dados de tráfego a elas inerentes, assim como, nos termos do n.º 2, estão proibidas de escutar, instalar dispositivos de escuta, intercetar ou vigiar as comunicações e seus dados de tráfego[123]. Ainda pela Lei n.º 41/2004 foi atribuída à CNPD e ao ICP-ANACOM – Autoridade Nacional de Comunicações[124], as questões relacionadas com a supervisão, controlo do funcionamento e garantia da segurança no tratamento de dados pessoais, no âmbito das comunicações eletrónicas.

Cabe ainda referenciar, no quadro normativo das comunicações eletrónicas, a Lei n.º 5/2004[125], de 10/02, denominada de Lei das Comunicações Eletrónicas, que estabelece

---

[121] Alterada pela Lei n.º 46/2012, de 29/08, que transpôs a Diretiva n.º 2009/136/CE, na parte que altera a Diretiva n.º 2002/58/CE, do Parlamento Europeu e do Conselho, de 12 de julho, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas.

[122] A Lei nº 41/2004, de 18/08, protege os interesses dos assinantes e utilizadores dos serviços, quer sejam pessoas singulares quer coletivas, contrariamente à Lei 67/98 que se aplica apenas a dados pessoais de pessoas singulares.

[123] O art.º 6.º, da Lei nº 41/2004, de 18/08, disciplina as circunstâncias em que devem ser tratados e armazenados os dados de tráfego pelas operadoras.

[124] A Autoridade Nacional de Comunicações – ANACOM tem por missão a regulação do setor das comunicações. Acessível *online* no endereço http://www.anacom.pt/render.jsp?categoryId=381611#.VSkKANzF9yU [acedido em 05 de Janeiro de 2017].

[125] Transpôs as Diretivas n.ºs 2002/19/CE, 2002/20/CE, 2002/21/CE (alteradas pela Diretiva n.º 2009/140/CE, do Parlamento Europeu e do Conselho, de 25/11) e 2002/22/CE (alterada pela Diretiva

o regime jurídico aplicável às redes e serviços de comunicações eletrónicas e aos recursos e serviços conexos, definindo as competências da autoridade reguladora nacional neste domínio (ICP-ANACOM).

Ainda no âmbito das comunicações eletrónicas, de salientar a Lei n.º 32/2008, de 17/7, que, transpondo a Diretiva n.º 2006/24/CE[126], do Parlamento Europeu e do Conselho, de 15/3, veio regular a conservação e transmissão dos dados de tráfego e localização, e os dados relevantes para a identificação do assinante ou o utilizador, garantindo a investigação e repressão de crimes graves, consagrando-se, desde logo, no n.º 2, do art.º 1.º, deste diploma, a proibição de conservação de dados que revelem o conteúdo das comunicações, sem prejuízo das exceções previstas na Lei.

Os significativos avanços tecnológicos, os caminhos alumiados pela jurisprudência do TJUE e o tão almejado mercado único digital para a Europa (em vista no *Horizon 2020*), levariam a que, no ano de 2016, fosse publicado o Regulamento (UE) 2016/679, do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares, no que diz respeito ao tratamento de dados pessoais e à livre circulação desses mesmos dados. Assim, tendo entrado em vigor no dia 25 de maio de 2016, e prevendo um período transitório de dois anos para a sua total aplicação (sendo aplicável a partir de 25 de maio de 2018), o RGPD vem revogar a Diretiva 95/46/CE[127], garantindo uma verdadeira harmonização legislativa, atendendo que é diretamente aplicável em todos os 28 Estados-Membros da União Europeia, sem necessidade de qualquer transposição, vinculando as empresas/organizações a iniciar procedimentos com vista a adaptarem as suas atuais estruturas às novas exigências legais, sob pena de lhes serem aplicadas as coimas previstas no art.º 83.º do RGPD.

De tal modo, contrariamente à existência das ainda vigentes 28 legislações, o que origina, conforme considerando 9 do RGPD, uma "*fragmentação da aplicação da proteção dos dados ao nível da união",* assim como *"insegurança jurídica ou o sentimento generalizado da opinião pública de que subsistem riscos significativos para a proteção das pessoas singulares, nomeadamente no que diz respeito às atividades por via eletrónica*", visa o RGPD contribuir: (1) para a realização de um espaço de liberdade, segurança e

2009/136/CE DO Parlamento Europeu e do Conselho de 25/11) todas do Parlamento Europeu e do Conselho de 07/03, e da Diretiva n.º 2002/77/CE, da Comissão de 16/09.

[126] Altera a Diretiva 2002/58/CE.

[127] Até 25 de Maio de 2018 continuará a vigorar a lei 67/98.

justiça e de uma união económica; (2) para o progresso económico e social; e (3) para o bem-estar das pessoas singulares[128].

Assim, ante este novo quadro jurídico em matéria de proteção de dados, são consagradas alterações de fundo no que respeita ao tratamento de dados pessoais, contemplando-se, para além de um novo conceito de dados pessoais, um avolumado número de medidas com vista à proteção da privacidade pessoal, como é o caso do reforço dos direitos do titular dos dados, designadamente, o aprofundamento do direito à transparência e do direito de informação e acesso aos dados pessoais, consubstanciado na exigência de maior rigor no tipo de informações a prestar ao titular dos dados e pelo incremento dos requisitos do consentimento[129], prevendo-se regras especiais de tutela de dados de menores[130]. Doutro passo, consagrando-se o "direito a ser esquecido" e o direito à portabilidade dos dados[131], vem o RGPD alargar o seu âmbito de aplicação às entidades responsáveis (*controllers*) pelo tratamento de dados pessoais no território da União Europeia, ou subcontratantes (*processors*), independentemente do responsável pelo tratamento se encontrar, ou não, localizado na UE, vinculando-o à implementação de mecanismos eficazes de códigos de conduta (*compliance*), densificando-se o princípio da transparência. Por seu turno, o RGPD implementa novos deveres aos responsáveis pelo tratamento dos dados, nomeadamente, impondo-lhes obrigações com vista à adoção de políticas específicas de proteção de dados, como é o caso do uso da pseudonimização, da confidencialidade e a cifragem de dados, da elaboração de avaliações de impacto sobre a proteção de dados, quando o uso de novas tecnologias for suscetível de implicar um elevado risco para os direitos dos titulares dos dados a tratar, passando a ser obrigatória uma consulta prévia à autoridade de controlo (CNPD) antes do tratamento destes mesmos dados, sendo ainda obrigatório o registo de todas as atividades de tratamento a cargo do

[128] TEIXEIRA, Angelina, *A Chave para a Regulamentação da Proteção de Dados*, Data Venia, Revista Jurídica Digital, n.º 6, Novembro 2016, p. 6-32. A destacar o facto do Tratado de Lisboa, de Dezembro de 2009, estabelecer no art.º 16.º do TFUE que "*Todas as pessoas tem direito à proteção dos dados de caráter pessoal que lhes digam respeito (…)"*.

[129] De acordo com o art.º 7.º, n.º 2, do RGPD, passa-se a exigir que o pedido de consentimento seja apresentado numa manifestação de vontade, livre, específica, informada e explícita, de uma forma inteligível, de fácil acesso e numa linguagem clara e simples.

[130] Estando em causa uma oferta direta de serviços a menores, o tratamento dos dados pessoais só será lícito se estes tiverem pelo menos 16 anos.

responsável pelo tratamento, ficando, ainda, plasmado um dever de cooperação institucional com a autoridade de controlo nacional, por via da nomeação de um encarregado de proteção de dados (*data protection officer*).

5. O Regime Jurídico Aplicável ao Correio Eletrónico no Código de Processo Penal

5.1. Do CPP de 1987 até à Reforma de 2007

A reflexão acerca da natureza do regime jurídico aplicável ao correio eletrónico, enquanto prova eletrónica apresentada sob a forma digital, compreende uma constelação de enigmas que exigem uma reconstrução conceptual complexa, vinculando-nos a viajar pelo conturbado percurso legislativo a que o correio eletrónico foi submetido, por via das várias reformas operadas ao CPP, só assim se percecionando a amplitude da intensa discussão doutrinária e jurisprudencial em que esta prova se vê mergulhada, mesmo após o seu desaguamento nas águas dos novos meios de obtenção de prova dispostos na nova Lei do Cibercrime.

Com efeito, reforçando o que temos vindo a expor, a tipificação criminal de condutas que envolvessem a violação de correspondência cedo mereceu a tutela do legislador português. De tal modo, no capítulo III, do título V, do Código Penal de 1886, sob a epígrafe "*Dos que abrem cartas alheias ou papéis e da revelação dos segredos*", era punido, no art.º 461.º deste diploma, todo o comportamento "*malicioso*" que atentasse à violação de escrito destinado a outrem. A par desta tipificação, também a nível processual, no CPP de 1929[132], era disciplinado o modo e a forma de apreensão da correspondência, evidenciando-se assim que, desde os tempos mais remotos, existiu uma efetiva preocupação de se consagrarem, no nosso ordenamento jurídico, normas que cuidassem de salvaguardar a proteção da privacidade como, *in casu*, o sigilo da correspondência. De resto, também na própria Constituição de 11 de abril de 1933, no art.º 8.º, n.º 6, eram salvaguardados os direitos e garantias da inviolabilidade do domicílio e o sigilo da correspondência[133], remetendo-se para a legislação ordinária a regulamentação desta inviolabilidade.

---

[132] O CPP de 1929 foi aprovado pelo Decreto n.º 16.489, de 15/02, e vigorou no ordenamento jurídico português até à criação do atual CPP que teve a sua génese no Dec. Lei n.º 78/87, de 17/02. No art.º 210.º, do CPP de 1929, era feita referência à apreensão de correspondência *"Nos correios, telégrafos e estações radiotelegráficas*", ali se prevendo a possibilidade de se realizarem "*buscas e apreensões de cartas, encomendas, valores, telegramas e qualquer outra correspondência dirigida ao arguido, ou a outras pessoas que tenham relação com o crime (...)."*

[133] Neste conspecto, também a Carta Universal dos Direitos do Homem, proclamada em 10 de Dezembro de 1948, consagrava, no seu art.º 12.º, a proteção contra as intromissões na vida privada, na família, no domicílio ou na correspondência.

Com a revolução de 25 de Abril de 1974, e consequente redação de uma nova Constituição (1976), manteve-se postulada constitucionalmente, no art.º 34.º da Lei mãe, a proibição de qualquer violação do domicílio e da correspondência, proteção esta que viria a ser estendida às vias telemáticas, acabando o legislador, na revisão constitucional de 1997, por aditar a esta disposição, no seu n.º 4, a expressão *"e nos demais meios de comunicação"*, consagrando-se, assim, uma ampla extensão da proibição de ingerências nas comunicações.

Em obediência aos princípios estruturantes da CRP de 1976, os ventos sopraram de feição ao nascimento de um novo Código Penal, materializado por via do DL n.º 400/82, de 23/09, tendo-se procedido à tipificação criminal do ilícito de violação de correspondência, prevendo-se, no art.º 182.º deste diploma, sob a epígrafe *"Violação do segredo de correspondência e telecomunicações",* a pena de "*prisão até 6 meses e multa até 50 dias*" para *"quem, sem consentimento de quem de direito, abrir encomenda, carta ou qualquer outro escrito que se encontre fechado e que não lhe seja dirigido (...)",* punindo-se, igualmente, quem se intrometesse *"no conteúdo de comunicação telefónica ou telegráfica"*.

Com a entrada em vigor do DL n.º 48/95, de 15/03, o qual procedeu a uma nova sistematização do Código Penal, a tipificação deste ilícito foi consagrada no art.º 194.º[134] deste diploma, mantendo-se esta redação inalterada, pese embora as sucessivas alterações ao CP.

Paralelamente, a nível processual penal, também na versão originária do CPP de 1987, eram consagradas no Capítulo IV, do Título III ("*Dos meios de obtenção de prova*"), normas processuais que regulamentavam a obtenção da prova e que acabariam, ainda hoje, por se manter vigentes. Falamos dos meios clássicos de obtenção de prova, aqui se

---

[134] *"Artigo 194.º*
Violação de correspondência ou de telecomunicações
1 – Quem, sem consentimento, abrir encomenda, carta ou qualquer outro escrito que se encontre fechado e lhe não seja dirigido, ou tomar conhecimento, por processos técnicos, do seu conteúdo, ou impedir, por qualquer modo, que seja recebido pelo destinatário, é punido com pena de prisão até um ano ou com pena de multa até 240 dias.
2 – Na mesma pena incorre quem, sem consentimento, se intrometer no conteúdo de telecomunicação ou dele tomar conhecimento.
3 – Quem, sem consentimento, divulgar o conteúdo de cartas, encomendas, escritos fechados, ou telecomunicações a que se referem os números anteriores, é punido com pena de prisão até um ano ou com pena de multa até 240 dias."

compreendendo os exames (art.ºs 171.º a 173.º), as revistas e buscas (art.ºs 174.º a 177.º), as apreensões (art.ºs 178.º a 186.º) e as escutas telefónicas (art.ºs 187.º a 190.º).

Ora, na sistematização do CPP de 1987, e no que à matéria do correio eletrónico se circunscreve, lograva destaque a contemplação de quatro artigos relativos às escutas telefónicas. Assim, desde início, mais propriamente no art.º 190.º do mencionado Capítulo IV, o legislador consagrou uma extensão da aplicação do regime das escutas "*(…) às conversações ou comunicações transmitidas por qualquer meio técnico diferente do telefone*", sendo que era, precisamente, esta expressão, "*diferentes do telefone*", que originava dúvidas interpretativas acerca do desiderato do legislador. De facto, à época, não existiriam dúvidas que, por referência às vias telemáticas, caberiam neste meio de obtenção de prova, para além do telefone, o telefax por exemplo. Todavia, faria sentido estender o âmbito de aplicação às comunicações realizadas por via da Internet? O convite à reflexão assume maior amplitude e elasticidade de articulação do regime se pensarmos que o fenómeno do fluxo de trocas comunicacionais, por via da Internet, apenas na década de 90 despontou e começou a ganhar dimensão, sempre se impondo a questão: Teria o legislador pensado esta extensão, da aplicação do regime das escutas, às comunicações realizadas por via da Internet?

De entre as vozes críticas à opção do legislador, estribando-se na Lei Fundamental, FARIA COSTA[135] pronunciou-se sobre este regime de extensão aludindo que *"Ninguém dúvida de que todo o regime das escutas telefónicas tem de ser entendido como verdadeiramente excepcional. De sorte que já a norma de extensão, em um horizonte crítico muito rigoroso, não se compreende de maneira satisfatória. Ou seja: o regime excepcional, porque excepcional, não pode alargar-se, sob pena de contradição palmar e insanável. No entanto, o legislador alargou-o. Que razoável e não contraditória razão de ser se pode, então, encontrar para um tal alargamento? Só uma resposta pode caber à pergunta anterior: o legislador quis que os novos meios de telecomunicação da palavra fossem também susceptíveis de sobre eles se escutar, nas condições legais previstas, as conversações ou comunicações, mas o legislador não quis nem podia - porque se o fizesse cairia na insuportável contradição ou aporia normativa - que outros instrumentos de telecomunicação que possibilitam outro tipo de palavra, que não a falada, caíssem no*

[135] COSTA, José de Faria, *As telecomunicações e a privacidade: o olhar (in)discreto de um penalista*..., p. 76-77.

âmbito das escutas telefónicas. Julgamos ser esta a interpretação mais correcta perante o carácter excepcional da norma que se estuda. O que, bom é de ver, não impede que o legislador - em diferente e autónoma valoração - possa, através de nova intervenção legislativa, vir a considerar que o conteúdo das comunicações levadas a cabo por meio da palavra virtual possa ser, legitimamente, apreendido. Mas para que isso aconteça deve antes haver norma que o permita. E isso é tarefa do legislador e não do intérprete". A propósito da extensão consagrada no art.º 190.º do CPP, também COSTA ANDRADE advogava que se tratava de *"um regime em princípio reservado às formas de comunicação oral, isto é, que possibilitam a emissão e recepção da própria palavra falada. Dele estarão, por exemplo, excluídas formas de comunicação como o telégrafo ou o telefax. Será, assim, desde logo, por razões atinentes à carência de tutela. Isto por ser manifesto que a intromissão indevida nas comunicações telegráficas não actualiza o atentado ao direito à palavra, que constitui um dos coeficientes de maior peso da danosidade social das escutas telefónicas. Acresce ser a própria lei a submeter expressamente o telegrama ao regime específico - e diferente do das escutas telefónicas - da apreensão de correspondência. Este é, de resto, o entendimento prevalecente na Alemanha, apesar de os preceitos homólogos da StPO (§§100a) e 100b)) se reportarem não às escutas telefónicas, mas antes e de forma mais genérica às intromissões nas telecomunicações (Überwachung dês Fermeldeverkehrs)*"[136].

Não obstante, certo é que, com a Lei n.º 58/98, de 25/08, o art.º 190.º do CPP sofreu uma significativa alteração, colocando o legislador, quanto às comunicações eletrónicas (ao que nos interessa o correio eletrónico), um ponto de ordem nas dúvidas que se levantaram na redação originária da norma. De tal modo, passou esta disposição legal a consagrar que "*O disposto nos artigos 187.º, 188.º e 189.º é correspondentemente aplicável às conversações ou comunicações transmitidas por qualquer meio técnico*

[136] ANDRADE, Manuel da Costa, *Sobre as proibições de Prova em Processo Penal*, Reimpressão, Coimbra Editora, 2006, p. 274-275. Sobre a matéria, *vide* ANDRADE, Manuel da Costa, *As Escutas Telefónicas como meio de obtenção de prova no novo Código de Processo Penal de Macau,* in Revista Jurídica de Macau, Volume IV, n.° 1, 1997, p. 75. No mesmo sentido apontam FARIA COSTA e HELENA MONIZ ao advertirem que a extensão incorporada no art. 190.° do CPP, não vale para os "*meios electrónicos cujo paradigma é a palavra escrita e não a palavra falada (e por isso mesmo não pode haver "escutas" do fax ou do telegrama).*" Cfr. COSTA, José de Faria e MONIZ, Helena, "*Algumas Reflexões sobre a Criminalidade Informática em Portugal*" in BFDUC, Vol. LXXIII, 1997, p. 344.

diferente do telefone, designadamente correio eletrónico ou outras formas de transmissão de dados por via telemática, bem como à intercepção das comunicações entre presentes". Assim, de forma elucidativa, a Lei n.º 58/98, de 25/08, representou um importante marco histórico na "vida" do correio eletrónico, ao ter reconhecido e disciplinado esta forma de comunicação no processo penal. Nasceria, porém, outro problema controverso, condizente à contemplação da terceira parte do aludido art.º 190.º, designadamente, a inserção da possibilidade de interceção das comunicações entre presentes, ou, se lhe quisermos chamar, ambientais.

Com a Lei 48/2007, de 29/08, o regime das escutas telefónicas viria a sofrer alterações substanciais, quer quanto aos requisitos de admissibilidade que lhe estavam intrínsecos, quer propriamente quanto às formalidades a que estava submetida esta diligência, convertendo os art.ºs 187.º e 188.º em disposições legais mais extensas e descritivas, acabando a reforma legal por introduzir inovações de fundo quanto ao papel do juiz no controlo da legalidade das escutas, particularmente, nas delimitações temporais, nos requisitos de destruição e no círculo de pessoas passíveis de ser escutadas.[137] A própria sistematização das disposições legais no CPP sofreu alterações, realizando-se uma inversão destes artigos, passando agora o art.º 189.º a realizar a extensão do regime das escutas telefónicas a outras formas de comunicação, e o art.º 190.º a consagrar o efeito da nulidade. Assim, com a revisão do CPP, operada pela Lei nº 48/2007, de 29/08, o legislador procedeu à ampliação do antigo art.º 190.º[138] (atual 189.º), estendendo a aplicação do regime das escutas telefónicas às comunicações ou conversações electrónicas armazenadas em suporte digital.

Neste seguimento, no que ao correio eletrónico diz respeito, com a reforma de 2007 ao CPP, o legislador consagrou no seu art.º 189.º duas inovações que, até então, eram desconhecidas na regulamentação processual penal. Assim, com a inserção do n.º 1 deste

---

[137] Sobre a matéria, *vide* CONCEIÇÃO*,* Ana Raquel*, Escutas Telefónicas - Regime Processual Penal,* Quid Juris Editora, 2009; LEITE, André Lamas, *Entre Péricles e Sísifo*…, p. 613-669; ALBRECHT, Hans-Jörg, "*Vigilância das telecomunicações. Análise teórica e empírica da sua implementação e efeitos"*, in *Que futuro para o direito processual penal? Simpósio em Homenagem a Jorge de Figueiredo Dias, por ocasião dos 20 anos do Código de Processo Penal Português*, Coord. Mário Ferreira Monte, Trad. Inês Fernandes Godinho, Coimbra Editora, 2009, p. 725-743. Com uma visão crítica da aplicação prática que vem sendo dada ao regime das escutas, *vide* JÚDICE, José Miguel, *Escutas telefónicas: a tortura do século XXI*, Revista da Ordem dos Advogados, Ano 64, Vol. I/II, Novembro, 2004.

[138] O antigo artigo 190.º passou a determinar que "*o disposto nos artigos 187.º, 188.º e 189.º é correspondentemente aplicável às conversações ou comunicações transmitidas por qualquer meio técnico diferente do telefone, designadamente correio electrónico ou outras formas de transmissão de dados por via telemática, bem como a interceção das comunicações entre presentes*."

acervo normativo, contemplar-se-ia a possibilidade de se intercetar as mensagens de correio eletrónico, assim como outras formas de transmissão de dados informáticos, *"mesmo que se encontrassem guardadas em suporte digital*"[139]. Para além desta consagração, o art.º 189.º, n.º 2, do CPP, passou a dispor que "*A obtenção e junção aos autos de dados sobre a localização celular ou de registos da realização de conversações ou comunicações só podem ser ordenadas ou autorizadas, em qualquer fase do processo, por despacho do juiz, quanto a crimes previstos no n.º1 do artigo 187.º e em relação às pessoas referidas no n.º 4 do mesmo artigo*".

Certo é que, com a reforma de 2007, sobretudo, no que toca à nova redação do art.º 189.º do CPP, n.ºs 1 e 2, o legislador veio semear o pânico entre os intérpretes e aplicadores do direito, emaranhando conceitos e adensando contradições, deixando escapar por entre os dedos a enorme chance de autonomizar o direito informático, designadamente, a prova digital, pois tinha na mão o poder de efetuar uma autonomização do direito informático, compilando tudo numa só legislação, ao invés de adensar a confusão gerada pelos diversos diplomas avulsos em vigor e que, por vezes, são contraditórios, acabando por comprimir e subsumir sob o mesmo regime, *mutatis mutandis*, duas formas de comunicação completamente distintas entre si: o telefone e o correio eletrónico.

[139] Conforme consta da primeira ata, dentro das trinta e uma reuniões levadas a cabo pela Unidade de Missão para a Reforma Penal, logo cuidou RUI PEREIRA de deixar claro que haveriam de ser introduzidas alterações à interceção de comunicações, atendendo à Jurisprudência que vinha sendo cultivada pelo Tribunal Constitucional.

5.2. Da (In)Submissão do Correio Eletrónico ao Regime das Escutas Telefónicas

Conforme temos vindo a aludir, a última grande reforma do CPP ficou aquém das expetativas, não tendo o legislador aproveitado os ventos que sopravam na direção de autonomizar a prova digital, misturando, utilizando-se os dizeres de MICHAEL MADISON[140], "*as coisas reais*" e as "*coisas jurídicas*" que "*acabam por ter implicações na legitimidade e na autoridade da lei*". Assim, ao invés de se repensar a regulação específica da prova digital decorrente dos fluxos comunicacionais, assegurando-se a centralidade normativa do CPP, o legislador optou por condensar e disciplinar a recolha das mensagens de correio eletrónico, independentemente de questionar o seu estado, no regime previsto para as escutas telefónicas, apresentando-se tal regime, nas palavras de PAULO DÁ MESQUITA, como o "*quadro global da regulação da intercepção e registo de telecomunicações*"[141].

Desta feita, até à entrada em vigor da Lei do Cibercrime, sobre a qual oportunamente nos debruçaremos, o art.º 189.º, n.º 1, do CPP, era a única disposição legal que disciplinava a admissibilidade da recolha da prova digital, acabando tal opção legislativa por se deparar com um intenso coro de críticas doutrinais e jurisprudenciais. Desde logo, FARIA COSTA aludiu ao facto da "*elaboração da respetiva proposta*" (que esteve na base da Lei nº 48/2007, de 29 de Agosto) exigir "*um labor e um rigor científicos, que visivelmente, não precederam a proposta em análise*.[142]. A este respeito, também FIGUEIREDO DIAS[143] acentuou a reforma como uma "*oportunidade perdida*", profundamente lacunosa, revelando a ausência de pensamento conceptual sobre a teleologia e semântica em torno dos institutos probatórios das novas tecnologias. Por sua vez, juntando-se ao coro de críticas à reforma, COSTA ANDRADE vem tecer reparos ao legislador, chegando mesmo a apelidar o art.º 189.º do CPP como a *"casa dos horrores hermenêuticos"*[144], devido ao facto de englobar várias realidades distintas, misturando

[140] MADISON, Michael, *Law as Design: Objects, Concepts, and Digital Things*, Case Western Reserv Law Review, v.56, 2005, p. 381-478.
[141] MESQUITA, Paulo Dá, *Processo Penal, Prova e Sistema Judiciário,* Wolters Kluwer, Coimbra Editora, 1.ª Edição, Set. 2010, p. 89.
[142] COSTA, José de Faria, *apud* MESQUITA, Paulo Dá, *Processo Penal, Prova e Sistema*…, p. 88.
[143] DIAS, Figueiredo, *Sobre a Revisão de 2007 do Código de Processo Penal Português*, RPCC, ano 18, n.º 2/3, 2008, p. 385.
[144] ANDRADE, Manuel da Costa, *Bruscamente no verão passado…,* p. 185.

diferentes exigências tutelares, causando incerteza e insegurança jurídica, dificultando, de resto, o controlo legal por parte das instâncias judiciais competentes. De tal modo, para COSTA ANDRADE, o facto de o legislador ter optado por um modelo assente numa cláusula de extensão, disciplinada a partir das escutas telefónicas, implicou tratar por igual três realidades distintas: *"(…) primeiro, intromissão nas telecomunicações; segundo, acesso a "documentos" guardados no computador e que resultaram de comunicações eletrónicas; terceiro, gravações de conversas entre presentes".*[145] Por seu lado, PAULO DÁ MESQUITA[146] destaca que a extensão do regime das escutas ao correio eletrónico, oferece graves repercussões na interação comunicacional e registos de dados informáticos, privilegiando os suportes digitais, sempre se exigindo que a extensão parasse, precisamente, onde acabariam as telecomunicações.

Sobrelevando o facto da solução normativa consagrada ter procedido a um alargamento inadmissível no "*âmbito de uma restrição a um direito fundamental: o direito à inviolabilidade do sigilo das comunicações privadas (artigo 34.º, n.ºs 1 e 4 da CRP)",* é por BENJAMIM SILVA RODRIGUES reprovada a opção do legislador, no sentido de trazer para dentro do regime das escutas telefónicas a regulação da interceção de comunicações, nomeadamente, do correio eletrónico, atendendo que nas "*mensagens escritas e imagens, o seu acesso não pode ocorrer a partir do regime das escutas telefónicas por não entrar dentro do ´paradigma da ponderação legalmente codificado´" que subjaz a tal regime, pensado apenas para as comunicações orais*.[147]

A este propósito, também na profícua jurisprudência cultivada em diversos arestos dos Tribunais Portugueses, acabaria o Julgador por fazer uma interpretação *contra legem* do preceito em questão, designadamente, e a título de exemplo, no não reconhecimento do previsto no art.º 189.º, n.º 1, segunda parte, do CPP, nos casos de apreensão de mensagens de telefone (SMS) que tivessem sido recebidas, lidas e armazenadas pelo destinatário, equiparando-as a um mero documento escrito, decidindo no sentido de que estas mensagens não beneficiariam da aplicação do específico regime de proteção previsto no art.º 189.º do CPP. Neste trilho, assim foi decidido e melhor motivado nos Acórdãos do

[145] ANDRADE, Manuel da Costa, *Bruscamente no verão passado…,* p. 185.
[146] MESQUITA, Paulo Dá, *Processo Penal, Prova e Sistema…,* p. 88.
[147] RODRIGUES, Benjamim Silva, *A Monitorização dos Fluxos Informacionais e Comunicacionais - (Contributo para a Superação do "Paradigma da Ponderação Constitucional e Legalmente Codificado" em Matéria de Escutas Telefónicas),* Vol. II, Coimbra, Coimbra Editora, 2009, p. 359 e 360.

Tribunal da Relação de Lisboa, de 15 de Julho de 2008[148], proferido sob o Processo n.º 3453/2008-5, da Relação de Guimarães, de 12 de Outubro de 2009[149], proferido sob o Processo n.º 1396/08.1PBGMR – A.G1 e da Relação do Porto, de 27 de Janeiro de 2010[150], proferido sob o Processo n.º 896/07.5JAPRT.P1.

Sem mais, nesta matéria, subscrevemos, na íntegra, a posição dos Autores que fizemos referência, comungando dos reparos que fazem relativamente à reforma operada ao CPP de 2007. Na verdade, é a partir das suas explanações que nos é permitido alavancar outras considerações, a fim de, em matéria de ingerências no correio eletrónico, suster aquela que é a nossa posição.

5.2.1. A Palavra Falada e a Palavra Escrita

A ponderação acerca da natureza da comunicação estabelecida por via do telefone e do correio eletrónico, enquanto meios manifestamente distintos de comunicação, só por si, já seria motivo suficiente para nos impedir de concordar com a cláusula de extensão operada no art.º 189.º do CPP. Assim, invocando aquelas que são as características do correio eletrónico e cotejando-as com as particularidades da conversação telefónica, cremos que, enquanto comunicação, apenas um dos meios, verdadeiramente, é suscetível de ofender o direito à palavra falada, colocando-se o outro no domínio da palavra escrita.

Conforme já referimos, COSTA ANDRADE e FARIA COSTA defendem que o regime das escutas telefónicas, estabelecido no CPP de 1987, foi estruturado e teleologicamente pensado para as conversações orais. Anuindo a tais considerações, é nossa convicção que o critério distintivo da aplicação do regime legalmente estabelecido para as escutas telefónicas, ainda que não se afira, propriamente, por via do equipamento técnico pelo qual a comunicação é transmitida (até porque como é consabido um

[148]Acessível online no endereço:
http://www.dgsi.pt/jtrl.nsf/0/9182245992c7c5d18025749000503b8c? OpenDocument [acedido em 18 de Dezembro de 2016].
[149]Acessível *online* no endereço:
http://www.dgsi.pt/jtrg.nsf/86c25a698e4e7cb7802579ec004d3832/4c03909839f95d5f8025767e004f83fe?OpenDocument [acedido em 18 de Dezembro de 2016].
[150]Acessível *online* no endereço:
http://www.dgsi.pt/jtrp.nsf/c3fb530030ea1c61802568d9005cd5bb/68fdcdf35dc62b6e802576c40041c7 9 [acedido em 19 de Dezembro de 2016].

smartphone possui hoje um vasto conjunto de funcionalidades que permitem que a comunicação se faça por via da voz e escrita), não deverá deixar de incidir sobre a natureza da comunicação em si mesma, colocando-se o critério distintivo no âmbito da pretensão de intercetar e registar conversações telefónicas, reconhecendo-se os desequilíbrios protecionais existentes entre a palavra falada e a palavra escrita.

Repare-se que, face ao aparecimento e *boom* das aplicações informáticas, como o *Skype, o Whatsapp, o Viber, o Hangouts*, entre outros, é possível estabelecer-se conversações orais por via de tecnologia VoIP, onde a voz é convertida em sinal digital, o qual, depois de circular pela Internet, é novamente convertido em voz, sendo suscetível de interceção e registo no processo de (des)codificação, desde que verificados e cumpridos os requisitos legais. Neste conspecto, é uma realidade objetiva que os processos comunicativos das novas tecnologias estão hoje desenvolvidos, quer para as conversações orais, quer para as comunicações escritas[151]. Ora, facto é que, quando se procede ao envio, a específico destinatário, de um determinado *e-mail*, a intencionalidade é perpetuar uma mensagem, deixando-se, inclusivamente, de se ter controlo sobre a mesma, podendo o seu destinatário, se assim o entender, apresentá-la a terceiros. O contrário já não sucede numa conversação oral. A palavra falada é dirigida para se extinguir naquele mesmo momento. Assim, se no caso da palavra escrita o emissor da mensagem sabe que esta ficará registada e no poder do destinatário, já no caso da palavra falada foi necessário impor ao destinatário da palavra a ilicitude do seu registo não autorizado.

Na verdade, no momento posterior à comunicação, a palavra escrita permanece no espaço cibernético, contrariamente à palavra falada que esgota o seu âmbito após o *términus* da comunicação, merecendo, conforme BENJAMIM SILVA RODRIGUES, a palavra escrita de uma proteção a nível do direito à privacidade e à autodeterminação informacional. No fundo, no trilho do Autor, ao ter tentado o legislador português adaptar o regime das escutas telefónicas às novas formas de comunicação de "*forma inepta e criticável, ao optar por um `alargamento´ ou `extensão´ das técnicas de intervenção e gravação das comunicações e conversações quando elas são levadas a cabo por outros*

[151] CATARINA CASTRO denomina a palavra comunicada por via de *e-mail* de "palavra virtual". Todavia, acompanhando-se o entendimento maioritário, cremos que a palavra virtual, consoante o caso, caberá na dual categoria de palava falada/escrita. CASTRO, Catarina Sarmento, *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.

meios técnicos `diferentes de telefone´"[152], acabou por negligenciar a circunstância do correio eletrónico não ser passível das ingerências configuradas pelo regime de obtenção de prova do regime das escutas telefónicas.

Nesta senda, também SIMAS SANTOS e LEAL – HENRIQUES pugnam que *"o regime das escutas telefónicas (…) apenas incide sobre os chamados processos de comunicação oral (ou seja os que aceitam e enviam a palavra falada), não se alargando, por isso, a outros expedientes de comunicação em que não entra a palavra falada, como, por exemplo, o telégrafo, o telefax, etc."*[153]. No mesmo sentido, a propósito da reflexão acerca das ingerências no correio eletrónico, e estribando-se nos ensinamentos da doutrina supra, conclui RITA CASTANHEIRA NEVES que "*se a pretensão da investigação criminal for outra, a de aproveitar as novas tecnologias de comunicação eletrónica e interceptar e gravar mensagens escritas, então aqui, seremos impelidos a aplicar diferente regime do consagrado para as escutas telefónicas"*.[154]

Assim, pugnamos na pista da doutrina que considera que existem manifestas diferenças na natureza da palavra escrita e da palavra falada, bem como distinta graduação a nível da sua proteção. Com isto, não queremos dizer que alguma delas se encontra a descoberto do manto constitucional. Como temos vindo a expor, se é verdade que a palavra falada encontra postulação no art.º 26.º, n.º 1, da CRP[155], não é menos verdade que a Lei Fundamental, nos art.ºs 34.º, n.º4, e 35.º, protege igualmente a palavra escrita.[156] O âmbito que aqui pretendemos alcançar é um outro. Coloca-se, sobretudo, no domínio das Leis ordinárias, nomeadamente, a nível da proteção legal que o legislador quis dar à palavra falada e à palavra escrita na tipificação de alguns crimes do Código Penal. De tal modo, julgamos que, neste particular, o legislador, objetivamente, criminalizou específicas

---

[152] RODRIGUES, Benjamim Silva, *Das Escutas Telefónicas – A Monitorização dos Fluxos Informacionais e Comunicacionais*, Tomo I, Coimbra, Coimbra Editora, 2008, p. 60.

[153] SANTOS, Simas e HENRIQUES, Leal, *Código de Processo Penal Anotado*, 2.ª Edição, I Vol., Editora Rei dos Livros, 1999, p. 926.

[154] NEVES, Rita Castanheira, *As Ingerências nas Comunicações Eletrónicas em Processo Penal – Natureza e respectivo regime jurídico do correio electrónico enquanto meio de obtenção de prova*, Coimbra Editora, 1.ª Edição, Junho de 2011, p. 173.

[155] HELENA MONIZ defende que o direito à palavra, entendido como direito à voz e às "*palavras ditas*", se integra no âmbito dos dados pessoais, encontrando positivação constitucional no art.º 26.º da CRP. Também COSTA ANDRADE reconhece que a proteção constitucional, na aludida disposição, é a palavra falada pela intensa necessidade de proteção que carece. MONIZ, Helena, *Notas sobre a proteção de dados pessoais perante a informática (o caso especial dos dados pessoais relativos à saúde),*…, p. 261; ANDRADE, Manuel da Costa, *Sobre as Proibições de Prova*…p. 174-190.

condutas olhando ao meio como são praticadas, considerando que a perturbação da vida privada é suscetível de ser mais lesada se a prática do crime ocorrer por via da palavra falada. Repare-se no exemplo sistematizado no art.º 190.º, do CP, relativo à "*Violação de domicílio ou perturbação da vida privada*" que consagra, no seu n.º 2, uma pena de prisão até 1 ano ou pena de multa até 240 dias para quem, com intenção de perturbar a vida privada, a paz e o sossego de outra pessoa, telefonar para casa de alguém ou para o telemóvel. Atente-se, igualmente, na conduta incriminadora ínsita no art.º 199.º do CP, que consagra, no seu n.º 1, al. a), que comete o crime de gravações e fotografias ilícitas quem gravar palavras proferidas por outra pessoa e não destinadas ao público, mesmo que lhe sejam dirigidas, sendo punido com pena de prisão até 1 ano ou com pena de multa até 240 dias. Se no primeiro exemplo, é possível extrair que o legislador apenas quis proteger a privacidade de agressões suscetíveis de ofender a esfera privada, praticadas por via do telefone, e, portanto, na extensão restrita da palavra falada (excluindo da norma os casos em que as agressões se dão por via de mensagens escritas), no segundo caso, de igual forma, somos forçados a concluir que apenas estatuiu o legislador a criminalização de condutas que atentassem à palavra falada (excluindo da norma os casos em que as palavras sejam utilizadas sob a forma de escritos). Assim, também por via destes exemplos, saí reforçado o que se vem expondo, no sentido de que a palavra falada é mais possante e capaz de perturbar a privacidade sendo que, por tal via, entendeu o legislador a acrescida necessidade de conferir, nesta modalidade, uma maior proteção da paz e do sossego pessoais. No fundo, parafraseando-se FARIA COSTA, *"falar é muito mais do que aquilo que se diz em texto. Correndo o risco da distorção conceitual – risco que se assume para sublinhar a dimensão única e insubstituível da palavra – poder-se-á afirmar que a palavra é o suposto, a condição e, simultaneamente, o`essencial´segmento onto – antropológico do humano."*[157].

Doutro passo, conforme já vertido, o regime das escutas telefónicas consagrado no CPP de 1987, foi, teleologicamente, orquestrado como uma medida de ingerência de *ultima ratio* nas chamadas conversações orais, atendendo ao seu caráter de intromissão na esfera privada, nomeadamente, no domínio da privacidade das pessoas. Neste compasso, tipificou-se no art.º 187.º do CPP, um restrito catálogo de crimes em que a sobredita escuta

[157] COSTA, José de Faria, *As telecomunicações e a privacidade: o olhar (in)discreto de um penalista*..., p. 50.

poderia ocorrer.[158] Por tal via, repare-se que, nos termos do art.º 187.º, n.º1, al. e), do CPP (ainda hoje vigente), consagrou-se a possibilidade de serem alvo de interceção os crimes de injúria, ameaça, coação e devassa da vida privada, cometidos através de telefone, sendo que, como adiante melhor tratado, somente com a Lei 109/2009, de 15/09, concretamente, no art.º 18.º, al. b), se veio a consagrar a possibilidade destes crimes puderem ser alvo de interceção e gravação, quando praticados por via de comunicações eletrónicas. De tal forma, também deste prisma, é possível conceber que, até 2009, não era permitido, por inadmissibilidade legal, a intercetação de comunicações eletrónicas quando estes específicos crimes fossem cometidos por via informática.

Assim, se fosse verdadeira intenção do legislador estender o regime das escutas aos crimes tipificados no art.º 187.º, n.º 1, al. e), do CPP, quando praticados por via informática, nomeadamente, com recurso ao uso da palavra escrita, teria aproveitado as sucessivas reformas do CPP, para introduzir nesta alínea os casos em que os crimes são cometidos por outra via que não apenas o telefone. O que não fez.

Atente-se num outro aspeto, fundamentalmente, de cariz conceptual. Recorrendo-se à noção de correio eletrónico, disposta no art.º 2.º, n.º1, al. b), da Lei n.º 41/2004, de 18/08, com a alteração que lhe foi operada pela Lei n.º 46/2012, de 29/08, bem como às concepções adiantadas pela doutrina a que já fizemos referência, podemos concluir que o correio eletrónico pode ter um suporte de texto, gráfico ou de voz, importando sempre a figura de um emissor e recetor (constituídos no mínimo por dois *IP`S),* sendo que, após o envio da mensagem, a mesma fica armazenada na rede ou no equipamento terminal do destinatário até que o mesmo, passe-se a redundância, decida "abrir o envelope". Se é certo que, quando estabelecemos uma ligação telefónica com outra pessoa, a exteriorização da palavra falada, instantaneamente, encontrará correspondência, do outro lado, com a exteriorização de uma outra palavra falada, estabelecendo-se em tempo real uma comunicação *in loco,* não podemos admitir que, no caso do correio eletrónico, similar realidade aconteça, porque tecnicamente impossível. Conforme supra aludimos, a intencionalidade do emissor da mensagem de correio eletrónico é perpetuar uma mensagem, podendo, inclusivamente, suceder que a mesma não seja intencionada para

[158] De realçar que o legislador contemplou, já nesta altura, um catálogo de crimes bastante amplo, permitindo uma compressão do direito à intimidade da vida privada, sendo expectável que somente a criminalidade mais grave constasse do catálogo.

obter "retorno" por parte do destinatário, ou que não chegue sequer por si a ser lida. De resto, não podemos olvidar que o processamento da mensagem eletrónica, pressupondo a distância entre interlocutores, está dependente de terceiros, ou seja, dos chamados operadores de serviços de comunicações eletrónicas, sendo a estes serviços confiado o envio/receção do correio eletrónico. Ora, é precisamente o facto do serviço da "entrega" estar confiada a terceiros, que torna a comunicação eletrónica extremamente vulnerável e suscetível de profundas lesões, na medida em que é possível aos operadores de serviços de comunicações eletrónicas intrometer-se arbitrariamente na comunicação, retirando assim o seu domínio ao emissor.

Assim, em virtude da natureza do processo comunicacional e do seu desfasamento temporal dialético, não podemos consolidar que, na verdadeira aceção da palavra, exista no correio eletrónico uma conversação, ou um diálogo em tempo real[159], precisamente, porque no caso do correio eletrónico, contrariamente ao que ocorre nas conversações telefónicas (em que o conteúdo se "evapora" do mundo real), existe todo um conteúdo comunicacional que subsiste. Repare-se que, ainda que o *e-mail* comporte a possibilidade de, em anexo, conter um ficheiro de voz, o facto da mensagem revestir um carácter sonoro não a deve subsumir à possibilidade de ser intercetada segundo o regime das escutas telefónicas, pois que, ainda aqui, não se vai aceder, verdadeiramente, a uma conversação, mas tão só a uma mensagem em suporte vocal[160]. De tal modo, não é pelo facto do correio eletrónico comportar a possibilidade de transmissão em mensagens de voz que se coloca em causa a sua natureza. Antes pelo contrário, cremos que esta realidade foi contemplada pelo legislador, cabendo perfeitamente na noção de correio eletrónico disposta no art.º 2.º, n.º1, al. b), da Lei n.º 41/2004, de 18/08, só assim se alcançando a referência ao mencionado "*suporte de voz*". Assim, também deste prisma, por muito tentador que se revista subsumir o correio eletrónico ao regime das escutas, não concordamos que se possa reconduzir a interceção e o registo do correio eletrónico ao regime da interceção e registo das escutas telefónicas.

[159] TEIXEIRA, Carlos Adérito, *Escutas Telefónicas: a mudança de paradigma e os velhos e novos problemas* – Jornadas sobre a revisão do Código de Processo Penal, Revista CEJ, 1.º semestre, número 9 (Especial), 2008, p. 282.
[160] NEVES, Rita Castanheira, *As Ingerências nas Comunicações…,* p.178 e 179.

5.2.2. A Encruzilhada Conceptual do art.º 189.º do CPP

Por seu turno, encontra-se consagrado no art.º 189.º, n.º 1, segunda parte, do CPP, que o disposto nos art.ºs 187.º e 188.º é também aplicável às mensagens de correio eletrónico *"(…)mesmo que se encontrem guardadas em suporte digital, e à intercepção das comunicações entre presentes"*. Conforme já aduzido, esta contemplação normativa veio semear o pânico entre os operadores judiciários, sendo alvo de veemente crítica por parte da doutrina, atendendo à consagração expressa, por parte do legislador, da aplicabilidade do regime das escutas telefónicas em situações onde o correio eletrónico já foi recebido, lido e armazenado pelo seu destinatário, indiferenciando-o das mensagens de correio eletrónico ainda não abertas e, por tal motivo, não lidas.

Assim, quer se trate de correio eletrónico lido ou não lido, guardado ou não guardado, por parte do destinatário, inexplicavelmente, confundindo-se o que julgamos ser inconfundível, reservou-se o art.º 189.º, n.º 1, do CPP, como uma espécie de "cura" para todos os "males" que a investigação padecesse no que tange à obtenção da prova digital. Com o devido respeito, não podemos concordar com tal opção legislativa pois que, não respeitando os desequilíbrios existentes nos diferentes graus de tutela constitucional das comunicações eletrónicas, o legislador submeteu, por via desta cláusula de extensão e sob o mesmo teto, estados de comunicações que reclamam tratamento diferenciado.

Tendo por referência o trajeto da mensagem de correio eletrónico, a que aludimos no capítulo 3.3., podemos concluir que o correio eletrónico, sendo uma mensagem e podendo ter um suporte de texto, gráfico ou de voz, importa sempre, conforme já aduzido, a figura de um emissor e recetor. De resto, como ensina JOEL TIMÓTEO PEREIRA[161], uma mensagem de correio eletrónico, antes de chegar ao seu destino, passa sempre por diversos pontos, adicionando, em cada ponto que passa, o IP do servidor (isto é a identificação da máquina), podendo aferir-se, através dos cabeçalhos do *e-mail,* quais os servidores por onde a mensagem passou, inclusive, com identificação do ISP de origem. Sequencialmente, após chegar ao seu destino, a mensagem de correio eletrónico fica jacente num determinado terminal (exemplo do *Outlook*) ou alojada virtualmente no servidor (como acontece, por exemplo, nos *Webmails*). Ora, é precisamente sobre este

[161] PEREIRA, Joel Timóteo, *Compêndio Jurídico da Sociedade da Informação – Notas Práticas, Legislação e Jurisprudência*, Quid Juris, Sociedade Editora, Lisboa, Outubro 2004, p. 13.

estado de coisas, nomeadamente nas etapas do processo dinâmico de transmissão de envio/receção da mensagem de *e-mail*, que se tem questionado qual o momento em que se deve considerar cessada a comunicação e, com ela, a tutela constitucional do sigilo das comunicações eletrónicas.

Nesta matéria, no que ao correio eletrónico diz respeito, e ainda antes da reforma de 2007 ao CPP, pugnava PEDRO VERDELHO por um regime tripartido de acesso em investigação criminal. De tal forma, segundo o Autor, seriam as etapas do processo comunicativo da mensagem eletrónica que revelariam qual a aplicação do regime de obtenção de prova que lhe seria aplicável. Assim, aplicar-se-ia o regime das escutas telefónicas para a *"fase de transmissão do e-mail",* o regime da apreensão de correspondência para a fase em que *"o e-mail já chegou ao destino, mas ainda não foi lido pelo destinatário",* e o regime da apreensão de normais ficheiros escritos *"quando o e-mail já foi aberto e lido pelo destinatário*"[162]. O Autor alicerçava o seu pensamento no facto de não existirem *"normas específicas que regulamentem a obtenção e utilização, como meio de prova, das mensagens de correio eletrónico",* argumentando que seria o próprio art.º 179.º, n.º1, do CPP, que consagrava esta extensão de aplicação ao correio eletrónico na parte alusiva a *"qualquer outra correspondência"*[163]. De resto, não soçobravam dúvidas ao Autor que quando o *e-mail* chegasse ao seu destinatário, sendo efetivamente por si lido, a comunicação cessaria, passando a ser um ficheiro digital.

Não obstante concordarmos com PEDRO VERDELHO, na parte em que defende que as mensagens de correio eletrónico, ainda não abertas e lidas, merecem um tratamento especial por parte do legislador, não podemos seguir, no entanto, a sua linha de raciocínio no sentido de autonomizar uma fase intermediária do processo comunicativo, pois que, para além de não existir nenhuma razão para submeter a regimes distintos a fase da comunicação que circula entre pontos de rede de emissão e receção, daquela outra onde o *e-mail* ainda não foi aberto pelo destinatário, tal opção mergulharia a investigação num verdadeiro caos processual.

---

[162] VERDELHO, Pedro, *Apreensão do Correio Eletrónico em processo Penal,* Revista do Ministério Público, Lisboa, Ano 25, n.º 100, Out./Dez., 2004, p.153-164. Não obstante a reforma do CPP, em 2007, o Autor não alterou a sua posição. *Vide* VERDELHO, Pedro, A *Técnica no novo C.P.P.: Exames, Perícias e Prova Digital*, Revista do CEJ, Lisboa, 1. º Semestre, n. 9, 2008, p. 145-171.

A este propósito, reconhecendo apenas dois momentos na vida do correio eletrónico, e apoiando-se no entendimento do Tribunal Constitucional Federal Alemão (*Bundesverfassungsgericht),* de 22 de Agosto de 2006, consolidava COSTA ANDRADE que a comunicação "*Só existe enquanto dura o processo dinâmico de transmissão, isto é, até ao momento em que a comunicação entra na esfera de domínio do destinatário. Vale dizer, até ao momento em que ela é recebida e lida pelo destinatário e, neste sentido, termina o processo de telecomunicação à distância*"[164], sendo que, conforme alude o Autor, após o conhecimento do conteúdo pelo destinatário, já não se coloca em causa a tutela do sigilo de telecomunicações, precisamente, porque a comunicação já perdeu a "*especifica situação de perigo*" decorrente do domínio que o terceiro (empresa fornecedora do serviço de telecomunicações) detém sobre o conteúdo e os dados emergentes à comunicação, e que lhe permitiriam intrometer-se na comunicação retirando o controlo ao comunicador[165]. Nesta medida, como defende o Autor, *"depois de recebido, lido e guardado no computador do destinatário, um e-mail deixa de pertencer à área de tutela das telecomunicações passando a valer como um normal escrito. E, como tal, sujeito ao mesmo regime em que se encontra um qualquer ficheiro produzido pelo utilizador do computador e nele arquivado. Podendo, como tal, figurar como objecto idóneo da busca, em sentido tradicional. Busca que pode ser executada já sob a forma de apreensão do computador, já – preferencialmente, porque menos lesiva – sob a forma de cópia.*"[166]. Neste cômputo, CARLOS ADÉRITO TEIXEIRA parece ir um pouco mais além. Reconhece o Autor os dois momentos distintos no correio eletrónico – o da transmissão da comunicação e o seu armazenamento em ficheiro – distanciando-se, porém, da doutrina que alude à possibilidade de intercetar o correio eletrónico em tempo real, sendo apologista que o correio eletrónico só poderia ser acedido, para efeitos de investigação criminal, através de diligências de busca e apreensão, atendendo que, tecnicamente, seria impossível intercetar o correio eletrónico em tempo real[167].

---

[164] ANDRADE, Manuel da Costa, *Bruscamente no verão passado*..., p. 159.

[165] A este propósito, no próprio art.º 4.º, da Lei n.º 41/2004, de 18/08, devem as empresas que oferecem as redes e ou serviços de comunicações eletrónicas "*garantir a inviolabilidade das comunicações e respetivos dados de tráfego realizadas através de redes públicas de comunicações e de serviços de comunicações eletrónicas acessíveis ao público*".

[166] ANDRADE, Manuel da Costa, *Bruscamente no verão passado...,* p. 159.

[167] TEIXEIRA, Carlos Adérito, *Escutas Telefónicas: a mudança de paradigma*…, p. 281-291.

Ainda nesta matéria, e a propósito de uma análise crítica ao Acórdão do Segundo Senado do Tribunal Constitucional Federal Alemão, de 02 de Março de 2006[168], aduz VÂNIA COSTA RAMOS que, embora o *e-mail* perca a condição de comunicação no momento em que chega à esfera de domínio do destinatário, o conteúdo da mensagem eletrónica continua a ser constitucionalmente protegido, enquanto dados pessoais pertencentes à esfera privada[169]. De resto, prossegue a Autora, há *"uma perda de domínio do indivíduo sobre a sua esfera privada, perda essa que decorre, forçosamente, da utilização dos serviços e equipamentos técnicos de terceiros*", sendo que, por tal motivo, conforme sumariado pelo *BVferG,* "*a proteção do segredo das comunicações termina no momento em que a mensagem chega ao destinatário e o processo de transmissão se encontra concluído. Isto porque ao utilizador não assistem possibilidades técnicas para evitar, nem sequer para influenciar, a criação e a gravação de dados de ligação pelo transmissor durante a comunicação*"[170].

Assim, partindo o *BVerfG*[171] da consagração constitucional do segredo das telecomunicações, previsto no art.º 10.º da *GG*, firma o entendimento que só fará sentido falar na proteção especial do segredo das comunicações, enquanto os dados ainda não atingiram a esfera de domínio do recetor, considerando-se que o processo comunicativo termina quando os *"dados de ligação e de conteúdo" são "guardados na esfera do receptor",* deixando a comunicação de estar exposta aos *"riscos específicos"* da utilização dos serviços de terceiros, decidindo que os *"§§94 ss. e §§102 ss. StPO cumprem os requisitos das disposições constitucionais em relação à apreensão de suportes de dados e dos dados neles armazenados"*, quando o fim que legitima a compressão do direito à autodeterminação informacional é prosseguido de forma adequada, necessária e proporcional, compatibilizando-se tal direito com as normas gerais que regulam as buscas e apreensões dos dados armazenados.

---

[168] O acórdão coloca em confronto duas teses referentes ao âmbito e extensão da proteção constitucional das telecomunicações: A primeira, defende que a proteção da comunicação eletrónica se estende para além da transmissão da comunicação propriamente dita, abrangendo os dados eletrónicos dessa comunicação que se encontram na esfera jurídica do recetor; A segunda, defende que aquela proteção só se aplica até ao momento em que cessa o processo de comunicação – RAMOS, Vânia Costa, *Âmbito e Extensão do Segredo das Telecomunicações*, Revista do Ministério Público, n.º 11, Out./Dez. 2007, p. 147.

[169] RAMOS, Vânia Costa, *Âmbito e Extensão do Segredo*…, p. 149-159.

[170] RAMOS, Vânia Costa, *Âmbito e Extensão do Segredo*…, p. 143.

[171] Decisão do Segundo Senado do *BVerfG* de 12 de Abril de 2005 – *apud* RAMOS, Vânia Costa, *Âmbito e Extensão do Segredo*…, p. 141-159.

Fora do processo comunicativo, atendendo que a comunicação perde a característica da vulnerabilidade à interceção de terceiros, termina assim a tutela do sigilo das telecomunicações, pertencendo a mensagem eletrónica à esfera privada do destinatário, estando o seu conteúdo sob o seu estrito domínio, fazendo sentido falar-se, já não da tutela do sigilo das comunicações eletrónicas, mas sim da tutela constitucional decorrente da autodeterminação informacional, enquanto espaço de privacidade. Por tal motivo, no encalço da doutrina maioritária, pugna RITA CASTANHEIRA NEVES[172] que a mensagem de correio eletrónico que cumpriu, com sucesso, o seu circuito comunicacional, ao ter sido recebida e lida pelo destinatário, deve ter-se como "*um ficheiro, ao lado de outros que o utilizador do computador cria, altera, elimina, etc.*", beneficiando, porém, o conteúdo da mensagem de *"uma protecção legal, e até constitucional por recondução ao artigo 26.º da Constituição da República Portuguesa, bem como ao artigo 35.º da mesma lei fundamental, que protege os dados pessoais no contexto dos sistemas informáticos*". Estribando-se nos ensinamentos de COSTA ANDRADE, defende a Autora que, *"para se conseguir obter conhecimento dos suportes digitais, resultantes da transmissão de mensagens de correio electrónico já abertas e lidas, para valerem como prova num determinado processo penal, o que se tem que levar a cabo é já uma busca. E, claro, no caso de se tratar de uma busca presencial (e não online) se ao tomar conhecimento desses mesmos suportes, houver interesse e legitimidade para os mesmos constarem dos autos, o meio através do qual se efectivará a obtenção de prova é o registo ou cópia dos suportes digitais, sendo certo, pois, que a apreensão propriamente dita será já relativa aos suportes / objectos físicos que contêm os conteúdos gravados".*[173]

Nesta matéria, partindo da definição de correio eletrónico consagrada na al. h), do art.º 2.º, da Diretiva 2002/58/CE, e apoiando-se nos ensinamentos de ROMEO CASABONA[174], BENJAMIM SILVA RODRIGUES fala-nos da monitorização dos fluxos internacionais e comunicacionais, questionando a recondução do correio eletrónico ao regime das escutas telefónicas. De tal forma, assinalando o facto da Diretiva, para efeitos

[172] NEVES, Rita Castanheira, *As Ingerências nas Comunicações…,* p. 260 e 261.
[173] NEVES, Rita Castanheira, *As Ingerências nas Comunicações…,* p. 260.
[174] ROMEO CASABONA, Carlos María, *La protección penal de los mensajes de correo eletrónico…*, p. 129. Ainda sobre esta temática, seguindo a mesma linha de orientação de ROMEO CASABONA, veja-se também GARCÍA GONZALEZ, Javier, *Intervenciones de terceros en el correo eletrónico. Especial referencia al ámbito laboral y policial*, *apud* Carlos María Romeo Casabona (Coordenação), *El cibercrim, nuevos retos jurídico-penales, nuevas respuestas politicocriminales*, Editorial Comares, Granada, 2006, p. 300-301.

penais, ser demasiado ampla e restritiva (atendendo que se fica pelas mensagens enviadas através das redes de comunicações públicas), pelo Autor é realçado o facto de que, quando se procede ao envio de determinada mensagem de correio eletrónico, a mesma é enviada através de uma rede pública de comunicações eletrónicas, podendo encontrar-se armazenada em dois locais distintos: no servidor de *e-mail* ou no equipamento terminal do destinatário (quando este possua um programa de receção de correio eletrónico). Nesta sequência, realça o Autor, é inevitável concluir-se que o "armazenamento" se mantém até que o destinatário aceda ao servidor de *e-mail,* ou ao seu equipamento terminal, com vista à recolha da aludida comunicação eletrónica[175]. Por tal motivo, segundo o Autor, não será assim pelo simples facto de se encontrar "*pendente ou armazenada*", na rede ou no equipamento terminal do destinatário, que a comunicação eletrónica se comuta numa outra realidade, devendo-se, assim, entender que mantém o seu estatuto de comunicação eletrónica*[176]*. Na resposta à questão sobre o regime que deverá ser aplicável ao correio eletrónico, enquanto meio de prova, o Autor considera que o regime de extensão consagrado no art.º 189.º do CPP, acaba por desvirtuar o paradigma constitucional projetado para as escutas telefónicas, concluindo que tal preceito apenas se restringe às formas de comunicação oral, pelo facto de estar, teleologicamente, concebido para a captação da palavra falada. Assim, para o Autor, a melhor solução para a regulamentação das mensagens de correio eletrónico, que ainda constituíssem comunicação, encontrar-se-ia numa autonomização de regime, construído a partir do CPP, sob a epígrafe de *"Monitorização dos fluxos informacionais e comunicacionais*"[177], aí abrangendo as "*comunicações orais, escritas (imagéticas ou não) ou mistas*", consagrando-se, ao lado dos meios de obtenção de prova clássicos, as perícias informático – digitais, bem como os exames e buscas informático – digitais, distante das remissões para os regimes das escutas ou da correspondência. Não obstante a solução de regime proposto, advoga BENJAMIM SILVA RODRIGUES que as comunicações eletrónicas bem-sucedidas, isto é, aquelas

[175] O Autor alude ao facto do correio eletrónico deter, nas suas diversas opções, a possibilidade de obtenção de "*um comprovativo de receção da mensagem pelo equipamento terminal do destinatário*", bem como *"um comprovativo de (leitura) que a mensagem foi apresentada, a uma certa hora, de determinado dia, no monitor do computador do destinatário da mensagem*", permitindo saber quando é que o *e-mail* foi lido. Cfr. VEIGA, Armando e RODRIGUES, Benjamim Silva, *Escutas Telefónicas, Rumo à Monitorização dos Fluxos Informacionais e Comunicacionais Digitais*…, p. 374.

[176] RODRIGUES, Benjamim Silva, *Das Escutas telefónicas à Obtenção da Prova*..., p. 99-140. RODRIGUES, Benjamim Silva, *Da Prova Penal, Tomo II, Bruscamente*…, p. 347-349.

[177] RODRIGUES, Benjamim Silva, *Das Escutas Telefónicas – A Monitorização dos Fluxos Informacionais e Comunicacionais*…, p. 442.

comunicações eletrónicas em que o destinatário acedeu, recolheu e procedeu à leitura da mensagem eletrónica que lhe era destinada, já não nos coloca no âmbito das monitorizações das comunicações eletrónicas, mas tão só perante um documento que contém dados de caráter pessoal no contexto das redes e serviços de comunicações eletrónicas acessíveis ao público, devendo *"ter-se em linha de conta o disposto na Lei de Protecção da Privacidade no Sector das Comunicações Electrónicas – Lei n.º 41/2004, de 18 de Agosto e na Lei n.º 67/98 de 26 de Outubro – Lei de Protecção de Dados Pessoais*"[178].

Não obstante a corrente doutrinária que defende que a comunicação apenas cessa no momento em que é conhecida pelo seu destinatário, ter vindo a consolidar-se com o calcorrear dos tempos, a verdade é que tal entendimento ainda não é unânime, resistindo-lhe alguma doutrina que pugna pela indiferença do destinatário ter aberto ou lido a mensagem, considerando que, a partir do momento em que a comunicação chega ao terminal do destinatário, ou ao servidor do *e-mail*, a comunicação eletrónica perde o seu estatuto de comunicação. Posicionando-se neste último entendimento, assim vêm advogando ROMEO CASABONA[179], ROGÉRIO BRAVO[180] e ARMANDO RAMOS[181], invocando, sobretudo, a volatilidade a que o processo comunicativo está sujeito, designadamente, o facto de a nível informático existir um conjunto de funcionalidades, em praticamente todos os programas de correio eletrónico, que permitem marcar como não lida uma mensagem de correio eletrónico já aberta e lida.

---

[178] RODRIGUES, Benjamim Silva, *Das Escutas Telefónicas – A Monitorização dos Fluxos Informacionais e Comunicacionais*..., p. 442.

[179] Referindo-se ao art.º 197.º do CP Espanhol, sustenta o Autor que "*El CP de 1995 introdujo de forma expresa como delito el apoderamiento de los mensajes de correo electrónico, así como la interceptación de las telecomunicaciones de outra persona. Sin perjuicio de las precisiones que se introducirán más abajo, puede adelantarse ya que en el primer caso se trata de conductas que pueden afectar al mensaje de correo electrónico o a cualquier otra comunicación a través de la red asimilable que se encuentra en una situación estática, esto es, guardados en un fichero una vez recibido, pendiente de recepción y guardado en el sistema del prestador de servicios o guardado en el terminal de remitente cuando se halla pendiente de remisión. Mientras que las segundas - las telecomunicaciones - se refieren a conductas que afectan a cualquier mensaje u otra forma de comunicación telemática semejante mientras se encuentran en el proceso de transmisión (y, en ocasiones, de creación), es decir, en "movimiento"*. ROMEO CASABONA, Carlos Maria, *La protección de los mensages de correo* electrónico..., p. 123-149.

[180] O Autor defende que as mensagens de correio eletrónico já recebidas, ainda que não lidas, encontrando-se alojadas num determinado sistema informático, mais não são do que meros dados informáticos localmente armazenados, à semelhança, de resto, de qualquer documento provindo de um processador de texto ou programa para apresentação de *slide*. BRAVO, Rogério, *Da não equiparação do correio - eletrónico ao conceito tradicional de correspondência por carta*, Polícia e Justiça, Revista do Instituto Superior de Polícia Judiciária e Ciências Criminais, III Série, n.º 7, Coimbra Editora, Janeiro - Junho 2006, p. 209.

[181] RAMOS, Armando Dias, *A Prova Digital em Processo Penal*, 1.º ed.,..., p. 51.

Embora se alcance a nível prático onde pretendem os Autores chegar, julgamos, porém, existir alguma falácia na esgrima de tal argumento, pois que, para além de desconsiderarem o momento fulcral do efetivo conhecimento da mensagem por parte do destinatário (atingindo a comunicação a sua perfeição), desconsideram em absoluto a posição do destinatário no processo de transmissão entre interlocutores, acabando por desvirtuar as vicissitudes que pode sofrer o processo comunicacional e deformar a delimitação da tutela constitucional da inviolabilidade do sigilo das comunicações. A este propósito, pense-se no exemplo de um *e-mail* que nunca foi aberto pelo seu destinatário, ou mesmo o caso de alguém, sem autorização, abrir um *e-mail* na *mail box* do destinatário, procedendo à sua eliminação, sem que o destinatário chegue a ter conhecimento da sua existência. Pegando em tais exemplos, fará sentido deslocar o momento da cessação da comunicação, desconsiderando o conhecimento dos dados de conteúdo pelo destinatário? Manifestamente, julgamos que não. Por ora, ater-nos-emos por aqui, teremos oportunidade de desenvolver em pontos posteriores.

Por tal motivo, de tudo quanto ficou dito, acompanhamos de perto a doutrina maioritária, segundo a qual a mensagem de correio eletrónico apenas altera o seu estatuto, isto é, muda o seu estado e deixa de ser comunicação, no preciso momento em que o *e-mail* é aberto e lido pelo seu destinatário, cumprindo, assim, *tout court*, a sua função de "informação", extinguindo-se aqui o circuito comunicacional. Neste ponto, em que o *e-mail* acaba por se "metamorfosear", a mensagem eletrónica já não é comunicação, deixando de ser possível a sua interceção. Já o foi, é um facto. Agora, fará todo o sentido dizer-se que o que existe é apenas um suporte digital que se encontra armazenado/guardado/alojado na caixa de correio eletrónico. Se assim é, a nível do rigor do processo penal, nomeadamente, para que não entrem em conflito conceitos, com os inerentes riscos para a validação da prova, somos forçados a procurar distinto meio de obtenção de prova adequado à sua recolha e preservação, distante do regime das escutas, concluindo-se assim, *inter alia*, pelo reconhecimento que, na falta de outros meios apenas consagrados mais tarde pela Lei do Cibercrime, sempre seria a partir das disposições legais previstas nos capítulos II ("Das Revistas e buscas") e III ("Das apreensões), do Título III ("Dos meios de obtenção de prova") do CPP, que se haveria de recorrer para disciplinar a recolha das mensagens eletrónicas abertas, lidas e armazenadas pelo destinatário.

6. A Lei n.º 32/2008, de 17 de Julho

Paralelamente, agravando as enormes dificuldades interpretativas geradas pela alteração ao CPP de 2007, transpondo para a ordem jurídica portuguesa a Diretiva n.º 2006/24/CE[182], de 15/03, do Parlamento Europeu e do Conselho, é publicada a Lei n.º 32/2008, de 17/07, uma Lei extravagante com vista à regulação, nos crimes graves, da conservação e transmissão dos dados de tráfego e localização, assim como os dados relevantes para a identificação do assinante ou do utilizador.

Conforme expusemos, os operadores de comunicações guardam informação respeitante à identificação dos seus clientes (ex. nome, morada - tradicionalmente conhecidos como dados de base), assim como informação respeitante às comunicações por si efetuadas – os chamados dados de tráfego. Por tal motivo, desde logo, a cedência de tais dados revela-se determinante para: (I) encontrar e identificar a fonte de uma comunicação; (II) encontrar e identificar o destino de uma comunicação; (III) identificar a data, hora e duração de uma comunicação; (IV) identificar o tipo de comunicação e (V) identificar o equipamento da comunicação, tanto no que respeita a comunicações telefónicas nas redes fixas e móveis, como nas redes da Internet. Quanto aos dados de conteúdo, atendendo que as operadoras de comunicações estão proibidas de guardar este tipo de dados, estão fora da alçada desta Lei[183].

Assim, a Lei n.º 32/2008, de 17/7, não tendo operado à revogação expressa das disposições do CPP, teve o seu âmbito de aplicação delimitado a um catálogo reduzido de crimes, nomeadamente, os consagrados no art.º 2.º, n.º1, al. g), clarificando-se que, para efeitos da presente Lei, apenas seriam considerados crimes graves os "*crimes de*

---

[182] A Diretiva n.º 2006/24/CE veio alterar a Diretiva n.º 2002/58/CE, de 12/07. A Diretiva n.º 2006/24/CE manifesta uma grande preocupação com a segurança nacional, a preservação da ordem pública e a prevenção das infrações criminais, assegurando que determinadas categorias de dados pessoais dos assinantes, ou utilizadores de redes ou serviços de comunicações eletrónicas, possam ser recolhidos e conservados pelos operadores de redes de comunicações ou prestadores de serviços de comunicações electrónicas. Quanto à necessidade da sua célere transposição já se tinham pronunciado JOSÉ MOURAZ LOPES e CARLOS ANTÃO CABREIRO. *Vide* LOPES, José Mouraz e CABREIRO, Carlos Antão, *A Emergência da Prova Digital na Investigação da Criminalidade Informática, in* Sub Judice — Justiça e Sociedade, n.º 35, Coimbra, Almedina, 2006.

[183] Por força do n.º 2, do art.º 1.º, da Lei nº 32/2008, de 17/07, "*a conservação de dados que revelem o conteúdo das comunicações é proibida*". Também no n.º 2, do art.º 4.º, da Lei n.º 41/2004, de 18/08, é proibido, fora do contexto processual penal, a escuta, interceção e armazenamento de comunicações. Tal proibição decorria já dos arts.º 32.º, n.º 8, e 34.º, n.º 4, da CRP.

terrorismo, criminalidade violenta, criminalidade altamente organizada, sequestro, rapto e tomada de reféns, crimes contra a identidade cultural e integridade pessoal, contra a segurança do Estado, falsificação de moeda ou títulos equiparados a moeda e crimes abrangidos por convenção sobre segurança da navegação aérea ou marítima". De resto, sob forma cumulativa, a par do requisito do específico tipo de ilícito, a Lei exige um despacho fundamentado do JIC para a cedência de tais dados por parte dos operadores de comunicações, e apenas nas situações em que houver razões para crer que tais dados são indispensáveis para a descoberta da verdade, ou que representam a única prova existente para provar que determinada pessoa praticou o crime contemplado no seu catálogo, assegurando-se o respeito pelos princípios da adequação, necessidade e proporcionalidade, conforme disposto no art.º 9.º, n.º 2, deste diploma. Para além destas exigências, no art.º 9.º, n.º 3, da Lei n.º 32/2008, de 17/07, acabaria por se delimitar que apenas podem ser transmitidos dados relativos: do suspeito/arguido; da pessoa suspeita de receber ou transmitir as mensagens provenientes, ou destinadas, aquele; da própria vítima, a seu pedido e quando o seja consentido.

Assim, podemos concluir que ao manterem-se inalterados, pela Lei 32/2008, os requisitos de acesso e obtenção aos dados informáticos, face às normas gerais no CPP, o legislador tornou este regime especial num regime desnecessário, sem motivo aparente para se denominar como autónomo. No fundo, a duplicação de regimes, para além de avolumar a desordem existente, veio adensar o quadro de problemas que emerge a nível da transmissão de dados, facilmente solucionados, na esteira de JOÃO CONDE CORREIA, se, ao invés de se ter consagrado normas gerais no CPP e normas especiais na Lei 32/2008, o legislador tivesse optado por manter a centralidade normativa do CPP, nomeadamente, disciplinando na Lei geral o acesso dos dados de tráfego, localização, bem como os dados relevantes à identificação do assinante/utilizador, reservando os aspetos técnicos da sua conservação, a título preventivo, para a legislação extravagante, parecendo claro que *"uma coisa é a conservação preventiva de dados; outra bem diferente, a sua aquisição e valoração processual penal, desencadeada pela suspeita da prática do crime"*.[184]

De resto, harmonizar a Lei 32/2008, de 17/7, com o CPP, bem como propriamente com outras Leis extravagantes vigentes no nosso ordenamento jurídico, torna-se, hoje, de

[184] CORREIA, João Conde, *Prova Digital: as leis que temos e a lei que devíamos ter*, Revista do Ministério Público, ISSN 0870-6107, Ano 35, n.º 139, 2014, p. 33 e 34.

aparente e difícil articulação, em virtude da entrada em vigor da Lei do Cibercrime, assim como a recente prolação do Acórdão do Tribunal de Justiça da União Europeia, de 8 de Abril de 2014[185], ao ter declarado a invalidade da Diretiva 2006/24/CE, ali se exarando o entendimento que esta Diretiva violaria os direitos fundamentais dos cidadãos, atendendo à sua permissibilidade na conservação de dados que possibilitam a extração de informações precisas sobre a vida privada dos seus titulares, designadamente, os seus hábitos diários, os locais frequentados, as atividades desenvolvidas e as relações por si estabelecidas. Assim, embora o TJUE reconheça a superior importância que o combate à criminalidade grave (em particular nos casos do crime organizado e terrorismo), reveste para a garantia da segurança pública, firmou o entendimento que esta Diretiva não justifica a compressão dos direitos fundamentais do cidadão. Outros argumentos que motivaram a declaração de invalidade da Diretiva, por parte do TJUE, prendem-se com a ausência de critérios precisos para a definição dos prazos aplicáveis à conservação dos dados, ou mesmo de adaptação do lapso temporal às categorias de dados existentes, bem como a inexistência de mecanismos que acautelem eventuais situações de abuso da informação recolhida, pronunciando-se o TJUE pela violação dos direitos à reserva da intimidade da vida privada, da proteção de dados pessoais e do princípio da proporcionalidade[186], que determinam a invalidade da Diretiva.

Apesar desta declaração não revestir força obrigatória geral, o legislador português foi cauteloso na transposição de tal Diretiva, prevendo, na Lei n.º 32/2008

---

[185] Tal acórdão surge na sequência dos reenvios prejudiciais provenientes do Supremo Tribunal Irlandês (*High Court of Ireland*) e do Tribunal Constitucional Austríaco (*Verfassungsgerichtshof*), no âmbito dos processos n.ºs C-293/12 e C-594/12, respetivamente. O pedido apresentado pela *High Court* é relativo a um litígio que opõe a *Digital Rights Ireland Ltd.* ao *Minister for Communications, Marine and Natural Resources*, ao *Minister for Justice*, *Equality and Law Reform*, ao *Commissioner of the Garda Síochána*, à Irlanda e ao *Attorney General,* tendo por objeto a legalidade de medidas legislativas e administrativas nacionais respeitantes à conservação de dados relativos a comunicações eletrónicas. O pedido apresentado pelo *Verfassungsgerichtshof* é relativo a recursos em matéria constitucional interpostos perante este órgão jurisdicional respetivamente pelo *Kärntner Landesregierung* (Governo do Land de Caríntia), bem como por M. Seitlinger, C. Tschohl e 11 128 outros recorrentes, acerca da compatibilidade da lei que transpõe a Diretiva 2006/24 para o direito interno austríaco com a lei constitucional federal (*Bundes - Verfassungsgesetz*). Pelo facto da decisão do TJUE ter resultado de questões prejudiciais (artigo 267.º do TFUE), colocadas pelo Supremo Tribunal Irlandês e pelo Tribunal Constitucional Austríaco, a mesma não implica que a Diretiva 2006/24 CE não produza efeitos na ordem jurídica, já que, para tanto, se exigiria que a decisão do Tribunal tivesse resultado de um recurso de anulação (artigo 263.º do TFUE). Isto é, a decisão do TJUE não se traduziu numa qualquer declaração com força obrigatória geral – mantendo-se assim vigente a Diretiva 2006/24/CE.

[186] Para tanto, fundamentou o TJUE a sua decisão com base nas normas contidas nos artigos 7.º, 8.º e 52.º, n.º 1, da Carta dos Direitos Fundamentais da União Europeia.

requisitos rigorosos de utilização dos dados preservados, com respeito pelos princípios constitucionais, aplicando-se a Lei somente em crimes graves, não deixando de se exigir o despacho fundamentado do JIC. Assim, a Lei mantém-se em vigor devido ao catálogo de crimes e à previsão de prazos de conservação de dados nela dispostos, devendo, no entanto, ter-se sempre presente o princípio da proporcionalidade na medida aplicada. Se os dados não forem conservados pelo período de um ano[187], ou não forem alcançados em tempo útil, não se criará prova ditando o insucesso da investigação. Doutro passo, conforme advertem DAVID SILVA RAMALHO e JOSÉ DUARTE COIMBRA[188], nada impede que, na base das razões supra vertidas, e à semelhança do que tem acontecido noutros ordenamentos jurídicos[189], venha o Tribunal Constitucional, desde que solicitado para o efeito, a pronunciar-se sobre a inconstitucionalidade de algumas das disposições da Lei n.º 32/2008, de 17/07.

[187] O art.º 6.º, da Lei 32/2008, de 17/07, impõe aos fornecedores de serviços de comunicações eletrónicas o dever de "*conservar os dados previstos no mesmo artigo pelo período de um ano a contar da data da conclusão da comunicação.*". Poder-se-ia questionar qual o prazo aplicável para efeitos de investigação criminal. Porém, da sistematização do art.º 12.º, n.º 5, da LC, e do art.º 6.º, da Lei 32/2008, de 17/07, não parecem restar dúvidas que o prazo máximo de acesso aos dados no âmbito de uma investigação criminal, relativa a crimes em que seja necessário proceder à recolha de prova em suporte eletrónico, é o prazo de um ano. Posição reforçada, de resto, pelo Acórdão do TRC, de 26.02.2014, no processo n.º 559/12.0GBOBR-A.C1. Coloca-se, ainda, a questão de saber se estamos perante um prazo cumulável ou não. A este propósito, BENJAMIM SILVA RODRIGUES entende que não, considerando que *"haverá que atentar ao prazo absoluto de conservação dos dados gerados e tratados no âmbito das comunicações electrónicas, disposto no artigo 6.°, da Lei n.º 32/2008: um ano. (…) a renovação da medida, nos termos do artigo 12.º, n.º 5, possa ocorrer, (…) por períodos de três meses, mas até um máximo inultrapassável de 1 ano. Portanto: teoricamente, a medida pode ser renovada por três vezes, por períodos máximos parcelares de 3meses (1 x 3 meses + 3 x 3 meses = 4 x 3 meses = 12 meses = 1 ano*)". RODRIGUES, Benjamim Silva, *Da Prova Penal - Tomo II, Métodos Ocultos de Investigação Criminal*, Rei dos Livros, 2010, p. 443. Acórdão disponível no endereço online http://www.dgsi.pt/jtrc.nsf/c3fb530030ea1c61802568d9005cd5bb /0e255b331c5eaecd8 0257c91005ae8bf?OpenDocument [acedido em 23 de Fevereiro de 2016].

[188] RAMALHO, David Silva e COIMBRA, José Duarte, *A Declaração de Invalidade da Diretiva 2006/24/CE: Presente e futuro da regulação sobre a conservação de dados por parte de fornecedores de serviços de comunicações eletrónicas*, Abril, 2014. Disponível *online* no endereço http://www.servulo.com/xms/files/publicacoes/Updates_2014/Update_TI_DSR_JDC_A_declaracao_de_invalidade_da_diretiva_2006_24_CE_10_04_2014.pdf. [acedido em 3 de Março de 2017].

[189] Cfr. Tribunal Constitucional da Roménia (Decisão n.º 1258, de 8 de outubro de 2009); Tribunal Constitucional da Alemanha (Sentença n.º 10/2010, de 2 de março); Tribunal Constitucional da República Checa (Sentença Pl. ÚS 24/10, de 31 de março de 2011).

7. A Lei 109/2009, de 15 de Setembro – A Lei do Cibercrime

Em 15 de Setembro de 2009, viria a ser publicada a Lei 109/2009, de 15/09 (Lei do Cibercrime), honrando os compromissos internacionais assumidos pelo Estado Português, transpondo para a ordem jurídica interna a Decisão – Quadro n.º 2005/222/JAI[190], de 24/02, do Conselho da União Europeia, relativa a ataques contra sistemas de informação (substituída pela Diretiva n.º 2013/40/UE[191], de 12/08, do Parlamento Europeu e do Conselho), adaptando o direito interno à Convenção sobre o Cibercrime do Conselho da Europa, adotada em Budapeste a 23 de Novembro de 2001[192].

---

[190] A Decisão-Quadro entrou em vigor a 16 de Março de 2005, tendo os Estados Membros adotado as medidas necessárias para o seu cumprimento até 16 de Março de 2007. Conforme consignado em pontos 1 e 5, a Decisão - Quadro teve como objetivo "*reforçar a cooperação entre as autoridades judiciárias e outras autoridades competentes (…) mediante uma aproximação das suas disposições de direito penal em matéria dos ataques contra os sistemas de informação*", atendendo que "*a natureza transnacional e sem fronteiras dos modernos sistemas de informação implica que os ataques contra esses sistemas têm frequentemente uma dimensão transfronteiriça, evidenciando assim a necessidade urgente de prosseguir a harmonização das legislações penais neste domínio.*". Disponível *online* no endereço http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32005F0222 [acedido em 3 de Fevereiro de 2017].

[191] Conforme resulta da exposição de motivos, a Diretiva 2013/40/EU tem como objetivos *"(…) aproximar o direito penal dos Estados-Membros no domínio dos ataques contra os sistemas de informação, estabelecendo regras mínimas relativas à definição de infrações penais e as sanções aplicáveis, e melhorar a cooperação entre as autoridades competentes, nomeadamente a polícia e outros serviços especializados dos Estados-Membros responsáveis pela aplicação da lei, bem como as agências e organismos especializados competentes da União, tais como a Eurojust, a Europol e o seu Centro Europeu de Cibercriminalidade e a Agência Europeia para a Segurança das Redes e da Informação (ENISA)."* Disponível *online* no endereço http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32013L0040 [acedido em 27 de Fevereiro de 2017].

[192] Legatária da Recomendação n.º R (89) 9, a Convenção foi adotada pelo Comité dos Ministros do Conselho da Europa, em 8 de Novembro de 2001, tendo sido assinada em Budapeste, a 23 de Novembro de 2001. A Convenção viria a ser complementada, em 28 de Janeiro de 2003, pelo Protocolo adicional relativo à incriminação de atos de natureza racista e xenófobos, cometidos através de sistemas informáticos. Fundamentalmente, visou a Convenção "*proteger a sociedade do cibercrime, inter alia, através da adopção de legislação adequada e da melhoria da cooperação internacional", de modo a "tornar mais eficazes as investigações e os processos penais respeitantes às infracções penais relacionados com sistemas e dados informáticos, bem como permitir a recolha de prova, em formato electrónico*". Com tal finalidade, a Convenção estimulou os Estados signatários a tomarem medidas de modo a adequarem o direito penal interno, substantivo e adjetivo, às especificidades dos crimes informáticos, tendo como objetivo a harmonização de legislações, incluindo, instrumentos processuais e de produção de prova adequados e simplificar a cooperação internacional, de modo a facilitar e agilizar a investigação, a recolha de prova e a perseguição. Foi assinada, até à data, por 42 Estados, entre os quais 4 Estados não membros do Conselho da Europa (África do Sul, Canada, EUA e Japão). Destaque, ainda, para o facto da Convenção recomendar à adoção de instrumentos processuais, tais como: "*a conservação expedita dos dados informáticos armazenados e a divulgação parcial de dados de tráfego* (arts. 16.º e 17.º)*, a injunção para divulgação de dados que estejam na posse de alguém* (art.º 18.º)*, a busca e apreensão de dados informáticos armazenados* (art.º 19.º)*, a recolha de dados em tempo real de dados informáticos* (art.º 20.º*) e a intercepção de dados relativos ao conteúdo* (art.º 21.º). Debruça-se, ainda, na formulação de princípios gerais, relativos à tão desejada rápida e eficaz cooperação internacional (arts. 23.º e ss.*),* na qual se insere a Rede 24/7 (art.º 35.º) e sobre a assistência mútua (29.º e 30.º). Pese embora Portugal ter subscrito a Convenção em 2001, apenas em 2009 procedeu à sua ratificação por Resolução da Assembleia da República nº 88/2009, e pelo Decreto do

Estamos perante um dos diplomas mais importantes e aguardados no ordenamento jurídico português no que a cibercriminalidade diz respeito, gerando-se a expetativa que viesse expurgar algumas vicissitudes que, até então, eram sobejamente conhecidas na regulação da prova digital a nível do processo penal, designadamente, ao que nos interessa, da prova relacionada com o correio eletrónico.

Com efeito, a LC trouxe consigo um conjunto de disposições penais materiais, processuais e de cooperação internacional, assente numa estrutura tripartida, tratando-se de uma Lei reformista, inovadora e audaz, dando, pela primeira vez, extrema relevância ao campo processual na obtenção da prova digital, contemplando um conjunto de disposições processuais aplicáveis aos crimes informáticos nela previstos, aos crimes cometidos por meio de um sistema informático, e aos crimes em que seja necessário proceder à recolha de prova em suporte eletrónico (art.º 11.º da LC), assumindo, conforme JOÃO CONDE CORREIA, *"uma inquestionável vocação transversal a todo o sistema processual penal",* podendo dizer-se que, em matéria de prova digital, este diploma constitui agora a sua *"pedra angular"*[193], por via da cláusula de extensão consagrada no seu art.º 11.º, potencialmente dirigida a todos os crimes do universo informático, como convergem PEDRO VENÂNCIO, PEDRO VERDELHO e PAULO DÁ MESQUITA[194].

Por tal motivo, já se antevê, será redutor olhar para a LC como uma nova lei que, na sua substância, apenas se confina à mera revogação da velha e deficitária Lei da Criminalidade Informática de 1991, pois que, logo por aqui, a LC avoca uma diversificada extensão, adaptando-se às novas exigências de condutas desviantes, nomeadamente, alterando tipos legais de crimes, consagrando rejuvenescidas disposições incriminatórias, introduzindo, inclusive, no seu art.º 2.º, conforme Exposição de Motivos da proposta de Lei n.º289/X, que aprovou a LC, "*modernas*" definições não existentes em 1991, tais como "*fornecedor de serviço*" e de "*dados de tráfego*", alterando o conceito de *"sistema informático",* que passa *"a ser mais abrangente, incluindo-se nele, por exemplo, dispositivos como os telemóveis*", suprimindo a noção de *"rede informática por deixar de*

Presidente da República nº 91/2009, ambos publicados a 15 de Setembro. Disponível *online* no endereço http://www.dgpj.mj.pt/sections/relacoes-internacionais/copy_of_anexos/convencao-sobre-o/ [acedido em 1 de Março de 2017].

[193] CORREIA, João Conde, *Prova Digital: as leis que temos e a lei que devíamos ter…*, p. 34.

[194] *Vide* VENÂNCIO, Pedro Dias, *Lei do Cibercrime – Anotada e Comentada…*, p. 90 a 91; VERDELHO, Pedro, *A nova Lei do Cibercrime, in Scientia Ivridica,* Revista de Direito Comparado Português e Brasileiro, Tomo LVIII, N.º 320, Out. – Dez. de 2009, ISSN 0870-8185, p. 733 e 734; MESQUITA, Paulo Dá, *Processo Penal, Prova e Sistema Judiciário…*, p. 108-110.

fazer sentido" e substituindo o "*limitado e hoje em dia insuficiente"* conceito de *"programa informático*", pelo de "*dados informáticos"*.

De tal modo, atento e preocupado com o forte avanço tecnológico e vulnerabilidades dos sistemas informáticos, tratou o legislador de adaptar os ilícitos tipificados na LC à evoluída produção e difusão de vírus e outros programas maliciosos, bem como à modificação e destruição de programas ou outros dados informáticos, assim como a perturbação destes. Por seu turno, com a Lei 109/2009, os comportamentos que instiguem ou auxiliem qualquer crime nela previsto, passam também a ser criminalizados, a par da introdução ilegítima em sistema informático alheio, da reprodução ou divulgação de programas protegidos por lei, da falsificação de dados com o intuito de provocar dissimulações nas relações jurídicas, produzindo documentos ou dados falsos (por exemplo cartões de crédito). Assim, no âmbito do direito penal material, é importante assinalar que se encontram consagrados na LC crimes informáticos em sentido estrito, como "*a falsidade informática*" (art.º 3.º), "*o dano relativo a programas ou outros dados informáticos*" (art.º 4.º), "*a sabotagem informática*" (art.º 5.º), "*o acesso ilegítimo* (art.º 6.º), "*a intercepção ilegítima*" (art.º 7.º) e a "*reprodução ilegítima de programa protegido*" (art.º 8.º), salientando-se, contudo, que não constam na LC algumas tipificações previstas na Convenção, atendendo ao facto de alguns tipos de crimes já se encontrarem previamente dispostos no CP, como é o caso da "*burla informática e nas comunicações*" (art.º 221.º), do "*abuso de cartão de garantia ou de crédito*" (art.º 225.º), da "*devassa por meio de informática*" (art.º 193.º), da "*violação de correspondência ou de telecomunicações* (art.º 194.º), da "*pornografia de menores* (art.º 176.º) e da "*discriminação racial, religiosa ou sexual*" (n.º 2, do art.º 240.º), sendo que, outros ilícitos, se reconduzem a outras tipificações já existentes em diversos diplomas legais no nosso ordenamento jurídico[195].

Doutro passo, conforme deixa o legislador expressamente vertido na Exposição de Motivos da proposta de Lei n.º289/X, justificar-se-ia criar um diploma onde, para além da tipificação de crimes informáticos[196], se achasse regulada a obtenção de dados de tráfego e

[195] Como é o caso do crime de contrafação e usurpação, previsto no art.º 199.º do Código do Direito de Autor e dos Direitos Conexos, e dos crimes previstos nos art.ºs 43.º a 47.º, da Lei da Proteção Dados Pessoais, relativos à proteção de dados pessoais.

[196] A este propósito, destaca RENATO MILITÃO que *"a Lei nº 109/2009 e os diplomas conexos tiveram sobretudo em vista responder aos apelos dos que reivindicavam a densificação, facilitação, agilização, enfim, o eficientismo dessas medidas, integrando-se na linha securitarista que caracteriza o processo penal neoliberal."* Cfr. MILITÃO, Renato Lopes, *A propósito da prova digital no processo penal,* Revista da Ordem dos Advogados – ROA, Ano 72, n.º 1, 2012, p. 281.

a realização de interceção de comunicações eletrónicas, na investigação de crimes não previstos no artigo 187.º do CPP, ali se reconhecendo que *"a recente revisão do Código de Processo Penal optou pela limitação, em abstracto, da possibilidade de realização de intercepções de comunicações telefónicas e electrónicas, não tendo incluído normas especiais para a área da cibercriminalidade. Assim, não está prevista a obtenção de dados de tráfego nem a realização de intercepção de comunicações electrónicas na investigação de crimes não previstos no artigo 187.º do Código de Processo Penal. Entre eles, encontram-se crimes previstos na Lei n.º 109/91, de 17 de Agosto, bem como crimes contra a propriedade intelectual cometidos por via de redes informáticas",* deixando-se claro que a realização de interceções de comunicações eletrónicas e, sobretudo, a obtenção de dados de tráfego, *"são ferramentas processuais essenciais em processo-crime em que se investiguem crimes cometidos por via das redes de comunicações, tendo essa preocupação ficado espelhada no diploma que obriga os operadores de comunicações a guardarem os dados de tráfego dos seus clientes, tendo em vista a sua eventual necessidade em investigação criminal – Lei n.º 32/2008, de 17 de Julho, que regula a conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas"*. De resto, na aludida Exposição de Motivos, o legislador foi taxativo ao ponto de firmar a extrema importância em *"superar o actual regime, de modo a fornecer ao sistema processual penal normas que permitam a obtenção de dados de tráfego e a realização de intercepções de comunicações em investigações de crimes praticados no ambiente virtual",* só assim se percecionando a objetiva e sagaz referência que *"é o que se pretende fazer por via da lei que agora se propõe"*[197].

De tal forma, a LC foi relevante para preencher uma lacuna existente no ordenamento processual penal português, enriquecendo-o com novas disposições quanto à obtenção de dados de tráfego e realização de interceções nas comunicações eletrónicas, introduzindo, e, sobretudo, ampliando diversos conceitos jurídico-informáticos, consagrando-se um conjunto de mecanismos processuais relativos à obtenção da prova digital de caráter geral:

[197] A Exposição de Motivos da proposta de Lei n.º289/X encontra-se disponível *online* no endereço http://app.parlamento.pt/webutils/docs/doc.pdf?path=6148523063446f764c3246795a5868774d546f334e7a67774c336470626d6c7561574e7059585270646d467a4c31677664475634644739 7a4c334277624449344f5331594c6d527659773d3d&fich=ppl289-X.doc&Inline=true [acedido em 4 de Março de 2017].

1. Preservação expedita de dados (art.º 12.º);
2. Revelação expedita de dados (art.º 13.º);
3. Injunção para apresentação ou acesso a dados (art.º 14.º);
4. Pesquisa informática (art.º 15.º);
5. Apreensão de dados informáticos (art.º 16.º);
6. Apreensão de correio eletrónico e registos de comunicações de natureza semelhante (art.º 17.º);

E meios de obtenção de prova digital restringidos a um conjunto determinado de crimes:

7. Interceção de comunicações (art.º 18.º); e
8. Ações encobertas (art.º 19.º).

Com a criação da LC, a prova digital encontra-se, no nosso ordenamento jurídico, essencialmente, regulada em três diplomas legais: o CPP, a Lei n.º 32/2008, de 17/07, e a Lei 109/2009, de 15/09. Se não restam dúvidas que, de facto, corroborando-se PEDRO VENÂNCIO, a entrada em vigor da LC "*impunha-se não só como um imperativo de direito internacional, face à ratificação da Convenção sobre Cibercrime, mas, acima de tudo, como uma inevitabilidade civilizacional*"[198], a verdade é que, com tal solução normativa, o legislador, distanciando-se dos caminhos que a doutrina e a jurisprudência apontavam, no sentido de optar por leis simples e claras da qual resultasse uma uniformização e integração das normas das leis extravagantes num capítulo autónomo do CPP[199], inserido no Título III ("Meios de Obtenção e Prova"), do respetivo Livro II ("Da Prova"), acabou por enveredar pela via do complexo, em que as camadas das leis ora

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

[199] No ordenamento jurídico Espanhol a prova eletrónica digital encontra-se regulada nos artigos 579.º a 588.º, da *Ley de Enjuiciamiento Criminal*, tendo a lei orgânica 13/2015, de 5 de outubro, modificado a própria sistematização da *LECrim*, adaptando a investigação criminal à salvaguarda e a garantia do segredo das comunicações, como garantia constitucional prevista no art.º 18.º da Constituição, em resposta às críticas da doutrina e jurisprudência relativamente à falta de densidade reguladora do então art. 579.º da LECrim. O mesmo sucede no ordenamento jurídico Italiano, consagrando-se, no *Codice di Procedura Penale,* normas para à apreensão de correspondência e dados informáticos (arts. 253.º a 265.º) e disposições relativas à "*Intercettazioni di conversazioni o comunicazioni*" (art.ºs 266.º a 271.º), sob apertados requisitos da lei em obediência ao art. 15.º da Constituição Italiana. Também no ordenamento jurídico Alemão, atribuindo-se particular destaque ao sigilo das comunicações, consagrado no § 10.º, n.º 1, da GG (Grundgesetz), o Código de Processo Penal Alemão (StPO) disciplina a regulamentação da prova digital nos §§100 a) e § 100 b) (relativos à "*vigilância das telecomunicações*", sujeitando a admissibilidade das medidas de vigilância à autorização do juiz) e §99 (referente à interceção de correspondência e telegramas). ROGALL, Klaus, *A nova regulamentação da vigilância das telecomunicações na Alemanha*, 2.º Congresso de Investigação Criminal, Coord. Científica de Maria Fernanda Palma, Augusto Silva Dias e Paulo de Sousa Mendes, Almedina, Out. 2010, p. 117‑143.

parecem convergir, ora divergir entre si, dificultando a tarefa ao intérprete na articulação destes três diplomas legais, atendendo à complexidade da identificação da norma jurídica aplicável. A este propósito, alude JOÃO CONDE CORREIA que a "*coexistência formal destas normas gera extensas zonas cinzentas de confronto e atrito, porventura impercetíveis ao observador menos atento*"[200], estando hoje a prova digital mergulhada num pântano no cômputo da chamada geografia processual penal, defendendo-se entre a doutrina, nomeadamente PAULO DÁ MESQUITA e RITA CASTANHEIRA NEVES[201], que as Leis 32/2008 e 109/2009 revogaram, tacitamente, parcelas importantes do regime consagrado no art.º 189.º do CPP, reduzindo em larga escala o seu campo de aplicação inicial.

Neste panorama, por mais tentador que seja dissecarmos o diploma da LC (tal a sua virtuosidade em torno de algumas das suas disposições submersas em controvérsia doutrinal), nesta nossa "autópsia", em abono da temática, apenas nos centraremos em torno de duas das suas disposições que vieram, em arrojada inovação, regulamentar a obtenção da prova digital das comunicações eletrónicas, particularmente, nos casos em que o correio eletrónico seja passível de ser apreendido (art.º 17.º da LC) ou intercetado (art.º 18.º da LC).

De tal forma, com o meio de obtenção de prova previsto no art.º 17.º da LC, consagrou o legislador a possibilidade de se apreenderem mensagens de correio eletrónico, bem como de registos de natureza semelhante, que se encontrem armazenadas, submetendo a regulamentação de tal diligência a partir do regime estatuído para a apreensão de correspondência, previsto no art.º 179.º do CPP. Por seu turno, o art.º 18.º da LC, veio contemplar um regime específico para a interceção e registo de comunicações eletrónicas, ali se determinando que, em tudo o que não lhe for contrariado, seja aplicado o regime da interceção e gravação de conversações ou comunicações telefónicas dos art.ºs 187.º, 188.º e 190.º do CPP.

Com a consagração na LC destes dois regimes específicos de obtenção de prova digital, e a remissão para os meios clássicos previstos no CPP, o legislador abriu flanco para uma acesa discussão doutrinária e jurisprudencial relativamente à aplicação e aparente equiparação de regimes que, na sua realidade, são bem diferentes. Com efeito, hoje,

[200] CORREIA, João Conde, *Prova Digital: as leis que temos e a lei que devíamos ter*..., p. 35.
[201] MESQUITA, Paulo Dá, *Processo Penal, Prova e Sistema Judiciário*..., p. 117.

confronta-se o pensamento jurídico com um conjunto de questões que estão longe de se tornar consensuais. Desde logo, a primeira, consiste em saber se fará sentido, ou não, considerar que a opção legislativa equiparou o correio eletrónico ao correio tradicional, assim como saber se a remissão ínsita no art.º 17.º da LC comporta, na íntegra, a aplicação em bloco das regras, formalidades e condicionantes dispostas no art.º 179.º do CPP. Doutro passo, atendendo que a LC não procedeu à efetiva revogação do famigerado art.º 189.º do CPP, revelar-se-á imperioso questionar a vigência e aplicação desta disposição legal, no que toca a interceção de mensagens de correio eletrónico já armazenadas em suporte digital, bem como questionar o sentido e alcance prático da remissão do art.º 18.º da LC para o regime das escutas telefónicas. Eis ao que nos propomos na exposição subsequente.

8. O Art.º 17.º da LC - A Apreensão do Correio Eletrónico

8.1. A Apreensão das Mensagens de Correio Eletrónico e a Cláusula de Extensão Operada pelo Art.º 11.º da LC

Conforme expusemos, a LC veio disciplinar e sobrelevar o tratamento da prova digital a um novo patamar em matéria de investigação criminal, almejando-se com este diploma, entre outros, adaptar as normas do processo penal à progressiva evolução do mundo dos dados, suportes e sistemas informáticos, sobressaindo, conforme PEDRO DIAS e MARTA VEIGA, o envolvimento do estado na procura de "*abordagens inovadoras e que garantam um crescente uso da rede com segurança, estabilidade e abrangência universal*"[202].

Uma das mais irreverentes novidades da LC ateve-se, precisamente, no que ao correio eletrónico diz respeito. De tal forma, aventurando-se o legislador português para além do que se achava circunscrito nos acervos consignados na CCiber, consagrou, na LC, concretamente, no seu art.º 17.º, um regime específico, concebido para a apreensão de mensagens de correio eletrónico armazenadas, rasgando com a matriz adotada no art.º 189.º, n.º 1, do CPP de 2007, libertando-se desta extensão legal que o submetia a uma difícil convivência com as regras do regime das escutas telefónicas, colocando fim à intensa crítica que se fazia sentir quanto à equiparação do correio armazenado em suporte digital, daquele outro ainda em transmissão. Assim, de acordo com o art.º 17.º da LC, "*quando, no decurso de uma pesquisa informática ou outro acesso legítimo a um sistema informático, forem encontrados, armazenados nesse sistema informático ou noutro a que seja permitido o acesso legítimo a partir do primeiro, mensagens de correio electrónico ou registos de comunicações de natureza semelhante, o juiz pode autorizar ou ordenar, por despacho, a apreensão daqueles que se afigurem ser de grande interesse para a descoberta da verdade ou para a prova, aplicando-se correspondentemente o regime da apreensão de correspondência previsto no Código de Processo Penal*". Atendendo à extensão do preceito legal, e para uma adequada análise da opção legislativa, importará decompor a redação.

[202] VEIGA, Pedro e DIAS, Marta, *A Governação da Internet*, Janus.Net, e-journal of International Relations, Vol. 1, n.º 1, 2010, ISSN: 1647-7251, p. 86.

De tal modo, numa simples leitura à redação da norma, desde logo, somos forçados a considerar que o seu campo de aplicação sofre uma compacta restrição legal, atendendo que é o próprio art.º 17.º da LC, a deixar claro que apenas tem aplicabilidade prática em situações onde, efetivamente, já esteja em curso, nos termos do art.º 15.º da LC, uma pesquisa de ficheiros ou outro acesso legítimo a um sistema informático. Isto é, de forma estanque, é a própria norma que condiciona a validação da apreensão de mensagens de correio eletrónico, impondo que estas sejam apreendidas no decurso de uma "busca informático – digital". Nesta medida, conforme RITA CASTANHEIRA NEVES, "*(…), não há, pois, uma ponderação a montante da diligência, mas sim uma ponderação realizada, in casu, na própria decorrência da mesma*"[203].

Ora, o certo é que, com o novo art.º 17.º da LC, e por via da cláusula de extensão operada pelo art.º 11.º, n.º1, al. a), b) e c), deste diploma legal, passa a ser admitido o acesso e apreensão de mensagens de correio eletrónico e registos de natureza semelhante, em todas as investigações criminais cujo crime esteja previsto na LC, bem como aos crimes cometidos por meio de um sistema informático, e, ainda, aos crimes em que seja necessário proceder à recolha de prova em suporte eletrónico. Com a contemplação desta disposição permitiu-se ultrapassar o penoso obstáculo normativo que, até então, existia no regime das escutas telefónicas, porquanto, apenas aos crimes do catálogo (art.º 187.º, n.º1, do CPP) era admissível à investigação a obtenção da prova digital, situação que originava um vazio legal, atendendo ao caráter bastante restritivo do catálogo (crimes puníveis com pena de prisão superior, no seu máximo, a três anos), bem como à exclusão da maior parte da criminalidade tipificada na obsoleta Lei n.º 109/91, sendo-lhe vedada a aplicação deste meio de obtenção de prova.

Pese embora, na resolução de um problema acabaria o legislador por originar outro, ressuscitando uma polémica desnecessária, negligenciando pautas conceptuais quando, no art.º 17.º da LC, *in fine*, remeteu a regulação da apreensão de mensagens de correio eletrónico armazenadas, para o instituto da apreensão de correspondência fechada do art.º 179.º do CPP, cedendo espaço para a criatividade do intérprete, trazendo para dentro desta disposição da LC a velha controvérsia em torno da tutela do correio eletrónico aberto, lido e guardado pelo destinatário, em oposição com aquele outro ainda por si não aberto e, por tal via, não lido.

[203] NEVES, Rita Castanheira, *As Ingerências nas Comunicações*…, p. 274.

Nesta senda, discutindo se o correio eletrónico deve ser equiparado a uma correspondência tradicional, fará sentido questionar o âmbito e alcance da remissão do art.º 17.º da LC, para as regras sobre a apreensão de correspondência que constam do art.º 179.º do CPP, particularmente, deslindando-se a aparente promiscuidade concedida por via da remissão para este regime legal, desconstruindo-se a ilusória tentação de considerar que as mensagens de correio eletrónico já "*armazenadas*" pelo destinatário, se encontram a coberto da tutela constitucional do sigilo da inviolabilidade das comunicações eletrónicas, por equiparação ao sigilo da correspondência de que gozam os documentos abrangidos pelo art.º 179.º do CPP.

8.2. O Correio Eletrónico Armazenado e a sua (não) Equiparação à Correspondência Tradicional

Chamando à colação o que expusemos a propósito da vulnerabilidade das comunicações, que tratamos no ponto 5.2.2., e tendo por assente o circuito de dados inerente ao processo de envio/receção de um *e-mail*, não nos soçobram dúvidas de que, chegados os dados de base, tráfego e conteúdo à esfera do recetor, tendo este efetivo conhecimento da mensagem, cessa a especial vulnerabilidade do sigilo da comunicação, particularmente, os riscos a que está exposto o processo comunicativo pela intromissão arbitrária de terceiros, a quem cabe assegurar a viagem da comunicação, passando, a partir daí, conforme COSTA ANDRADE*, "o destinatário a dispor de meios de autotutela, desde a instalação de sistemas de segurança, programas anti-vírus, codificação críptica, firewall (programas que vigiam o tráfego na internet e avisam o titular do computador das tentativas de envio de programas, do género ´cavalo de Tróia`), até ao apagamento ou destruição, pura e simples, dos dados*"[204].

Valendo-nos das lições do Ilustre Professor Conimbricense, apenas faz sentido falar da proteção do sigilo das comunicações eletrónicas enquanto durar o processo comunicativo, isto é, enquanto o destinatário não tiver, efetivamente, recebido e lido a mensagem que lhe for destinada, radicando assim a tutela de tal sigilo na específica situação de perigo que o terceiro detém sobre o conteúdo e dados da comunicação, impondo-se dizer que, "*não deve identificar-se o fim do processo dinâmico da transmissão com a sua chegada ao (último) aparelho (telefone, computador, etc) do destinatário",* pois que, ainda aqui, a posição do domínio do sistema de telecomunicações sobre a mensagem pode "*revelar-se e actualizar-se*", permanecendo a possibilidade da intromissão no conteúdo da comunicação "*à margem do controlo dos interlocutores*".[205]

De tal forma, aplicando, *mutatis mutandis,* o que vertemos quanto ao momento posterior à vulnerabilidade das comunicações eletrónicas, somos forçados a concluir que os regimes de obtenção de prova dispostos no art.º 17.º da LC, e no art.º 179.º do CPP, sendo autónomos entre si, albergam distintos âmbitos de tutela constitucional: De um lado, os

[204] ANDRADE, Manuel da Costa, *"Bruscamente no verão passado…,* p. 160.
[205] ANDRADE, Manuel da Costa, *"Bruscamente no verão passado…,* p. 160.

dados informatizados processados, tratados e armazenados através das redes, integrados em mensagens de correio eletrónico ou registos de natureza semelhante (art.º 17.º da LC) – sob a proteção constitucional conferida pelo direito à autoderminação informacional - e do outro, a correspondência postal fechada, que utiliza as redes postais públicas - a coberto do sigilo da correspondência (art.º 179.º do CPP).

Por tal motivo, conforme aclara DÁ MESQUITA[206], a propósito da remissão ínsita no art.º 17.º da LC, será errado ver nesta remissão uma qualquer equiparação do art.º 17.º da LC, ao regime processual disposto no art.º 179.º do CPP, relativo à apreensão de correspondência, pois que, neste regime geral, *"não são objecto da sua tutela especial, nomeadamente, mensagens de correio eletrónico já acedidas pelo destinatário"*, defendendo o Autor que, apesar do art.º 17.º da LC ser pouco claro, o que há é uma "*remissão para as regras do processo penal sobre a apreensão de correspondência*", algo substancialmente diferente. De resto, segundo o Autor, é o próprio preceito subsequente na LC (art.º 18.º), a revelar a "*teia sistemática*" que presidiu ao pensamento do legislador, nomeadamente, reservando um meio de obtenção de prova para as mensagens eletrónicas ainda não abertas e lidas.

E a verdade é que, se dúvidas existissem, a mera revisita a génese da criação do art.º 179.º do CPP, conforme já o havíamos feito a propósito do regime das escutas, bastar-nos-ia para concluir que o elemento teleológico que emergiu à criação deste meio de obtenção de prova foi, concretamente, a apreensão "corpórea", e, portanto, material de objetos, cartas, encomendas, valores e telegramas, ainda não recebidos pelo destinatário, onde se coloca em causa a violação do sigilo da correspondência pontificado no art.º 34.º da CRP[207]. De resto, como alumia COSTA ANDRADE[208], é precisamente o facto de "*estar fechada - que define a fronteira da tutela penal do sigilo de correspondência e dos escritos, em geral*", considerando-se que a carta está fechada quando exista "*um procedimento que estabeleça um obstáculo físico à tomada de conhecimento e que só seja ultrapassável à custa de uma actividade física que pode ou não (...) implicar uma ruptura material (...)"*, não bastando *"(...) a sua arrumação num dossier ou numa gaveta aberta*",

[206] MESQUITA, Paulo Dá, *Processo Penal, Prova e Sistema Judiciário*…, p. 118.
[207] Sobre esta matéria *vide* ALBUQUERQUE, Paulo Pinto, *Comentário do Código Penal à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem*, 3.ª Edição, Universidade de Católica Editora, 2015, p. 762-767.
[208] ANDRADE, Costa, *Comentário Conimbricense do Código Penal*…, p. 758.

concluindo o Autor que *"uma carta que foi (ainda que indevidamente) aberta, deixa de ser uma carta fechada mesmo que persista reservada, tendo de se concluir que a correspondência já aberta pelo seu destinatário passa a ter a natureza de documento*", podendo ser apreendida nos termos do art.º 178.º do CPP, gozando "*apenas da proteção que todos os documentos merecem*". Em comentário e anotação a esta disposição processual (art.º 179.º do CPP), a isso mesmo alude PAULO PINTO ALBUQUERQUE referindo-se ao facto desta disposição proteger *"toda a correspondência enquanto ela não foi aberta pelo seu destinatário",* sendo que *"(...)a apreensão da correspondência já aberta pelo seu destinatário está subordinada ao regime geral do artigo 178.º, com ressalva do disposto quanto à correspondência abrangida pelo segredo profissional ou segredo médico"*[209]. De resto, para o Autor, a diligência de apreensão implica que a correspondência seja retirada do "*circuito normal do correio*", não sendo possível apreender uma carta para dela se extrair uma certidão, devolvendo-se em seguida ao seu circuito normal.

Nesta esteira, analisando a temática e ancorando-se nos ensinamentos de COSTA ANDRADE, antes mesmo de se debruçar sobre a nova LC, RITA CASTANHEIRA NEVES sustentava que o correio eletrónico – tal como a SMS – já aberto e lido, deve ser tratado como um ficheiro digital[210]. Assim, segundo a Autora, *"o correio eletrónico que já foi aberto e lido, que já cumpriu a sua função de comunicação, deve ser entendido como um ficheiro informático. Ora, se assim é, a forma de se aceder ao mesmo no âmbito de uma investigação criminal deve cumprir os requisitos de admissibilidade e forma já não de regimes assentes na intercepção de comunicações, como o regime das escutas*

---

[209] ALBUQUERQUE, Paulo Pinto, *Comentário do Código de Processo Penal à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem*, 2.ª Edição, Universidade Católica, Lisboa, 2008, p. 509. Ainda antes da reforma de 2007 ao CPP, defendia PEDRO VERDELHO que as mensagens eletrónicas já "*abertas e porventura lidas e mantidas no computador a que se destinavam, não deverão ter mais protecção que as cartas em papel em que são recebidas, abertas ou porventura guardadas numa gaveta, numa pasta ou num arquivo"*, devendo ser tratadas como *"meros documentos escritos que podem sem qualquer reserva ser apreendidos numa busca*". VERDELHO, Pedro, *Apreensão de Correio Electrónico em Processo Penal*..., p. 157-159.

[210] A este propósito, questionando se o correio eletrónico seria comparável a uma carta, VÂNIA RAMOS responde que "*relativamente à correspondência temos uma barreira corpórea – o invólucro da carta – que pode continuar a existir, claramente, mesmo depois da recepção, mantendo o carácter confidencial da carta. Já no que diz respeito às comunicações electrónicas, não existe, propriamente, essa barreira corpórea. O próprio regime processual penal, ao diferenciar as situações de apreensão e intercepção da correspondência das de intercepção das comunicações, reconhece a sua diferente natureza e reconduz a comunicação electrónica a esta última(...)". Cfr.* RAMOS, Vânia Costa, *Âmbito e Extensão do Segredo*..., p. 156.

telefónicas – ou mesmo da apreensão de correspondência -, mas sim de regimes pensados e direccionados para o acesso e obtenção de objectos, lata categoria na qual se incluem documentos e também suportes digitais. Estamos neste campo, assim, perante diligências de prova como as buscas e as apreensões".[211] Também CARLOS ADÉRITO TEIXEIRA, a propósito das mensagens eletrónicas já abertas, lidas e armazenadas, alumiando à diferença entre o suporte de papel e suporte digital, sustentava, já após a reforma ao CPP de 2007, que, cessando o sigilo da comunicação, não "*deveria avaliar-se à luz do regime da correspondência, porquanto, ainda que pudesse ser equiparada, tinha deixado de estar sujeita àquele regime, após a tomada de conhecimento do destinatário"*[212]*,* admitindo, no entanto, uma "*ponderação diferenciada*" por parte do juiz, pelas "*dimensões de sigilos e de direitos (v.g. intimidade),* " implicados no seu conteúdo.

Pelos argumentos expostos, concordamos com os Autores supra. De facto, se admitíssemos que o correio eletrónico, por via do enunciado no n.º 1, do art.º 179.º do CPP, caberia na parte da redação que alude a "*qualquer outra correspondência*", não mais estaríamos senão a submeter esta disposição legal numa falaciosa e perigosa extensão conceptual, para a qual o legislador não estava intencionado, desconsiderando-se, desde logo, a virtuosa existência de um diploma legal hoje vigente, como é a LC, que regula toda a prova digital, sendo incontornável dizer-se que o correio eletrónico, enquanto veículo privilegiado no campo das novas formas de comunicação, é, em si mesmo, uma alternativa à via da correspondência tradicional.

Por seu lado, caso se pugnasse pela aplicação ao correio eletrónico, em bloco, de todos os requisitos constantes dos n.ºs, 1, 2, 3 e 4, do art.º 179.º do CPP, não restariam grandes dúvidas em concluir que, neste domínio, o correio eletrónico sairia beneficiado atendendo à maior proteção da privacidade da pessoa visada que goza deste regime, por via dos rígidos requisitos de obtenção de prova que lhe estão subjacentes, desde logo, a exigência de que, em causa, esteja um crime com pena máxima de prisão superior a três anos, originando, mais uma vez, que o intérprete caísse na inadvertida tentação de ignorar a cláusula de extensão operada pelo art.º 11.º da LC, ou na basilar premissa de negligenciar os próprios requisitos de admissibilidade consagrados no art.º 17.º da LC.

---

[211] NEVES, Rita Castanheira, *As Ingerências nas Comunicações*…, p. 190.
[212] TEIXEIRA, Carlos Adérito, *Escutas Telefónicas: a mudança de paradigma* …, p. 284.

Ora o certo é que, ainda antes da reforma operada ao CPP de 2007, ROGÉRIO BRAVO[213] esgrimia três argumentos de direito, e um argumento técnico informático, pugnando pela não equiparação do correio eletrónico à correspondência postal para efeitos de apreensão a nível processual penal. Em primeiro lugar, ancorando-se num argumento de natureza histórica, aludia o Autor ao facto do legislador, já após ter consciência com a nova realidade do correio eletrónico, não ter aproveitado as revisões ao CP realizadas em 1995, em 1998, 2001, em 2003 e em 2004 (acrescentaríamos 2007), no sentido de equiparar, na legislação penal (art.º 194.º do CP), os dois tipos de correio[214]. Doutro passo, sustenta o Autor que todas as expressões consagradas pelo legislador na redação do artigo 194.º do CP ("*Violação de correspondência ou de telecomunicações*"), tais como "*carta*", "*escrito fechado*", "*abrir carta*", se referem a sobrescritos e a encomendas (corpóreos) fechados, sendo que a expressão "*intrometer*", utilizada pelo legislador**,** constante no n.º 2 deste artigo, aponta manifestamente no sentido de uma interceção de mensagem em trânsito, que não encontra paralelismo com dados armazenados num sistema informático, "*seja ele um servidor de uma empresa, seja um computador de secretária*". Por tal via, ao contrário da correspondência tradicional, uma mensagem de correio eletrónico não está, nem nunca poderá vir a estar, "fechada", não podendo de resto ser "envelopável". Num terceiro argumento, ROGÉRIO BRAVO destaca o facto de, a nível do CPP, o legislador não ter aproveitado as revisões operadas ao diploma para realizar, na sistematização do art.º 179.º, uma equiparação entre o correio eletrónico e o correio tradicional, realçando o facto de, no caso do correio eletrónico, se ter dado primazia à regulação a partir do regime das escutas telefónicas, por via da cláusula de extensão do art.º 190.º do CPP [atual 189.º com a revisão de 2007]. Como argumento de caráter técnico-informático, aduzia o Autor que não existem programas informáticos capazes de detetar se uma mensagem de *e-mail* foi "aberta", "lida" e posteriormente "fechada", sendo que, *"por natureza, uma mensagem de correio-eletrónico não é fechada, não é envelopável, não é unívoca quanto ao número*

[213] BRAVO, Rogério, *Da não equiparação do correio - eletrónico ao conceito tradicional de correspondência por carta*…, p. 207-216.

[214] A este propósito, já em 2004, PEDRO VERDELHO pugnava que *"não tendo o legislador alargado ao correio eletrónico a protecção criminal que confere ao correio e às telecomunicações, é legitimo concluir-se que não pretendeu fazê-lo*". VERDELHO, Pedro, *Apreensão do Correio Eletrónico em processo Penal*…, p. 163.

de destinatários e não circula em ambiente seguro (por algum motivo a "SEGNAT 3" classifica o correio-eletrónico como "meio de comunicação não seguro)"[215].

Efetivamente, concordando-se com ROGÉRIO BRAVO, julgamos que do ponto de vista técnico – informático, e tendo em consideração aquelas que são hoje as evoluídas características do *software* utilizado pelos programas de envio/receção de correio eletrónico, é impossível determinar quando é que um *e-mail* foi ou não lido. De resto, não existe na ciência digital um programa informático forense que determine, com exatidão, essa mesma operação, daí emergindo a volatilidade da mensagem de correio eletrónico e os riscos a que esta prova digital se encontra exposta, designadamente, a facilidade de alteração do *status* de uma mensagem eletrónica que já foi lida e armazenada, remarcando-a como não lida. Por aqui, somos forçados a concluir que a integridade, a fiabilidade e a genuidade da prova física permitem, com acuidade, considerar que, no caso da correspondência tradicional, a especial proteção constitucional do sigilo da correspondência cessa quando a "carta" é deixada na caixa de correio postal do destinatário, entrando na sua esfera de disponibilidade fática, deixando assim os serviços postais de ter domínio sobre a correspondência[216], podendo o destinatário, a partir da entrega, conforme COSTA ANDRADE, citando LECKNER e MAIWALD, consentir a abertura ou tomada de conhecimento por terceiro (ainda que contra a vontade do remetente), passando a ser, por inteiro, o portador do bem jurídico da privacidade.

Com pertinência nesta matéria, e numa referência ao que apelida de *"zonas cinzentas"*, enaltece VÂNIA COSTA RAMOS que nos serviços de *webmail,* ou IMAP, os dados de ligação permanecem armazenados na esfera de terceiros (*provider*), ainda que já acedidos pelo destinatário, acabando por ser difícil determinar o momento em que termina a comunicação e, com ela, a proteção do segredo das comunicações[217], não se deixando,

---

[215] BRAVO, Rogério, "*Da não equiparação do correio - eletrónico ao conceito tradicional de correspondência por carta*…, p. 214. Ainda neste âmbito, destaque-se a conclusão avançada por PEDRO MAURÍCIO, aludindo ao facto de que, mesmo num produto de troca de mensagens eletrónicas tão como completo e avançado como é o "*Outlook*", foi possível escrever código em laboratório que permitiu confirmar a impossibilidade de se determinar se uma determinada mensagem de *e-mail* já foi aberta e, tendo sida, quantas vezes foi aberta depois de recebida. *Vide* MAURÍCIO, Pedro, *O Correio Eletrónico – Aspectos importantes para a investigação criminal*, Área de Documentação e Tradução da Policia Judiciária, Lisboa, 2006.

[216] ANDRADE, Manuel da Costa, *Comentário Conimbricense do Código Penal*…, p. 1087.

[217] Em Portugal, como também entendido pelo *BVERG*, vigora o entendimento que os dados de ligação armazenados no servidor, mesmo após a comunicação, gozam da proteção do sigilo das comunicações, imposta pelo risco específico do processo comunicativo estar confiado a terceiros. RAMOS, Vânia Costa, *Âmbito e Extensão do Segredo*…, p. 156.

contudo, aqui de perfilhar o entendimento dominante da doutrina, à giza de COSTA ANDRADE invocando a decisão do Tribunal Constitucional Federal alemão, de 16.06.09, (a propósito da extensão do art.º 10.º da Lei Fundamental), que vai consolidando que, independentemente de lidos ou não lidos, "*a intromissão e apreensão de e-mails no mail server do provider devem enquadrar-se no direito fundamental da inviolabilidade das telecomunicações*", pois que, ainda aqui, "*o provider detém o domínio exclusivo sobre a comunicação*", tendo acesso livre aos dados de tráfego e conteúdo[218].

Acompanhando-se tal reflexão, de facto, não apenas no caso dos *webmails*, bem como propriamente nas *Private Messages* das plataformas de redes sociais (nomeadamente no *Facebook*, no *Twitter*, no *Instagram,* entre outras aplicações), onde o utilizador se regista e cria uma conta de "natureza semelhante" ao *e-mail*, o acesso é feito a partir de um *browser* da Internet, sem necessidade de instalação de qualquer programa informático no dispositivo eletrónico, bastando, para o seu acesso, introduzir as credenciais da aludida conta. Ora, quando se procede a uma pesquisa e apreensão, a não ser que o suspeito tenha gravado um ficheiro no seu computador[219], pode suceder que os dados a pesquisar se encontrem alojados/armazenados no servidor do *webmail*, tornando-se, por tal motivo, impossível apreender as mensagens de correio eletrónico por não se possuírem as credenciais da conta (a não ser que o visado da pesquisa colabore fornecendo a respetiva *password*[220]). Em tal hiato temporal, facto é que o próprio visado pode eliminar remotamente estas mensagens, contrariamente ao que sucede no correio tradicional, motivo

---

[218] ANDRADE, Manuel da Costa, *Comentário Conimbricense do Código Penal*..., p. 1098-1099. Partilhando do mesmo entendimento *vide* RODRIGUES, Benjamim Silva, *Da Prova Penal – Tomo II, Bruscamente*..., p. 381-383.

[219] Neste âmbito, é curiosa a reflexão que ARMANDO RAMOS faz a propósito dos ficheiros anexos ao *e-mail*. Assim, convida-nos o Autor a fantasiar a situação em que determinado indivíduo recebe um *e-mail* que vem acompanhado, em anexo, de um ficheiro. Ora, "*Sem ler este e-mail e o seu respetivo anexo, o referido indivíduo efetua uma cópia ou procede à gravação do anexo para o disco do seu computador ou outra qualquer partição amovível e apaga a mensagem de correio eletrónico que recebera. No caso de o indivíduo vir a ser alvo de uma busca e apreensão (…) Obviamente que o juiz vai considerar que este anexo, gravado numa parte do disco ou numa partição amovível, não passa de um ficheiro, ainda que o suspeito da busca alegue que o tinha recebido por correio eletrónico, que ainda o não tinha lido e que deverá por isso, ter o mesmo tratamento que é dado, por força da equiparação legal vigente, à correspondência recebida e ainda fechada"*. RAMOS, Armando Dias, *A Prova Digital em Processo Penal*, 1.º ed...., p. 62.

[220] A recusa do arguido, no decurso de uma pesquisa informática, em facultar o acesso da *password* do computador, ou de qualquer outro sistema informático, legitima, nos termos do art.º 16.º da LC, as autoridades judiciárias a apreender o suporte onde está instalado o sistema ou onde estão armazenados os dados do computador. Por seu turno, a recusa do arguido em facultar as credenciais das contas de *e-mail* detidas no servidor de *webmail*, legitima, nos termos do art.º 14.º da LC, as autoridades a intervir diretamente junto do servidor/alojador dessa conta. Cfr. NEVES, Rita Castanheira e CORREIA, Hélder Santos, *A lei do cibercrime e a colaboração do arguido no acesso aos dados informáticos,* Actualidad Jurídica Uria Menéndez, n.º 38, 2014, p. 146-149.

pela qual, a coexistência desta possibilidade de operação informática, é, também ela, suficientemente dissuasora para justificar a não equiparação entre estes meios de comunicação.

Doutro passo, a gradual adesão à utilização do envio/ receção de mensagens por via de *e-mail*, brinda-nos, todos os dias, com toda uma panóplia de *e-mails* não solicitados, nem sempre fidedignos e bem-intencionados, sendo disso exemplo os *e-mails* acompanhados com ficheiros que visam a distribuição de *malware*[221] pelo dispositivo onde são abertos e descarregados. Tal circunstância ocorre atendendo que os sistemas informáticos estão formatados para permitir o envio automático de mensagens, sem que o seu destinatário o tenha requerido, pesa embora a criação de filtros por parte da grande maioria dos servidores (são disso exemplo o *Hotmail, Gmail, o Outlook Express, Sapo, Yahoo,* entre outros) que, cada vez mais, protegem o utilizador/recetor alertando-o, quando não ocorra o seu bloqueio, para não abrir determinada mensagem, nomeadamente, sinalizando-a como SPAM[222] (no fundo tratando-a como correio não solicitado e potencialmente lesivo da privacidade, redirecionando-a para outra pasta).

Por seu turno, a evolução de alguns programas informáticos, aliada à permissividade dos sistemas de rede, tornou possível que determinado dispositivo, uma vez infetado com *malware*, possa, ele mesmo, de forma automática e robotizada, proceder ao reenvio *de e-mails* em massa, contaminando num par de horas milhões de computadores, existindo, assim, apenas mão humana na criação do *software* malicioso. Neste conspecto, estando o SPAM associado ao envio em massa de uma mensagem eletrónica, difundida por um número indeterminado de destinatários, pode suceder que, sem qualquer intervenção humana, e com recurso a servidores denominados de *botnets*[223], determinado utilizador não

---

[221] Em linguagem informática, o *malware* é vulgarmente conhecido como vírus malicioso. No fundo, trata-se de um *software* desenvolvido para infiltrar-se no sistema informático de um equipamento, de forma ilícita, com o intuito de causar alterações programáticas, normalmente concebido para a obtenção de informações e dados confidenciais.

[222] O termo SPAM, tendo aparecido sensivelmente em meados da década de 90, começou por estar associado ao ato de interferir no normal funcionamento dos protocolos da Internet, com o objetivo de causar a inoperância dos sistemas operativos. Atualmente, segundo a definição da SPAMHAUS, organização de referência a nível mundial no combate ao SPAM, o termo é utilizado para designar correio eletrónico não-solicitado enviado em massa. Disponível *online* no endereço https://www.spamhaus.org/ [consultado em 26 de Abril de 2017]. Sobre esta matéria *vide* COSTA, Bruto da, e BRAVO, Rogério, *Spam e Mail Bomb, Subsídios para uma perspectiva criminal*, Quid Juris, 2005, p. 14-40.

[223] O termo está associado à criação de um *software* malicioso que permite ao *cracker*, de forma remota, obter controlo completo do computador afetado em modo *bot* (robô). Ou seja, o computador é transformado num "zombie" para realizar tarefas de forma automática na Internet, sem o conhecimento do utilizador. Os

se aperceba que o seu dispositivo esteja a ser monitorizado para o envio de mensagens de correio eletrónico que, por tal via, procuram contaminar o computador de terceiros. No fundo, o intuito dos meliantes do crime é o acesso, ainda que remoto e sem que o *user* se aperceba, a dados confidenciais que os destinatários possuem, como por exemplo dados de acesso a *sites* com as credenciais da área reservada. Bastar-nos-á recordar dos imensuráveis danos provocados pelas célebres *Cartas da Nigéria*[224], ou dos recentes ataques provocados pelo *malware "Marai"*[225], para percebermos a amplitude e *modus operandi* deste tipo de ilicitude, sempre se impondo a questão: Seria pensável instrumentalizar o correio tradicional para a prática destes atos? Manifestamente, a resposta não pode deixar de ser negativa.

Por outro lado, a reflexão sobre a possibilidade dos próprios servidores de correio eletrónico, poderem, *per si*, filtrar as mensagens de correio eletrónico, nomeadamente, procederem ao bloqueio ou sinalizando-as como SPAM, interferindo na mensagem que é destinada a determinada pessoa, vem desnudar um paradigma referente à responsabilidade criminal do administrador do sistema informático a que o direito penal não consegue dar resposta. O art.º 384.º do CP tipifica criminalmente a conduta violadora do segredo de correspondência ou de telecomunicações, por parte de funcionário de serviços dos correios, telégrafos, telefones ou telecomunicações, catalogando o art.º 386.º do CP o que é considerado de "funcionário". De tal modo, acompanhamos a reflexão de ARMANDO RAMOS que *"nos leva a defender a não equiparação, pois caso contrário os*

---

computadores afetados, por sua vez, formam uma *botnet* (rede de agentes de software ou *bots*) concebida para o envio de spam, disseminação de vírus, ataque a computadores e servidores, utilizada para fins ilícitos.

[224] Tendo despoletado na década de noventa, as "*Cartas da Nigéria"* ficaram conhecidas como um esquema fraudulento, consistindo a fraude no envio de cartas (e posteriormente *e-mails*) por um emissor (geralmente domiciliado na Nigéria) a pessoas, empresas ou organizações, a quem se prometia um negócio altamente rentável, por via de um prémio ganho numa lotaria. O agente criminoso solicitava a ajuda da vítima, alegando tratar-se de uma personalidade pública (geralmente membro do governo nigeriano), a quem não convinha a publicidade sobre o prémio, pedindo à vitima o envio de algum dinheiro para custear despesas com a obtenção de visto para o estrangeiro, deslocação e outras diligências que lhe permitissem poder vir a Portugal e dar à vitima parte do seu prémio. Nunca tendo a lotaria existido, a finalidade do esquema de burla visava o envio de pequenas quantias, por parte do recetor, ao remetente da missiva. Informação disponível *online* no endereço http://www.apav.pt/cibercrime/ [acedido em 25 de Março de 2017]. Também sobre a matéria, FERNÁNDEZ TERUELO, Javier Gustavo, *Cibercrim, Los delitos cometidos através de Internet*, Constitutio Criminalis Carolina, 2007, p. 33-41.

[225] O *Mirai* é um *software* que explora várias vulnerabilidades de segurança em sistemas informáticos e que tem o poder de controlar equipamentos. O último grande ataque sucedeu em 21 de Outubro de 2016, deixando paralisado o sistema informático da *Dyn*, um dos maiores serviços de comunicação norte-americano responsável pela monitorização de tráfegos de empresas como a *Twitter, Spotify e Netflix*. Informação disponível *online* no endereço http://www.acriacao.com/sexta-feira-dyn-e-o-inicio-da-guerra-cibernetica/ [acedido em 30 de Março de 2017].

administradores/gestores de servidores de correio eletrónico estariam a cometer o ilícito criminal de violação de correspondência ou de (tele)comunicações, ao "bloquearem" e "reterem" mensagens de correio eletrónico que não lhes estavam dirigidas, e desta forma impedirem que as mesmas fossem recebidas pelos destinatários, conforme estipulado pelo art. 194.º, n.º 1, do CP"[226]. Assim, apenas poderia, porventura, existir equiparação, se se representasse que o administrador do servidor do correio eletrónico pudesse assumir a qualidade de funcionário para efeitos do art.º 386.º CP, impedindo-o, assim, de filtrar as mensagens com destino a um qualquer recetor[227].

Do exposto, não seria necessário chegarmos até aqui para firmarmos a nossa convicção que, de facto, o legislador teve efetivamente em conta, pese embora a técnica remissiva operada no art.º 17.º da LC para as regras (ou apenas para algumas conforme veremos) da apreensão de correspondência do CPP, duas realidades distintas: a apreensão de mensagens de correio eletrónico armazenadas, tratadas no art.º 17.º da LC, e a apreensão de correspondência fechada, disciplinada no art.º 179.º do CPP. E se é um facto que acabou o legislador por não ser muito claro, concordando-se que a remissão deixou espaço para uma polémica desnecessária, não soçobram dúvidas que se pretendeu conferir ao correio eletrónico, já armazenado, uma tutela superior à garantia conferida aos vulgares escritos, cuidando-se, particularmente, de não o submeter ao livre arbítrio da investigação, protegendo-o das vicissitudes que a "*vasculhagem*" da diligência de apreensão pudesse comportar, sem o olhar atento e legitimador do juiz, reservando-se-lhe um papel fundamental quanto à autorização judicial legitimadora da apreensão destas concretas mensagens eletrónicas.

No fundo, conforme RITA CASTANHEIRA NEVES, pretendeu o legislador conferir um "*plus de proteção*" ao correio eletrónico armazenado, em nome da salvaguarda

---

[226] RAMOS, Armando Dias, *A Prova Digital em Processo Penal*, 1.º ed..., p. 58. A este propósito, recentemente, obtiveram-se notícias que a *Google* lê os *e-mails* dos seus utilizadores, informando que "*os nossos e-mails recebidos, enviados ou armazenados, são analisados por um software para desenvolver anúncios específicos para cada utilizador*". Informação disponível *online* no endereço https://www.google.pt/intl/en/policies/terms/regional.html [acedido em 15 de abril de 2017].

[227] Neste âmbito, não podemos ficar alheios à circunstância de ser extremamente fácil criar uma conta de *e-mail* recorrendo a determinado servidor. A crescente proliferação de servidores e o galopante número de utilizadores veio criar um problema de identidade de *users,* ao ponto das "moradas" do correio eletrónico se terem tornado altamente confundíveis e, inclusivamente, semelhantes, divergindo apenas no servidor. Inevitavelmente, a confusão pode facilmente induzir o utilizador a enviar determinada mensagem para um destinatário de correio eletrónico que não o desejado, com o prejuízo deste destinatário acabar por ler o seu teor. No campo do correio tradicional tal nunca aconteceria, atendendo à tipificação da conduta criminosa ínsita no art.º 194.º, n.º1, do CP, que impediria o terceiro de abrir a carta.

da privacidade da autodeterminação informacional, acabando o legislador, claramente, por colocar em *"pé de desigualdade o grau de protecção conferido aos meios de obtenção de prova que têm por objecto ficheiros informáticos resultantes de correio eletrónico e os meios de obtenção de prova que têm por objecto arquivos resultantes de comunicações postais*"[228], reconhecendo-se, assim, à luz dos parâmetros constitucionais, por recondução aos art.ºs 26.º e 35.º da Lei mãe, uma proteção adicional da "*privacidade eletrónica digital*"[229], no sentido de evitar qualquer fenómeno anómalo que implique uma perda irreparável no desapossamento da identidade pessoal e da reserva da intimidade da vida privada. De resto, conforme exposto, colocando-se o correio eletrónico no domínio da prova digital e imaterial, dado o seu caráter volátil, coloca-se com acuidade a questão da conservação e obtenção dos dados gerados pela comunicação, pelo que sempre se tornaria imperioso controlar e fiscalizar o ciclo informacional e comunicacional entre interlocutores, reforçando-se a expectativa de que, quem confia as suas palavras aos operadores de comunicações, fá-lo na legítima confiança que a integridade das redes mantenha a segurança, confidencialidade e integridade da comunicação.

8.3. A Importância da Pesquisa Informática na Apreensão das Mensagens de Correio Eletrónico

Conforme veiculamos, a LC, enquanto Lei extravagante, condensou num só diploma especial os novos meios de obtenção de prova concebidos para a recolha da prova digital, aglutinando, de forma sistematizada, disposições processuais adaptadas à pesquisa e recolha de dados informáticos, revelando o diploma uma efetiva cautela no que concerne à harmonização da recolha da prova com os direitos fundamentais do visado, designadamente, a salvaguarda dos seus direitos, liberdades e garantias.

De tal forma, no que nos ocupa, no art.º 17.º da LC, cuidaria o legislador de contemplar um conjunto de pressupostos de verificação prévia de que, sob exigência legal, dependeria a diligência de apreensão de mensagens de correio eletrónico. Desde logo, ao condicionar que, sob pena de nulidade, a apreensão de mensagens de correio eletrónico só poderia ocorrer *"no decurso de uma pesquisa informática ou outro acesso legítimo a um*

[228] NEVES, Rita Castanheira, *As Ingerências nas Comunicações*..., p. 277.
[229] RODRIGUES, Benjamim Silva, *Da Prova Penal – Tomo II, Bruscamente*... , p. 342-347.

sistema informático", tornar-se-ia imperativo considerar que a diligência de apreensão ficaria, umbilicalmente, dependente de um prévio despacho por parte da autoridade judiciária[230] que legitimasse a aludida "*pesquisa de ficheiros ou acesso a sistemas informáticos*", prevista no art.º 15.º da LC. Dada a elevada importância que reveste a diligência de pesquisa de dados informáticos, descrita no aludido art.º 15.º, impõe-se fazer uma breve consideração sobre a mesma.

Em termos informáticos, podemos definir o processamento de dados como o conjunto de todas as operações (reconduzíveis a esquemas "se" e "então"), controladas por um programa informático, efetuadas a partir de um computador ou outros dispositivos eletrónicos, com o objetivo de transformar dados, desde a entrada de informação (*inputs*), até à sua saída (*outputs*).[231] Neste percurso informático, assume primordial importância a etapa do armazenamento de dados, atendendo que é aqui que se permite deslindar todas as etapas do processo comunicativo e os seus resultados. Os sistemas informáticos modernos podem chegar a ter uma capacidade de armazenamento de dados gigantesca, sendo que, tal circunstância, pode obstaculizar uma investigação, podendo, inclusivamente, estar votada ao fracasso por via da impossibilidade em rastrear todo o conteúdo de dados armazenados em determinado suporte digital, colidindo com os prazos processuais reservados à fase de inquérito, dispostos no art.º 276.º do CPP.[232]

Por tal motivo, o legislador consagrou no art.º 15.º da LC, um mecanismo que permite às autoridades judiciárias, sempre que verificarem oportuno e necessário à descoberta da verdade material, competência para pesquisar, dentro de determinado sistema informático, específicos e determinados dados informáticos neles armazenados. Por outro lado, procurou-se que este meio de obtenção de prova fosse menos invasivo na esfera privada, não sendo exigível a apreensão física dos computadores e outras máquinas ou dispositivos físicos[233], pretendendo-se, tão só, o acesso aos dados armazenados num

---

[230] Nos termos do art.º 1.º, al. b), do CPP, é considerado "*Autoridade Judiciária - o juiz, o juiz de instrução e o Ministério Público, cada um relativamente aos actos processuais que cabem na sua competência*".

[231] A este propósito vide SCHNEIDER, Jochen, *Processamento electrónico de dados – informática jurídica - Introdução à Filosofia do Direito e à Teoria do Direito Contemporâneas*, org. de A. Kaufmann e W. Hassemer, Fundação Calouste Gulbenkian, Lisboa, 2002, p. 547 e ss.

[232] Inúmeros processos judiciais, em fase de inquérito, demonstram-nos que o processo de rastreabilidade da prova digital não se apraz e compadece com os prazos reservados ao inquérito.

[233] Nos termos do art.º 16.º, n.º 7, al. a), b), c) e d), da LC, a apreensão de dados pode fazer-se sob a forma: (1) de apreensão do suporte onde está instalado o sistema ou apreensão do suporte onde estão armazenados os dados informáticos, assim como os dispositivos necessários à sua leitura; (2) de cópia em suporte

sistema informático para recolha da informação que estes contenham (sendo suficiente a sua cópia em PEN's, com a versão do "*FTK Imager*" da *AccessData,* ou CD-R[234]). Em termos simplistas, o que é importante é a memória e não a máquina.

De tal modo, conforme consignado em Acórdão do TC, n.º 210/2017[235], de 27.04.2017, há que denotar que na pesquisa informática do art.º 15.º da LC, "*não está em causa a pesquisa específica de correio eletrónico e, muito menos, a forma de acesso ao conteúdo e/ou apreensão dos mesmos, uma vez localizados no interior de um sistema informático, matéria que, aliás, está regulada no artigo 17.º da citada Lei",* sendo que, como vem veiculando PEDRO VERDELHO, "*será completamente errado ver nesta figura algum tipo de substituto para os exames, clássicos meios de obtenção de prova, previstos nos arts. 171.º e segs. do Código de Processo Penal (CPP). Aliás, a lei é clara e expressa, dizendo que a esta diligência são aplicáveis, naquilo que não estiver expressamente previsto e com as necessárias adaptações, as regras de execução das buscas previstas no Código de Processo Penal"[236],* sendo, de resto, o que resulta do art.º 15.º, n.º 6, contendo, os seus n.ºs 2 a 4, procedimentos idênticos ao regime das buscas, não se perdendo de vista que se está perante um meio de prova realizado no espaço digital.

Assim, se tivermos presente que a realização da busca, prevista e disciplinada no CPP, obedece a distintos procedimentos e critérios de admissibilidade na recolha e obtenção da prova, consoante o objeto físico a buscar se encontre num domicílio/local reservado [237], ou, inversamente, num local acessível ao público, concluímos, adaptando o

---

autónomo; (3) de preservação, por meios tecnológicos, da integridade dos dados, sem realização de cópia nem remoção dos mesmos e (4) por via de eliminação não reversível ou bloqueio do acesso aos dados.

[234] Nos termos do art.º 16.º, n.º 8, da LC, a "*cópia é efectuada em duplicado, sendo uma das cópias selada e confiada ao secretário judicial dos serviços onde o processo correr os seus termos e, se tal for tecnicamente possível, os dados apreendidos são certificados por meio de assinatura digital*".

[235] Ac. disponível *online* no endereço http://www.tribunalconstitucional.pt/tc//tc//tc/acordaos/20170210.html [acedido em 11 de Maio de 2017].

[236] VERDELHO, Pedro, *A Nova Lei do Cibercrime*..., p. 740. Idêntica solução é consagrada no regime de apreensão de dados informáticos, previsto no art.º 16.º da LC, contemplando, na sua matriz, um regime próximo das apreensões dispostas nos art.ºs 178.º e ss. do CPP.

[237] As buscas domiciliárias pautam-se pela procura de objetos que estão escondidos num local reservado, ou não livremente acessível ao público, devendo definir-se o grau de intervenção da busca em ordem a preservar-se a privacidade emanada do direito à inviolabilidade do domicílio e à reserva da intimidade da vida privada. O legislador prevê o "domicílio" em sentido amplo, como todo o espaço onde decorre a vida familiar, incluindo a casa de férias, a tenda (Cfr. Ac. TRE de 04.07.1995), o carro, o barco, a roulotte, entre outros espaços – desde que haja indícios de serem locais de habitação (Cfr. Ac. TC nºs 7/1987 e 459/1989), não devendo ser extensível a outros espaços que tenham caráter laboral, como por exemplo oficinas, escritórios e empresas, entre outros. GOMES CANOTILHO e VITAL MOREIRA incluem no conceito de domicílio a sede das pessoas coletivas, contrariamente a VIEIRA DE ANDRADE, que as afasta deste conceito, adotando uma conceção mais restrita. CANOTILHO, Gomes e MOREIRA, Vital, *Constituição*

regime geral do CPP ao art.º 15.º da LC, que a remissão releva, por exemplo, se numa determinada pesquisa de dados informáticos houvesse a suspeita de que o sistema informático em causa pertencesse a um cibercafé - portanto num local acessível ao público - o que ocasionaria que os procedimentos a adotar fossem os previstos no art.º 174.º do CPP, sendo bastante, para legitimar a diligência, um mandado de autorização da autoridade judiciária. Ao invés, se a suspeita recaísse sob um endereço IP cuja origem tivesse sido numa determinada habitação, já seria a partir dos procedimentos ínsitos da busca domiciliária (art.º 177.º do CPP) pelos quais a pesquisa informática se regularia, exigindo-se que tal diligência fosse *"ordenada ou autorizada por um juiz e efectuada entre as sete e as vinte horas, sob pena de nulidade*", excetuando-se os casos em que esteja em causa um crime de terrorismo, criminalidade violenta ou altamente organizada, quando haja indícios de que vai ser cometido um crime susceptivel de pôr em risco a integridade física ou a vida de alguém, quando o visado consentir a busca ou em caso de flagrante delito pela prática de crime punível com pena de prisão superior a 3 anos, casos em que estaria o MP legitimado a ordenar a busca.

Nos termos do art.º 15.º, n.º 2, da LC, a autorização de pesquisa é válida por 30 dias, tendo o efeito da nulidade quando ocorra em desrespeito a tal prazo, com a inerente insuscetibilidade de valoração da prova para efeitos criminais. A este propósito, como alerta BENJAMIM SILVA RODRIGUES, deve a autoridade judiciária indicar no despacho de autorização, qual a data de início da contagem para a "*vasculhagem*", a fim de se "*evitar os tais "cheques em branco" que, vulgarmente ocorre, já que o órgão de polícia guarda, no bolso, a autorização judicial e executá-la-ia, a coberto de razões de ordem técnica ou táctica, para um momento oportuno"*[238], correndo o risco de se tornar um despacho que conceda ao OPC uma inadmissível arbitrariedade, desrespeitando os princípios da legalidade e da atualidade.

Destaque, ainda, para o facto desta específica diligência, conforme resulta do art.º 15.º, n.º 1, *in fine,* dever ser presidida, sempre que possível, pela autoridade judiciária competente, consoante a fase processual. Entre a doutrina, BENJAMIM SILVA RODRIGUES tem pugnado pela interpretação restrita da norma, no sentido de se apagar a

---

Republica Portuguesa Anotada, Volume I, 4ª Edição Revista, Coimbra Editora, 2007, p. 303; ANDRADE, José Carlos Vieira de, *Os Direitos Fundamentais na Constituição de 1976*..., p. 117-126.

[238] RODRIGUES, Benjamim Silva, *Da Prova Penal – Tomo IV, Da Prova - Electrónico - Digital e da Criminalidade Informático – Digital*..., p. 525 e 526.

sua aparente abertura, não deixando de se exigir que à diligência "*presida a autoridade judiciária que a ordenou ou autorizou"*[239]*,* tanto mais que, à semelhança do que ocorre no art.º 179.º, n.º 3, do CPP, é a presença da autoridade judiciária que garante a autenticidade, fidedignidade e não contaminação da prova. Por seu turno, o n.º 3, do art.º 15.º, contempla a possibilidade da pesquisa de dados informáticos (armazenados em determinado sistema informático) ser efetuada pelo OPC, sem autorização judicial, em situações especiais de urgência ou *periculum in mora* e desde que, de acordo com a al. a), do n.º 3, desta disposição, voluntariamente, seja consentida a pesquisa por quem tiver a disponibilidade ou controlo dos dados específicos a pesquisar, ou quando, de acordo com a al. b), estejamos perante crimes de terrorismo, criminalidade violenta ou altamente organizada, em que existam fundados indícios da prática iminente de crime que ponha em causa a vida ou integridade de terceiros.

A natureza excecional deste regime impõe o cumprimento dos requisitos previstos no art.º 15.º, n.º 4, devendo, assim, a diligência ser imediatamente comunicada à autoridade judiciária competente, que apreciará a sua validação, devendo ser sempre lavrado um relatório da diligência (art.º 253.º do CPP). Na mesma linha de raciocínio que temos vindo a expor, cremos que o legislador atribuiu ao OPC um perigoso poder discricionário, sob a qual temos as mais prevenidas reservas, porquanto, perante uma fundada suspeita da prática de crime, pelo menos sob a forma de ensaio académico, existe um efetivo perigo do OPC atuar de forma desleal na preterição do direito de esclarecimento do suspeito (que até já poderia ser constituído arguido atendendo à suficiente prova indiciária que fora recolhida), designadamente, à informação do direito que lhe assiste de não ceder as credenciais de acesso de determinado sistema informático, convidando-o a *"auto – incriminar-se",* ainda que em manifesta violação do princípio *"nemo tenetur se ipsum accusare"*[240], forçando-se assim a sua colaboração na permissão de acesso a dados que, doutro modo, o OPC nunca teria acesso.

---

[239] RODRIGUES, Benjamim Silva, *Da Prova Penal – Tomo IV, Da Prova – Electrónico*…, p. 525.

[240] Para garantir a eficácia e reforçar a consistência do conteúdo material de tal princípio, a Lei portuguesa impõe à autoridade judiciária e aos órgãos de polícia criminal, nas declarações e depoimentos feitos pelo Arguido, o prévio dever de esclarecimento ou advertência dos direitos decorrentes deste princípio (v.g. art.ºs 58.º, n.º2, 61.º, n.º1, al.g), 141.º, n.º 4, 343.º, n.º 1, do CPP), designadamente, o direito ao silêncio, proibindo-se a prova obtida em violação de tal princípio. ANDRADE, Manuel da Costa, *Sobre as Proibições de Prova em processo Penal*, Coimbra Editora, 1.ª Edição, Reimpressão, Outubro, 2013, ISBN 978-972-32-2196-1, p. 127 e 128.

Por via do art.º 15.º, n.º 5, da LC, configurou-se, ainda, a possibilidade de estender-se a pesquisa inicial a outro sistema informático, ou parte diferente do sistema já pesquisado, permitindo-se o acesso legítimo aos dados a partir de um sistema inicial. Conforme salientam PEDRO VERDELHO, ROGÉRIO BRAVO e MANUEL LOPES ROCHA, era de particular importância esta inovação, aludindo ao facto do n.º 2, do art.º 19.º da Convenção, contemplar *"algo não previsto no direito português, embora não proibido nem contrariado"*.[241] De realçar, ainda, que nos termos do art.º 15.º, n.º 6, da LC, com remissão para as regras especiais dispostas no CPP e no estatuto do jornalista, encontra-se consagrada uma medida restritiva para as pesquisas realizadas a sistemas informáticos utilizados para o exercício da advocacia, das atividades médicas, bancárias e da profissão de jornalista[242], por serem, eles próprios, garantes de segredos de natureza profissional.

8.4. A Exigência Prévia de Despacho Judicial para a Apreensão de Correio Eletrónico

Conforme vertemos, a remissão do art.º 17.º da LC, para o regime geral da correspondência, por força da cláusula de extensão operada no art.º 11.º da LC, permitiu ultrapassar o obstáculo existente no art.º 179.º, n.º 1, al. b), do CPP, na parte que condiciona a sua aplicação à exigência de em causa estar um crime punível "*com pena de prisão superior, no seu máximo, a três anos*".

Doutro passo, pacificamente, há que reconhecer que o legislador, no próprio art.º 17.º da LC, dotou este meio de obtenção de prova digital de requisitos próprios de admissibilidade, designadamente, condicionando a diligência de apreensão ao "*decurso de uma pesquisa informática ou outro acesso legítimo a um sistema informático",* assim como ao facto das mensagens de correio eletrónico ou registos de comunicações de natureza semelhante se encontrarem *"armazenadas*", podendo o juiz autorizar ou ordenar, por despacho, *"a apreensão daqueles que se afigurem ser de grande interesse para a*

[241] VERDELHO, Pedro, BRAVO, Rogério e ROCHA, Manuel Lopes, *Leis do Cibercime – Volume I*, Centro Atlântico, 1ª edição, Julho de 2003, ISBN: 972-8426-69-0, p. 17.

[242] Sobre a proteção do sigilo profissional *Vide* ARNAUT, António*, Iniciação à Advocacia: História, Deontologia, Questões Práticas*, Coimbra, Coimbra Editora, 11ª ed. revista, 2011; CANAS, Vitalino, *O Segredo Profissional dos Advogados*, in Estudos em Memória do Professor Doutor António Marques dos Santos, coord. Jorge Miranda, Luís Lima Pinheiro, Dário Moura Vicente, Vol. II, Coimbra, Almedina, 2005.

descoberta da verdade ou para a prova", aplicando-se, correspondentemente, o regime da apreensão de correspondência previsto no CPP.

Significa isto que, paralelamente aos requisitos dispostos no art.º 17.º da LC, encontramos no próprio art.º 179.º do CPP, que vem regulamentar a diligência de apreensão de correio eletrónico, um segundo crivo e subsequente sujeição de "prova de vida", à admissibilidade da obtenção e recolha da prova digital, daqui dependendo a sua validade, consagrando, desde logo, o art.º 179.º, n.ºs 1 e 2, do CPP, o efeito da nulidade quando ocorra o desrespeito pelos requisitos aqui estabelecidos.

Denote-se que, nos termos do art.º 179.º, n.º 1, al. a), b) e c), do CPP, cumulativamente, e sob pena de nulidade, somente pode haver lugar a apreensão de correspondência se houver fundadas razões para crer que: (1) "*a correspondência foi expedida pelo suspeito ou lhe é dirigida, mesmo que sob nome diverso ou através de pessoa diversa*"; (2) "*Está em causa crime punível com pena de prisão superior, no seu máximo, a três anos*" e (3) "*A diligência se revelará de grande interesse para a descoberta da verdade ou para a prova*". Nesta esteira, dispõe o art.º 179.º, n.º 3, do CPP, que "*O juiz que tiver autorizado ou ordenado a diligência é a primeira pessoa a tomar conhecimento do conteúdo da correspondência apreendida. Se a considerar relevante para a prova, fá-la juntar ao processo; caso contrário, restitui-a a quem de direito"*, vinculando-se a um indissociável dever de segredo relativamente ao conteúdo que tiver tomado conhecimento (art.º 179.º, n.º 3, do CPP).[243]

Ora, conforme se deixou exposto, se por um lado as normas especiais do art.º 17.º e 11.º da LC, porque precisas, enquanto normas reguladoras da prova digital, nos permitem firmar que, para aplicação deste regime especial, não existe um acoplamento simétrico aos requisitos cumulativos de que depende a apreensão da correspondência, ínsitos no art.º 179.º, n.º 1, do CPP, como interpretar e conjugar a necessidade da exigência prévia – ou *quiçá* não – de despacho judicial que legitime a apreensão de mensagens de correio eletrónico? No fundo, a questão que persiste é a de saber se, de facto, sob pena de nulidade, deve prevalecer o entendimento que (1) somente com a autorização ou ordem do juiz é possível proceder à apreensão de mensagens de correio eletrónico (assim como (2) deverá ser o juiz a primeira pessoa a tomar conhecimento do conteúdo dos *e-mails*

[243] Razões de ordem prática demonstram que a "restituição" de *e-mails* deve considerar-se desadequada, pois que, verdadeiramente, os mesmos nunca deixaram de estar com a pessoa visada, tendo-se apenas procedido a uma mera cópia.

apreendidos), ou se, ao invés, pode conceber-se que, por extensão, também o Ministério Público, enquanto autoridade judiciária, pode*, per si*, legitimar a admissibilidade da diligência.

Como já se antevê, a resposta a tal paradigma não é unívoca, tendo-se revelado alvo de divergência entre a doutrina e jurisprudência, atendendo que o legislador acabou por não ser claro sobre este aspeto, obrigando o intérprete a um esforço ciclópico.

Debruçando-se sobre a matéria, já após a publicação da Lei 109/2009, de 15/09, PEDRO VERDELHO[244] vem a firmar o entendimento que a Lei não exige um prévio despacho judicial para a apreensão de mensagens de correio eletrónico armazenadas, assim como não exige que seja o juiz o primeiro a ter conhecimento destas mensagens. O Autor apoia o seu pensamento no facto das mensagens serem encontradas ou descobertas no decurso de uma pesquisa a um sistema informático, estando a investigação legitimada a proceder "*a uma apreensão cautelar de mensagens de correio eletrónico*", condicionada a um posterior despacho judicial, bastando, para tanto, na "*apreensão provisória*", a existência de um despacho, por parte da autoridade judiciária competente, que legitime a pesquisa ao sistema informático onde estas estavam armazenadas. Com efeito, conforme firma o Autor, é o próprio art.º 17.º da LC quem concede legitimidade ao OPC, sob direção e autorização do MP, para apreender mensagens de correio eletrónico, atendendo que o despacho judicial de autorização por parte do juiz será sempre posterior à apreensão das mensagens de quem conduz a investigação, reconhecendo, porém, PEDRO VERDELHO que, ainda que a Lei não exija um prévio despacho judicial para a apreensão de mensagens eletrónicas, a verdade é que a apreensão será sempre provisória e condicionada à efetiva autorização por parte do juiz. Assim, caso o juiz considere que a apreensão ocorreu à luz das exigências normativas vigentes da pesquisa informática, bem como reúna os requisitos ínsitos no art.º 17.º da LC, nomeadamente, considere que as mensagens revistam grande interesse para a descoberta da verdade material ou para a prova, deverá proferir despacho judicial a autorizar a apreensão e ordenará a sua junção ao processo. Assim não o entendendo, então não terá outro caminho senão considerar inválida a apreensão, tratando-se de meio de prova proibido, cabendo-lhe ordenar judicialmente a sua devolução ou, no caso da apreensão tiver sido feita por cópia, ordenar a sua destruição. A favor de tal entendimento, assim foi decidido nos Acórdãos do Tribunal da Relação do Porto, de 24 de

[244] VERDELHO, Pedro, *A Nova Lei do Cibercrime*…, p. 743-744.

Abril de 2013, proferido sob o Processo n.º 585/11.6PAOVR.P1[245] e do Tribunal da Relação de Lisboa, de 02 de Março de 2011, proferido sob o Processo n.º 463/07.3TAALM-A.L1-3[246].

Sustenta PEDRO VERDELHO que as mensagens de correio eletrónico, via de regra, são detetadas no decurso de uma pesquisa a um sistema informático, não se sabendo sequer, antes da realização da busca, se se vai encontrar um computador ou qualquer outro dispositivo, ou tão pouco se em tais dispositivos serão encontradas mensagens de correio eletrónico, sendo que, a ser encontradas, não é possível saber-se se existe interesse para a investigação. Nesta senda, pugna o Autor que a *"vida real revela que seria inviável um sistema oposto, que exigisse, antes de toda e qualquer busca, a obtenção de autorização judicial para a eventual possibilidade de vir a ser encontrado no decurso da busca, um computador e que tal computador contivesse registos de comunicações, e que tais comunicações fossem prova necessária à investigação do caso concreto"*[247], concluindo que não pode fazer-se outra interpretação da Lei, sob pena de *"optar-se por uma solução inviável face à grande quantidade de computadores que nos dias de hoje se apreendem",* acentuando a impossibilidade prática de se exigir que fosse exclusivamente o juiz a verificar todas as mensagens de correio eletrónico que fossem encontradas no computador. Com o devido respeito, e com a promessa de aqui voltarmos, discordamos do Autor.

Nesta esteira, ARMANDO RAMOS[248] fazendo uma minuciosa explanação da metodologia de procedimentos a adotar por peritos forenses na recolha das mensagens de correio eletrónico, armazenadas em dispositivos eletrónicos, à giza de PEDRO VERDELHO, defende uma aparente legitimidade do OPC para apreender mensagens de correio eletrónico, ainda que sem previamente estar munido de despacho de autorização do JIC, apenas relevando que, após o encapsulamento das mensagens em suporte digital adequado (CD ou DVD), sejam as mesmas remetidas ao JIC, para que seja este o primeiro delas a tomar conhecimento. De resto, o Autor pugna pelo regime das buscas como o

[245] Disponível *online* no endereço: http://www.dgsi.pt/jtrp.nsf/d1d5ce625d24df5380257583004ee7d7/872f3063233d8de480257b78003e60f3?OpenDocument [acedido em 05 de Abril de 2017].
[246] Disponível *online* no endereço: http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/d10c400a16882e9e80257853005d65c1?OpenDocument [acedido em 05 de Abril de 2017].
[247] VERDELHO, Pedro, *A Nova Lei do Cibercrime…,* p. 744.
[248] RAMOS, Armando Dias, *A Prova Digital em Processo Penal,* 2.º ed…., p. 107.

"*paradigma perdido*" a que devia ser cotejada a apreensão de correio eletrónico, independentemente do seu estado.

Por seu turno, partindo das considerações a propósito das mensagens eletrónicas abertas, lidas e armazenadas, já não protegidas pelo sigilo das comunicações, estribando-se nos ensinamentos de COSTA ANDRADE, JOÃO CONDE CORREIA caminha mais além, considerando que, neste estado, deverão equiparar-se a *"um mero documento"*. Por tal motivo, alude o Autor, é bastante para a sua apreensão "*a intervenção legitimadora do magistrado do Ministério Público (art.º 16.º da Lei n.º 109/2009). À semelhança de uma carta recebida, também o correio eletrónico aberto deverá poder ser, por ele, apreendido"*[249], defendendo que é um contra - senso invocar-se o ritualismo da apreensão de correspondência quando esta já não existe. De resto, conforme argumenta o Autor, não faz sentido privilegiar-se o correio eletrónico em relação a uma carta aberta, quando as necessidades de tutela são idênticas para ambos os casos[250], aduzindo o exemplo que *"por estranho que pareça, o Ministério Público pode apreender uma carta guardada num cofre, mas não um email guardado num computador"*.

Nesta matéria, numa breve apreciação ao art.º 17.º da LC, e no que julgamos discorrer sob algum desalinho, BENJAMIM SILVA RODRIGUES alude que o legislador foi "*infeliz*" ao contemplar na redação da norma, quer a remissão para o art.º 179.º do CPP, quer a exigência das sobreditas mensagens se afigurarem *"ser de grande interesse para a descoberta da verdade"*, realçando a problemática compatibilidade da cumulação de requisitos ínsitos na norma. Assim, assinala o Autor que a aparente permissibilidade concedida pelo art.º 17.º da LC, na apreensão de mensagens eletrónicas "*que se afigurem ser de grande interesse para a descoberta da verdade*", no decurso de "*investigações digitais*", ainda que não presididas pelo juiz, não se coaduna e harmoniza com a remissão, *in fine*, para o regime geral, nomeadamente o n.º 3, do art.º 179.º, que *"estipula um regime específico de abertura de correspondência já que somente o juiz o pode fazer e somente ele lê a correspondência e somente ele decide a sua junção. A esta luz, há aqui, nesta remissão do art.º 17.º, da LCiber 2009, para o artigo 179.º, n.º 3, do CPP, uma qualquer confusão legislativa, já que a não ser que se admita uma (desproporcional) apreensão*

[249] CORREIA, João Conde, "*Prova Digital: as leis que temos e a lei que devíamos ter*…, p. 41.

massiva dos correios eletrónicos, já que o juiz não está presente e somente se pode seleccionar após a sua leitura, então verifica-se que foi infeliz o legislador ao esquecer a regulamentação complexa do artigo 179.º, n.º 3, do CPP (…)"[251]. De resto, referindo-se ao art.º 189.º, n.º 1, do CPP, e à utilização, por parte do legislador, da expressão "*mesmo que se encontrem guardadas em suporte digital*", o Autor amplia a discussão em torno do correio eletrónico, enunciando que esta expressão abrange igualmente as mensagens de correio eletrónico ou registos de natureza semelhante do art.º 17.º da LC, o que significa, segundo o Autor, "*que há uma encruzilhada – e uma nova face oculta – nesta matéria, pois o correio eletrónico continuará a fazer o seu constrangedor e confrangedor curso, na doutrina e na jurisprudência, uma vezes como comunicação electrónica (ou antigamente "telecomunicação") a levar ao altar das escutas telefónicas, outras vezes como comunicação electrónica a levar ao altar da correspondência clássica, outras vezes como amálgama de dados a levar ao altar das escutas telefónicas e, por último, enquanto dados a implicar outros dados de tráfego e, por isso, a fazer intervir a legislação específica da Lei n.º 32/2008".*

Expostas as posições doutrinárias, e sempre com o devido respeito pela mestria e autoridade científica dos seus doutrinadores, não aderimos à corrente de pensamento que defende ser bastante a intervenção legitimadora do MP para a apreensão de mensagens de correio eletrónico, ainda que provisoriamente e de forma condicionada.

Desde logo, discordando-se de BENJAMIM SILVA RODRIGUES e ARMANDO RAMOS, não cremos que faça sentido continuar a chamar-se à colação o art.º 189.º do CPP, para a regulação da apreensão de mensagens de correio eletrónico armazenadas. Embora não esgrimam argumentos que estribem o seu raciocínio, é pacífico entre a doutrina e jurisprudência que, no plano normativo – processual, o art.º 17.º da LC operou a uma direta revogação da matriz adotada na redação do n.º 1, do art.º 189.º, do CPP, distanciando-se da extensão legal do regime das escutas, surgindo tal comando da LC como um novo e especial meio de obtenção de prova, concebido para a apreensão das mensagens de correio eletrónico armazenadas e registos de natureza semelhante, regulando-se a diligência pelo regime da correspondência do art.º 179.º do CPP. De resto, parafraseando-se COSTA ANDRADE, "*é patente a contradição entre o n.º1 do art.º 189.º do CPP e o art.º 17.º da Lei do Cibercrime*", tudo se passando "*como se os distintos*

[251] RODRIGUES, Benjamim Silva, *Da Prova Penal – Tomo II, Bruscamente*…, p. 454.

diplomas fossem obra de diferentes legisladores, incomunicavelmente separados no espaço, na história, nas concepções de fundo político-criminal e axiológico", reconhecendo-se, indelevelmente, que os *e-mails* recebidos, efetivamente lidos pelo destinatário, são passíveis de *"apreensão (acesso, leitura e cópia) nos termos normais e gozando apenas da tutela decorrente do direito de autodeterminação e da privacidade em sentido material (neste sentido o art.º 17.º da Lei 109/2009 de 15 de Setembro)*".[252]

Doutro passo, afirmar que a Lei não exige um prévio despacho judicial para a apreensão de mensagens de correio eletrónico, é, assim o julgamos, fazer uma interpretação *contra legem* do preceito em questão, colocando-se em causa o princípio da legalidade, expondo-se a prova às vicissitudes decorrentes da teoria dos frutos da árvore envenenada[253]. De tal forma, só o juiz, e apenas se considerar ser de grande interesse para a descoberta da verdade, ou para a prova, tem a exclusiva competência para autorizar (sob promoção do MP) ou ordenar (por sua iniciativa)[254] a apreensão de mensagens de correio eletrónico que se encontrem armazenadas, determinando a sua junção aos autos (*Ubi lex non distinguit nea nos distinguere debemos).* De resto, conforme SANTOS CABRAL[255], a não observância de tal exigência, sob pena de nulidade expressa absoluta, prevista no art.º 179.º, n.º 1 do CPP, reconduzirá a diligência ao regime de proibição de prova, devendo considerar-se que, nos termos do art.º 268.º, n.º1, al. d), do CPP, constitui ato da exclusiva competência do JIC ser o primeiro a tomar conhecimento do correio eletrónico já convertido em ficheiro digital.

Por seu lado, conforme já aduzido, atendendo à relação de dependência existente entre a diligência de apreensão de correio eletrónico e a pesquisa informática, não podemos perder a basilar premissa que, na pesquisa a um sistema informático, a investigação está condicionada e vinculada à obtenção de "*dados informáticos específicos e determinados"*, dispondo, ela própria, de ferramentas informático-forenses criadas para estes fins[256], testadas e utilizadas por diversas entidades policiais à escala mundial, tais como o *FBI* ou a

---

[252] ANDRADE, Manuel da Costa, *Comentário Conimbricense do Código Penal*..., p. 1098 e 1113.

[253] A teoria tem origem na doutrina americana "*fruits of the poisonous tree*" (equivalente à teoria da nódoa na doutrina alemã), tendo surgido no caso *Silverthorne lumber & Co v. United States* de 1920, estabelecendo o entendimento de que toda a prova produzida em consequência de uma descoberta obtida por meios ilícitos, estará contaminada pela ilicitude desta pelo efeito da derivação. ANDRADE, Manuel da Costa, *Sobre as Proibições de Prova em Processo Penal*..., p.175.

[254] LOBO, Fernando Gama, *Código de Processo Penal Anotado*, Almedina Coimbra, 2015, p. 305.

[255] CABRAL, Santos, *Código de Processo Penal Comentado*, in A.A. VV., Almedina Editora, 2.ª edição, 2016, p. 708.

[256] A este propósito vide MARQUES, Pedro P. Leitão da Costa, *Informática Forense*..., p. 34-87.

European Cybercrime Centre - EC3 (propriamente a nível nacional a recém criada UNC3T[257]), impondo-se apenas a apreensão dos *e-mails* que se afigurem, realmente, determinantes para a prova, segundo apertados critérios de abrangência. Por tal motivo, destacando-se o papel primordial deste meio de obtenção de prova, enquanto primeiro crivo de que depende a apreensão de *e-mails*, não concebemos que se atribua primazia às dificuldades práticas resultantes da apreensão de *e-mails* em "grandes quantidades", em detrimento dos direitos do visado. Assim, conforme RITA CASTANHEIRA NEVES, "*não há que deixar de exigir que seja o juiz o primeiro a tomar conhecimento do conteúdo do correio eletrónico pelas dificuldades práticas de atribuir a um só juiz essa tarefa"*, podendo, inclusive, o juiz, como realça RICARDO OLIVA LEÓN, ser auxiliado por um perito informático *"ajudando-o a esclarecer se houve ou não manipulação de um meio de prova eletrónico"* e apoiado por *"um prestador de serviços de certificação que o ajude a determinar a integridade dos dados*"[258].

Como se pode constatar, o art.º 17.º da LC e o art.º 179.º, n.º1, do CPP, contêm um requisito de admissibilidade comum: apenas ao juiz é conferida competência para poder autorizar ou ordenar, se entender revestir grande interesse para a descoberta da verdade ou para a prova, a apreensão de *e-mails*. Ora, se por si só, a convergência entre disposições já seria dissuasora para perfilharmos o entendimento dos doutrinadores que pugnam pela aparente competência do MP para legitimar a admissibilidade da diligência de apreensão, doutro passo, cremos que somente com a exigência do prévio despacho judicial do juiz, se acautelam os potenciais abusos cometidos pelos agentes de investigação criminal, na medida em que o resultado das diligências de apreensões revela, muitas vezes, que a investigação, com recurso a aplicações que permitem a realização de pesquisas gerais nos servidores (normalmente com obtenção de *passwords* ou sem dela estar munida), estendeu-se a dados partilhados no sistema informático comum, não abrangidos e delimitados pelo despacho judicial que autorizou a diligência, acabando por se ter acesso a ficheiros pertencentes a pessoas por ela não visadas, que nenhuma conexão têm com a matéria que se investiga nos autos, apreendendo-se *e-mails* com conteúdos da esfera

[257] Tendo sido criada pelo DL n.º 81/2016, de 28/10, a Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica está afeta organicamente à PJ, dispondo de extensões nas unidades territoriais, substituindo a Unidade Nacional da Investigação da Criminalidade Informática.

[258] OLIVA LEÓN, Ricardo, *La Prueba Electrónica Envenenada*, in *La Prueba Electrónica – Validez y Eficacia procesal*, Coordenadores Ricardo Oliva León Sonsoles Valero Barceló, Colección Desafíos Legales, 1º edição, Setembro de 2016, p. 50-67.

reservada e íntima da vida das pessoas, trazendo-se para dentro dos processos judiciais uma quantidade indeglutível de informação referente às suas compras, vendas, planificações de negócios, património, movimentos bancários, fotografias de cariz sexual, informação sobre o estado de saúde, religião, expondo-se, gratuitamente e ao livre arbítrio, a vida privada das pessoas[259].

Para além deste risco, não raras são as vezes em que o próprio OPC, no decurso da pesquisa informática, acaba por ter acesso a correio eletrónico que se encontra jacente e que ainda não foi lido pelo seu destinatário, tratando-se ainda de comunicação, e, portanto, ainda suscetível de interceção nos termos do art.º 18.º da LC. Bastará aqui pensar-se nos casos dos sistemas de armazenamento local, em que o correio eletrónico é rececionado localmente bastando-se abrir o programa a que determinada conta de correio eletrónico está configurada (exemplo Outlook). Ora, o facto é que, a volatilidade de alterar o estatuto da comunicação (por via da opção "*read"/"unread*"), coabita com a íntima possibilidade de contaminação da prova por parte da investigação, inquinando-a de nulidade. Nesta esteira, numa posição que manifestamente nos revemos, não deixaremos, à giza de RITA CASTANHEIRA NEVES[260] e NOEL MCCULLAGH[261], de avançar com a solução da encriptação[262] nas ferramentas próprias da investigação, como medida cautelar a utilizar na diligência de apreensão de *e-mails*, impermeável à arbitrariedade da investigação e aos potenciais vícios de inquinação da prova. Assim, para nós, são também as particulares

---

[259] A este propósito, num artigo publicado no jornal "*Sol*", advertiu PAULO SARAGOÇA DA MATTA para os abusos cometidos pela investigação, designadamente, exemplificando com um recente caso em que "*Além de apreenderem e desligarem, de imediato, todos os telefones dos presentes, até os que estavam nos bolsos e carteiras dos mesmos, exigiram entrar nas contas de correio eletrónico da buscada (…) Ou seja, tendo mandado de busca, resolveram fazer revista, sem que nada o autorizasse. E não contente com copiar o teor completo das contas de correio eletrónico em questão, a investigação resolveu, sem que qualquer mandado sequer o pudesse ordenar, mudar as palavras-chave das contas de e-mail, para que a titular não mais lhes pudesse aceder (…) Questão: onde está o cumprimento do que a lei manda fazer nesses casos? Não está!*". Disponível *online* no endereço https://sol.sapo.pt/artigo/552582/processo-penal-verdades-indiziveis [consultado a 16 de Abril de 2017].

[260] NEVES, Rita Castanheira, *As ingerência nas comunicações*…, p. 194.

[261] MCCULLAGH, Noel, *Securing E-Mail with Identity Based Encryption*, IT Pro, May June, EUA, 2005, p. 61-64.

[262] A sua origem linguística deriva dos termos gregos *Kryptos* que significa "ocultar" e *Graphein* que significa "representação escrita de palavras". Entende-se por "Criptografia" a área do conhecimento que estuda e desenvolve algoritmos para implementação de serviços de segurança de informação, através da ocultação do significado dos dados. Curiosamente, a própria CCiber, no seu art.º 25.º, n.º 3, já sugeria a encriptação como uma forma de assegurar a segurança e autenticação no envio de correio eletrónico. De resto, recentemente, surgiram notícias que, em determinados *Webmails*, a encriptação já é possível. Disponível *online* no endereço http://exameinformatica.sapo.pt/noticias/internet/2014-03-21-Google-passa-a-encriptar-todas-as-mensagens-do-Gmail [consultado a 3 de Junho de 2017].

características da prova digital, concretamente, a sua volatilidade, que justificam a prévia exigência de despacho do juiz que autorize ou ordene a apreensão de mensagens de correio eletrónico.

Do exposto, embora se concordando com a doutrina que acentua a negligência e promiscuidade conceptual que emerge na redação do art.º 17.º da LC, particularmente, a ilusória tentação de equiparar, por via da remissão, o correio eletrónico ao tradicional, julgamos, tal como PAULO DÁ MESQUITA, ser de aplaudir o facto de tal solução ter abandonado "*o texto do anteprojeto onde se verificava uma recuperação descontextualizada e infundada da antiga redacção do art.º 188.º, n.º 1, do CPP*", que pressuponha o acesso prévio do OPC aos conteúdos das comunicações, não nos soçobrando dúvidas que, somente com o mandado judicial emitido pelo juiz, eventualmente cumulado, quer com a autorização da busca, quer com a legitimação da pesquisa informática, pode o OPC apreender mensagens de correio eletrónico que se encontram jazidas no terminal do dispositivo eletrónico ou alojadas no servidor. Doutro passo, a perfilharmos o entendimento da doutrina que defende a legitimidade de apreensão de *e-mails* por parte do OPC, sem necessidade de prévio despacho do juiz, não vislumbramos qual a utilidade prática da coexistência do art.º 252.º, n.º 2 e 3, do CPP, ficando destituída de sentido esta diligência cautelar confiada ao OPC quanto à possibilidade de apreensão de *e-mails* no decurso de pesquisas, em casos de urgência ou perigo na demora, necessárias à conservação ou manutenção da preservação da prova, transformando-se em regra geral uma diligência que seria excecional[263].

A favor do entendimento que somente o juiz tem legitimidade para ordenar ou autorizar a apreensão de mensagens de correio eletrónico armazenadas, ou registos de natureza semelhante, *vide* acórdãos da TRL de 11 de Janeiro de 2011[264], proferido sob o

[263] Neste compasso, inclusive, sairia beneficiado o próprio meio de obtenção de prova disposto no art.º 16.º da LC, relativo à apreensão de outros dados informáticos que não fossem correio eletrónico ou registos de natureza semelhante, na medida em que, nos termos dos n.º 2 e 3, o OPC apenas poderia efectuar apreensões, sem prévia autorização da autoridade judiciária, se houvesse uma efetiva "*urgência ou perigo na demora*" que colocassem em causa a prova, devendo, no prazo de 72 horas, ser sujeita a validação pela autoridade judiciária.

[264] Disponível *online* no endereço: http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/e5ed1936deb44eb180257824004ab09d?OpenDocument [acedido em 02 de Janeiro de 2017].

Processo n.º 5412/08.9TDLSB-A.L1-5, do TRG, de 29 de Março de 2011[265], proferido sob o Processo n.º 735/10.0GAPTL – A.G1 e do TRP, de 07 de Julho de 2016[266], proferido sob o Processo n.º 2039/14.0JAPRT.P1.

De facto, cremos que, teleologicamente, a criação do novo art.º 17.º da LC materializou-se no reconhecimento, por parte do legislador, dos dois momentos do correio eletrónico: O momento em que a mensagem de *e-mail* jaz no terminal ou servidor do destinatário, ainda que por si não acedida, e o momento em que, por aberta e lida, cessou tal comunicação. Ora o facto é que, ainda que aberto, lido e armazenado, em nome da salvaguarda da privacidade da autodeterminação informacional, não deixa o destinatário de ficar desapossado de uma proteção adicional em relação a outros suportes digitais que podem ser apreendidos, acabando o legislador, deliberadamente, por colocar em pé de desigualdade o grau de proteção conferido aos meios de obtenção de prova que têm por objeto ficheiros informáticos, resultantes de correio eletrónico, e os meios de obtenção de prova que têm por objeto escritos, resultantes de comunicações postais.

[265] Disponível *online* no endereço: http://www.dgsi.pt/jtrg.nsf/86c25a698e4e7cb7802579ec004d3832/6aa96edf91e899b2802578a00054631f?OpenDocument [acedido em 05 de abril de 2017].
[266] Disponível *online* no endereço: http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/cffe710b2cb8d91e8025800500475ea9?OpenDocument [acedido em 03 de Março de 2017].

9. O Art.º 18.º da LC – A Interceção do Correio Eletrónico

9.1. A Interceção dos Dados Informáticos em "Trânsito"

Com a entrada em vigor da LC, concretamente, no seu art.º 18.º, produto da transposição das medidas processuais compreendidas nos art.ºs 20.º e 21.º da CCiber, consagrou o legislador um regime específico para a interceção[267] de comunicações eletrónicas, corrigindo-se, conforme BENJAMIM SILVA RODRIGUES[268], "*uma falha tremenda, existente na legislação anterior, que não permitia lançar-se mão do regime das escutas telefónicas, para a investigação da principal criminalidade informático – digital*", ultrapassando-se a difícil encruzilhada a que a prova digital vinha sendo submetida pelo caráter deficitário do regime das escutas telefónicas. De resto, conforme exposição de motivos da Proposta de Lei n.º 289/X/4ª, justificar-se-ia a criação de uma norma especial que permitisse "*superar o actual regime",* guarnecendo-se o sistema processual penal de *"normas que permitam a obtenção de dados de tráfego e a realização de intercepções de comunicações em investigações de crimes praticados no ambiente virtual*".

De tal forma, com este novo meio de obtenção da prova digital, nos termos do art.º 18.º da LC, passaria a ser possível intercetar as comunicações eletrónicas relativamente aos crimes: "a) *Previstos na presente lei;* ou b) "*cometidos por meio de um sistema informático ou em relação aos quais seja necessário proceder à recolha de prova em suporte electrónico, quando tais crimes se encontrem previstos no artigo 187.º do Código de Processo Penal*".

O art.º 18.º da LC coloca-nos, assim, perante uma medida que se insere, à giza do que sucede com as ações encobertas, as gravações/filmagens entre presentes (no domicílio ou fora dele), a videovigilância, ou as próprias buscas *online*, nos chamados métodos ocultos de investigação, entendidos, nas palavras de COSTA ANDRADE, como verdadeiras intromissões *"nos processos de acção, interacção e comunicação das pessoas concretamente visadas, sem que estas tenham conhecimento do facto nem dele se apercebam (…)"*[269]*,* implicando uma renúncia ao *privilege against self-incrimination*,

[267] A LC, no seu art.º 2.º, al. e), define a "intercepção" como *"o acto destinado a captar informações contidas num sistema informático, através de dispositivos electromagnéticos, acústicos, mecânicos ou outros"*.

[268] RODRIGUES, Benjamim Silva, *A Monitorização dos Fluxos Informacionais e Comunicacionais*…, p. 532.

[269] ANDRADE, Manuel da Costa, *Bruscamente no verão passado*…, p. 105.

originando potenciais lesões ao princípio *nemo tenetur se ipsum acusare*, permitindo a obtenção *"fraudulenta de ´confissões´ inconscientes e, como tais, não livres",* sacrificando, em si mesmo, um conjunto de bens jurídicos como a "*privacidade/intimidade, palavra, imagem, sigilo profissional, inviolabilidade do domicilio, segredo de Estado, sigilo das telecomunicações, confidencialidade e integridade dos sistemas técnico-informacionais e autodeterminação informacional*".[270]

Há que notar que a nova interceção e registo de transmissões de dados de conteúdo, e/ou dados de tráfego, paralelamente à exigência da diligência somente poder ser autorizada na pendência do inquérito (art.º 18.º, n.º 2, da LC), comporta, igualmente, a premissa que tal interceção seja realizada em tempo real, isto é, que a mensagem de correio eletrónico, ainda em curso, não tenha sido aberta e lida pelo seu destinatário, revestindo-se assim, *in nomine,* ainda de comunicação. De resto, nas palavras de PEDRO VENÂNCIO, falamos da interceção de mensagens de correio eletrónico em tempo real, referindo-nos ao ato de interferir no *"seu trajecto do computador do emissor para o computador do receptor através da rede de servidores",* interceção esta que pode ocorrer em *"mensagens trocadas através de processos de comunicação instantânea (usualmente designados por serviços de "chat", como são os casos do "IRC", do "MSN Messenger", ou do "ICQ*".[271]

De tal forma, em substância, apenas nesta disposição da LC está disciplinada, verdadeiramente, a possibilidade das comunicações eletrónicas serem alvo de ingerência por parte da investigação (nomeadamente a possibilidade do processo comunicativo ser idóneo aos "grampos"), encontrando-se, quer os dados de conteúdo, assim como os dados relacionados com a comunicação, protegidos pelo direito à privacidade e a coberto da garantia constitucional do direito à inviolabilidade do sigilo das comunicações, plasmado no art.º 34.º da CRP. Ora, equivale isto dizer, todo o correio eletrónico que já tenha cumprido a sua função junto do destinatário, que recebeu e leu integralmente a mensagem, apresenta-se como um ficheiro informático insuscetível de ser intercetado pelo comando do art.º 18.º da LC. Doutro passo, há que reconhecê-lo, é a própria LC, através da consagração de vários meios de obtenção de prova, designadamente, os art.ºs 14.º

[270] A este propósito, pugna COSTA ANDRADE que, para além da observância de outros pressupostos materiais e da exigência de cariz orgânico - procedimental (reserva de juiz), o princípio da subsidiariedade "*veda o recurso a um qualquer meio oculto de investigação sempre que seja possível lançar meio menos gravoso e igualmente idóneo para a prossecução dos interesses da investigação"*. ANDRADE, Manuel da Costa, *Bruscamente no verão passado*…, p. 106 e 107.

[271] VENÂNCIO, Pedro Dias, *Lei do Cibercrime: Anotada e Comentada*…, p. 119.

(*Injunção para apresentação ou concessão do acesso a dados*), 15.º (*pesquisa e apreensão de dados informáticos*), 16.º (*Apreensão de dados informáticos*), e propriamente o art.º 17.º, quem acaba por criar desequilíbrios nas exigências legais que devem presidir às diligências de acesso e obtenção dos dados informáticos. De tal forma, é emergente na Lei 109/2009 um tratamento diferenciado para os dados informáticos que já se encontram armazenados e que, por tal motivo, não colocam em causa a comunicação, daqueles outros que ainda estão "incorporados" numa mensagem eletrónica suscetível de ser alvo de interceção, porque ainda em transmissão, reconhecendo-se assim diferentes graus de proteção constitucional e, concomitantemente, distintos requisitos de admissibilidade na obtenção dos mesmos.

Por seu turno, conforme resulta da conjugação dos n.ºs 2 e 3, do art.º 18.º da LC, na interceção e registo de transmissão de dados informáticos, impõe-se que apenas o JIC, mediante requerimento do MP, possa autorizar a ingerência na comunicação, se "*houver razões para crer que a diligência é indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter"*, estando o juiz vinculado a um dever de fundamentação do despacho judicial de acordo com as necessidades concretas da investigação.

Questão controversa, alvo de discussão no seio da doutrina e da jurisprudência, é o sentido prático da remissão ínsita no art.º 18.º, n.º 4, da LC, que manda aplicar a este regime, em tudo o que não lhe for contrariado, o regime da intercepção e gravação de conversações ou comunicações telefónicas, constante dos art.ºs 187.º, 188.º e 190.º do CPP. Com efeito, com a entrada em vigor do regime consagrado pelo art.º 18.º da LC, divide-se o pensamento jurídico na aplicação do regime processual a aplicar à interceção de comunicações eletrónicas. Assim, questiona-se se o art.º 18.º da LC revogou a cláusula de extensão ínsita no art.º 189.º do CPP ou se, ao invés, não deixará de prevalecer o entendimento que, é a partir da cláusula de extensão do art.º 189.º do CPP, que continua a ser possível intercetar as comunicações eletrónicas. Expondo as duas teses em confronto, debrucemo-nos sobre a contenda.

9.2. O Art.º 18.º da LC e a (In)Adequação à Cláusula de Extensão Prevista no Art.º 189º do CPP

Conforme temos vindo a aludir, com a entrada em vigor da LC, nasceram novos meios de obtenção da prova digital, acabando este diploma por erigir um regime rejuvenescido no direito processual penal, vocacionado para a obtenção da prova eletrónica (art.ºs 11º a 19º), concluindo-se que, *prima facie*, haveria de tornar-se extremamente complexa a harmonização destas normas especiais, com a previsão geral dos art.ºs 187.º a 190.º do CPP.

Nesta esteira, valendo-nos das considerações feitas a propósito do regime processual penal das escutas telefónicas, fará sentido recordar que os art.ºs 187.º a 189.º do CPP de 1987 (alterado pela Lei 59/98, de 25/08), continham, desde início, uma norma de extensão – no então art.º 190º - concebida para a interceção das conversações telefónicas, não aprazadas às complexas comunicações eletrónicas estabelecidas por via das redes informáticas. Tal norma de extensão, veio, posteriormente, com as alterações introduzidas pela Lei n.º 48/2007, de 29/08, a sedear-se no artigo 189.º do CPP (transitando a nulidade do art.º 189º para o art.º 190º), passando tal disposição a alargar, consideravelmente, a aplicação do regime das escutas a outras realidades ali previstas, incluindo, a conversação entre presentes, tendo este comando normativo abrangido e disciplinado a obtenção dos dados informáticos resultantes de "conversações e comunicações", materializando-se numa cláusula de extensão com profundas dissimetrias conceptuais. Nesta evolução – que aqui pretendemos delimitar apenas à vertente da interpretação histórica – é essencial notar que a revisão do CPP de 2007, encarou os crimes e a regulação da prova de crimes informáticos de forma profundamente superficial e lacunosa.

Denote-se que a considerável extensão, consagrada no art.º 189.º do CPP, nos doutos ensinamentos de COSTA ANDRADE e FARIA COSTA, vem tornar o regime das escutas telefónicas, estruturado para disciplinar o "artefacto" telefone, o regime afluente de realidades para as quais não foi pensado, emaranhando-se com novas realidades que não se coadunavam com a tal "*palavra falada*" que emergiu à criação deste regime de obtenção de prova, acabando esta "*casa dos horrores hermenêuticos*" por se revelar uma autêntica "manta de retalhos*",* antevendo-se, desde logo, uma problemática harmonização desta disposição em simultâneo com a vigência de dois importantes diplomas legais, posteriores

à reforma ao CPP de 2007: Primeiro a Lei n.º 32/2008, de 17/07 e, sobretudo, a irreverente Lei 109/2009, de 15/09.

Nesta linha de pensamento, em rigor cartesiano, trazendo-se à colação a exposição de motivos da Proposta de Lei n.º 289/X/4ª, não há que deixar de realçar que o art.º 18.º da LC, separando "*o trigo do joio*", consubstancia-se num novo e autónomo regime de prova, especialmente instrumentalizado para a interceção e registo de transmissões de dados informáticos, sistematizado para os crimes informáticos, designadamente, a recolha e obtenção da prova digital, não diluído e confundido com as disposições dos art.ºs 187.º a 190.º do CPP. De tal forma, é inevitável partir da premissa que o art.º 11º da Lei 109/2009, numa leitura confirmada pelos n.ºs 1 e 4, do seu art.º 18.º, constitui uma disposição chave, na medida que permite uma desconstrução de aparências.

Ora, com isto, pretendemos desde logo firmar, de forma estanque e sem nos soçobrarem dúvidas, que, nas disposições do Capítulo III, da LC, o conceito de "intercepção" em tempo real de comunicações, abrangendo os dados de tráfego e de conteúdo, acaba por servir como um verdadeiro elemento distintivo entre os regimes processuais dispostos nos art.ºs 11.º a 17.º da LC (referentes a dados informáticos que se encontram armazenados) e o regime previsto no art.º 18.º da LC (onde falamos de intercetar em tempo real os dados de tráfego e de conteúdo), só saindo legitimada a diligência disposta no art.º 18.º da LC, à semelhança do que ocorre nos art.º 16.º, n.º 3, e 17.º deste diploma, com a necessária intervenção do juiz.

Assim, no que à interceção de comunicações eletrónicas diz respeito, a leitura da Lei 109/2009 não pode iniciar-se e bastar-se com o seu art.º 18º, n. 1, al. b), sob pena de se cair na tentação de considerarmos que o art.º 18.º apenas se aplica aos crimes previstos no art.º 187º do CPP, quando, afinal, a interpretação sistemática da norma impõe que se faça notar que, por via da al. a), a interceção de comunicações passou a ser admissível a todos os crimes tipificados na LC, forçando-nos a concluir que o art.º 189.º do CPP nunca é aplicável à interceção de comunicações de crimes informáticos, atendendo que, relativamente a estes, existe agora a nova disposição consagrada no art.º 18.º da LC, não obstante, conforme consigna a Relatora Desembargadora ALDA TOMÉ CASIMIRO, em Acórdão do TRL, de 22.01.2013, subsistir um *"desprezo da praxis sobre a sua existência,*

que apenas é explicável pelo efeito de atracção, quase hipnótico e excludente, que é exercido pelos artigos 187.º a 190.º do C.P.P."[272].

De tal forma, analisando o sentido e utilidade prática da remissão ínsita no art.º 18.º, n.º 4, da LC, que manda aplicar a este regime, em tudo o que o que não lhe for contrariado, o regime das escutas telefónicas, constante dos art.ºs 187.º, 188.º e 190.º do CPP, vem sendo defendido por RITA CASTANHEIRA NEVES[273], numa posição que nos revemos, que a remissão para o catálogo de crimes previsto no n.º 1, do art.º 187.º do CPP, não se concretiza, desde logo, por via do n.º 4, do art.º 18.º da LC, mas sim da al. b), do n.º 1, do art.º 18.º, que consagra expressamente o âmbito de aplicação da norma a todos os crimes do art.º 187.º, n.º1, do CPP, quando "*cometidos por meio de um sistema informático ou em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico*". Neste esteio, prossegue a Autora, o sentido da remissão do art.º 18.º, n.º4, para o art.º 187.º do CPP, materializa-se no facto de, para além dos requisitos enunciados no próprio art.º 18.º, n.ºs 2 e 3, da LC[274], se exigirem, adicionalmente, os pressupostos de admissibilidade constantes nos n.ºs 2 a 8, do art.º 187.º do CPP, devidamente adaptados[275], e na medida que não contrariem o preceito da LC. Doutro passo, serão aplicáveis à interceção de comunicações, no âmbito da criminalidade tipificada no art.º 18.º da LC, na medida em que não o contrariem, as formalidades previstas no art.º 188.º do CPP,

[272] Disponível *online* no endereço: http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/7bd2dd8af10b34c380257b27003a5697?OpenDocument [acedido em 15 de abril de 2017].

[273] NEVES, Rita Castanheira, *As Ingerências nas comunicações eletrónicas…,* p. 279.

[274] Apenas durante o inquérito, e mediante requerimento do MP, pode o JIC, por via de despacho fundamentado, autorizar a interceção e registo de transmissões de dados informáticos, se houver razões para crer que a diligência é indispensável para a descoberta da verdade, ou que a prova seria impossível ou muito difícil de obter de outra forma.

[275] Nesta matéria, a interceção e registo de comunicações eletrónicas só pode ser autorizada contra (1) suspeito ou arguido, (2) pessoa que sirva de intermediário (relativamente à qual haja fundadas razões para crer que recebe ou transmite mensagens destinadas ou provenientes de suspeito ou arguido) ou (3) vítima de crime, mediante o respetivo consentimento, efetivo ou presumido (art.º 187.º, n.º 4, al. a) b) e c)), sendo proibida a interceção e a gravação de comunicações entre o arguido e o seu defensor (art.º 187.º, n.º 5). Por seu turno, a interceção e registo de comunicações são autorizadas pelo prazo máximo de três meses, renovável por períodos sujeitos ao mesmo limite, e desde que se verifiquem os respectivos requisitos de admissibilidade (art.º 187.º, n.º 6). Sem prejuízo do disposto no artigo 248.º, o registo de comunicações só pode ser utilizada em outro processo (em curso ou a instaurar), se tiver resultado de interceção de meio de comunicação utilizado por pessoa referida no n.º 4, do art.º 187.º, e na medida em que for indispensável à prova de crime abrangido pelo n.º 1, do art.º 18.º da LC (art.º 187.º, n.º 7). No que respeita aos registos das comunicações e aos despachos que fundamentaram as respetivas interceções, mediante despacho do juiz, são juntos ao processo em que devam ser usados como meio de prova (art.º 187.º, n.º 8, do CPP).

nomeadamente, as relacionadas com a transcrição[276] das comunicações, adaptando-se esta redação às comunicações eletrónicas escritas, motivo pela qual todos os requisitos de admissibilidade e de forma, dispostos nos art.ºs 187.º e 188.º do CPP, deverão ser observados, sob pena dos efeitos da nulidade disposta no art.º 190.º do CPP.

Já em relação à harmonização do art.º 18.º da LC, com o art.º 189.º do CPP, a Autora é perentória ao firmar que não existe nenhuma remissão para o art.º 189.º do CPP. Assim, conforme RITA CASTANHEIRA NEVES, "*nem podia"*, pois que *"o artigo 18.º da Lei do Cibercrime, substitui quase por completo aquele artigo da lei penal adjectiva, no âmbito, claro está, da criminalidade definida ao nível do seu n.º1"*. Significa isto que, a interceção e o registo de transmissões de correio eletrónico, "*em todas as investigações em que esteja em causa um crime informático ou um crime do art.º 187.º mas em que haja necessidade de recorrer à recolha de prova em suporte electrónico, far-se-á, não directamente segundo o regime das escutas telefónicas, com base na remissão estabelecida no art.º 189.º do Código de Processo Penal, mas já por aplicação das regras definidas na nova Lei do Cibercrime"*[277] . A Autora conclui referindo que "*sobra pouco campo de aplicação para o art.º 189.º*" do CPP, sustentando que, com a entrada em vigor da Lei n.º 109/2009, é esta Lei que disciplina agora toda a obtenção da prova informática, acabando por ficar "*esvaziado o âmbito de aplicação do artigo 189.º do Código de Processo Penal, na parte relativa a comunicações electrónicas*".

No mesmo sentido da Autora caminha BENJAMIM SILVA RODRIGUES[278]. Assim, tecendo um rasgado elogio à técnica remissiva adotada pelo legislador, que adjetiva de "cautelosa", firma a convicção que a mesma surge em resultado das críticas que vinham sendo tecidas no que respeita à interceção de dados, considerando que, até então, o regime de extensão consagrado no art.º 189.º do CPP apenas se restringia às formas de comunicação oral, pelo facto de estar teleologicamente orquestrado para a captação da palavra falada, não deixando o Autor de alertar, contudo, para os perigos de se ver no novo

[276] Através da cópia dos conteúdos selecionados para suportes autónomos, o OPC, nos termos do art.º 188.º, n.º1, do CPP, "*lavra o correspondente auto e elabora relatório no qual indica as passagens relevantes para a prova"*, descrevendo, de "*modo sucinto o respectivo conteúdo*", explicando "*o seu alcance para a descoberta da verdade*", levando-os, nos termos do n.º 3, "*ao conhecimento do Ministério Público, de 15 em 15 dias a partir do início da primeira intercepção"*, para que este, por sua vez, "*no prazo máximo de quarenta e oito horas*", e de acordo com o n.º 4 da referida disposição, os leve ao conhecimento do JIC para validação.

[277] NEVES, Rita Castanheira, *As Ingerências nas comunicações eletrónicas…*,p. 285.

[278] RODRIGUES, Benjamim Silva, *Da Prova Penal – Tomo II, Bruscamente…*, p. 532.

art.º 18.º da LC, uma qualquer espécie de interceção do processo comunicativo em "*ações preventivas* ou *proactivas de investigação criminal"*, impondo-se circunscrever o seu âmbito.

No mesmo trilho dos aludidos Autores, vem considerando PAULO DÁ MESQUITA que, *"apesar de o legislador de 2009 não ter alterado, de forma expressa, o disposto no art.º 189.º, n.º 1, do CPP, envergonhadamente veio a confiná-lo implicitamente através do art.º 18.º da Lei do Cibercrime que regula o recurso à intercepção e registo de comunicações. E se dúvidas houvesse sobre a revogação parcial do n.º 1 do art.º 189.º do Código de Processo Penal, as mesmas dissipavam-se com o teor do n.º 4 do art.º 18.º da lei do cibercrime, em que se sublinha que os regimes dos arts. 187.º, 188.º e 190.º daquele código apenas são aplicáveis «em tudo o que não for contrariado pelo presente artigo»"*[279], extraindo-se que foi intenção do legislador não contemplar na remissão o art.º 189.º do CPP. De resto, salienta o Autor que, face ao novo regime do art.º 18.º da LC, *"o art.º 189.º do CPP encontra-se restringido nos seguintes termos: O disposto nos arts. 187.º e 188.º é correspondentemente aplicável à intercepção das comunicações entre presentes e outros meios à distância que não constituam comunicações electrónicas ou transmissões de dados informáticos",* afiançando que, com a autonomização do regime de prova ínsito no art.º 18.º da LC, terá o legislador pretendido demarcar balizas entre desiguais meios de comunicação: o telefone (disciplinado pelo regime das escutas) e os demais meios de comunicações eletrónicas, onde, claro está, incluído o correio eletrónico[280].

Também para JOÃO CONDE CORREIA[281] parece inquestionável que*, "primeiro a Lei n.º 32/2008 e depois a Lei n.º 109/2009, revogaram, tacitamente, parcelas importantes do regime consagrado no art.º 189.º do Código de Processo Penal*", salientando a "*perniciosidade*" do facto do legislador não ter revogado, formalmente, tal normativo, "*expurgando-o daquilo que não tem aplicação e impedindo que se continue a invocar a sua vigência.*" Tal rutura é também reconhecida por PEDRO DIAS

[279] MESQUITA, Paulo Dá, *Processo Penal, Prova e Sistema Judiciário*…, p. 104 e 105.
[280] O Autor considera que as interceções de comunicações, em que a transmissão de dados ocorre através de *modems*, ainda que os equipamentos operem na rede telefónica (v.g. fax), são subsumíveis ao art.º 18.º da LC. MESQUITA, Paulo Dá, *Processo Penal, Prova e Sistema Judiciário…,* p. 103.
[281] CORREIA, João Conde, *Prova Digital: as leis que temos e a lei que devíamos ter*…, p. 36.

VENÂNCIO[282], justificada à luz do conflito existente entre a prova digital e as tradicionais escutas telefónicas.

De resto, chamando à colação o entendimento jurisprudencial, designadamente, os Acórdãos do TRE, de 06 de Janeiro de 2015[283] (proferido sob o Processo n.º 6793/11.2TDLSB-A.E1), do TRL, de 22 de Janeiro de 2013[284] (proferido sob o Processo n.º 581/12.6PLSNT-A.L1-5), e do TRC, de 04 de Fevereiro de 2015[285] (proferido sob o Processo n.º 73/14.9JALRA-A.C1), viriam tais arestos a firmar posição a favor do entendimento que o art.º 18.º da LC, tacitamente, revogou o art.º 189.º do CPP.

Em "contramão", defendendo a manutenção da aplicabilidade do art.º 189.º do CPP, e aduzindo que o novo art.º 18.º da LC constitui uma extensão ao regime geral de obtenção de prova disposto no CPP, caminha PEDRO VERDELHO. Assim, servindo-se do argumento que muito antes da publicação da LC, o CPP já previa uma extensão do regime das interceções telefónicas a outras comunicações, como são as eletrónicas, o Autor defende que o art.º 189.º do CPP permanece vigente já que não foi revogado pela LC, sendo que *"aquilo a que esta última procedeu foi à instituição de um regime especial, destinado a ser aplicado em casos específicos, como resulta do art.º 11.º."*[286] Assim, para o Autor, deverá concluir-se que o novo meio de obtenção de prova, previsto no art.º 18.º da LC, tem "*o seu âmbito limitado*", visando apenas a regulação de interceções de comunicações em investigações relativas aos crimes informáticos, catalogados neste

---

[282] VENÂNCIO, Pedro Dias, *Lei do Cibercrime*…, p. 119.

[283] De entre o extenso sumário deste aresto destacamos três importantes conclusões: *"1. As Leis nº 32/2008, de 17-07 e 109/2009, de 15-09 (Lei do Cibercrime) revogaram a extensão do regime das escutas telefónicas, previsto nos artigos 187º a 190º do Código de Processo Penal, às áreas das "telecomunicações electrónicas", "crimes informáticos" e "recolha de prova electrónica"; 10 - Face à Lei nº 109/2009 devem ter-se em consideração três catálogos de crimes: a - o catálogo de crimes do n. 1 do artigo 11º da Lei 109/2009 como pressuposto de aplicação do regime processual contido nos artigos 11º a 17º dessa Lei; b - o catálogo de crimes do n. 1 do artigo 18º da Lei 109/2009 como pressuposto de aplicação do regime processual contido nesse artigo 18º e no 19º dessa Lei; c - o catálogo de crimes do n. 1 do artigo 187º do Código de Processo Penal, por remissão expressa da Lei 109/2009, como pressuposto de aplicação do regime processual contido nesse artigo 18º e no 19º dessa Lei para os crimes previstos na al. b) do artigo 18º. 12 - O artigo 189º do Código de Processo Penal nunca é aplicável a crimes informáticos, seja qual for o catálogo aplicável."* Disponível *online* no endereço http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/847dae6b85353cb880257de10056ff4c?OpenDocument. [acedido em 11 de Maio de 2017].

[284] Disponível *online* no endereço: http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/7bd2dd8af10b34c380257b27003a5697?OpenDocument [acedido em 13 de Maio de 2017].

[285] Disponível *online* no endereço: http://www.dgsi.pt/jtrc.nsf/8fe0e606d8f56b22802576c0005637dc/85a30a1f50f67a2780257de8004fd90b?OpenDocument [acedido em 15 de Maio de 2017].

[286] VERDELHO, Pedro, *A Nova Lei do Cibercrime*…, p. 746 e 747. VERDELHO, Pedro, *Lei do Cibercrime*, in AA. VV., *Enciclopédia de Direito e Segurança*, Coord. Jorge Bacelar Gouveia e Sofia Santos, Almedina, 2015, p. 255-263.

específico diploma, colmatando uma lacuna existente no art.º 187.º do CPP onde tais crimes não eram consagrados. De tal forma, o regime do art.º 189.º do CPP manter-se-á em vigor para todos os restantes casos, sendo através do recurso a esta cláusula de extensão, prevista no CPP de 2007, que continuará a ser possível intercetar os crimes catalogados no art.º 187.º do CPP, nomeadamente, quando os meios utilizados na prática de algum dos crimes aqui tipificados forem as comunicações eletrónicas de que seja necessário recolher prova digital. Doutro passo, o sentido da remissão consagrada no art.º 18.º, n.º 4, da LC, para o regime das escutas, foi "*transpor para o ambiente digital o mecanismo da intercepção de comunicações previsto no Código de Processo Penal*", recorrendo à sua regulamentação específica.

A tal pensamento, e na senda que o art.º 18.º da LC não revogou o art.º 189.º do CPP, adere PAULO PINTO DE ALBUQUERQUE[287] vincando o facto das "*insuficiências da Lei n.º 48/2007 no tocante à investigação dos crimes informáticos ou cometidos por via informática"* não terem sido *"supridas pelo artigo 18.º da Lei 109/2009, de 15/09*". De resto, ainda que em contra – senso, conforme aduzido *infra*, o Autor pugna que *"a lei nova prevê a intercepção de comunicações (incluindo dados sobre o conteúdo das comunicações e/ou dados de tráfego) para prova de crimes previstos na referida lei, de crimes cometidos por meio informático ou em relação aos quais seja necessário proceder à recolha de prova em suporte electrónico (isto é, quaisquer crimes, independentemente da sua tipicidade), mas somente quando tais crimes se encontrem previstos no artigo 187.º do Código de Processo Penal, isto é, quando os crimes sejam puníveis com pena máxima superior a 3 anos de prisão*",[288] valendo tal restrição, "*quer para a al. a), quer para a al. b)*" do art.º 18.º LC. Indagando sobre a possibilidade de, por interpretação extensiva ou analógica, se considerar incluído no catálogo dos crimes elencados no n.º1, do art.º 187º do CPP, o crime de difamação, por equiparação ao crime de injúria, que consta da al. e), o Autor não só se pronuncia pela sua exclusão, como vai mais longe ao concluir que *"o juiz não pode, em face do artigo 18.º da Lei 109/2009, ordenar a intercepção de comunicações*

[287] ALBUQUERQUE, Paulo Pinto, *Comentário ao Código de Processo Penal*, 4º Edição Atualizada, Universidade Católica Editora, Lisboa 2011, p. 525 e 549.

[288] Idêntico entendimento foi perfilhado nos Acórdãos do TRE, de 13 de Novembro de 2012, proferido sob o Processo n.º 315/11.2PBPTG-A.E1 (disponível *online* no endereço http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/d147ed8908009d4980257de10056f9c9?OpenDocument - acedido em 20 de Maio de 2017), da Relação de Guimarães, de 29 de Março de 2011, proferido sob o Processo n.º 735/10.0GAPTL – A.G1 e da Relação de Lisboa, de 11 de Janeiro de 2011, proferido sob o Processo n.º 5412/08.9TDLSB-A.L1-5. Ambos disponíveis *online* no endereço www.dgsi.pt [acedidos em 21 de Maio de 2017].

para prova dos crimes de ameaças e injúrias cometidos pelo correio electrónico"[289], ancorando-se ao princípio da legalidade para justificar a exclusão das bagatelas penais[290], responsabilizando o legislador por ter pervertido o regime das escutas para fins que nada têm a ver com a obtenção de prova, mas tão só a captura do agente do crime em manifesta violação dos princípios da proporcionalidade e da adequação.

No mesmo sentido, desconsiderando o facto das mensagens se encontrarem abertas ou fechadas, e atribuindo pouca relevância à existência do art.º 18.º da LC, parece caminhar ARMANDO RAMOS, ao considerar que *"quando se interceta a troca de mensagens, através do correio eletrónico, já serão os OPC's, no desenvolvimento dessa investigação por despacho do JIC, que tomam conhecimento em primeiro lugar deste tipo de correspondência, conforme regime estipulado no art. 188.º, ex vi 189.º, ambos do CPP."*[291]

Com o devido respeito, discordamos dos Autores que pugnam pela manutenção da aplicação do famigerado art.º 189.º do CPP.

Desde logo, julgamos que os seus defensores fazem uma interpretação bastante restritiva do art.º 18.º da LC, que não se coaduna com o aduzido condicionalismo da sua aplicação depender, *sine qua non*, que em causa estejam crimes puníveis com pena máxima superior a 3 anos de prisão. De resto, a vingar tal tese, atendendo à sua moldura legal, seria incompreensível a inadmissibilidade de se poderem intercetar, como vem defendendo PAULO PINTO ALBUQUERQUE, os crimes de dano relativo a programa informático (art.º 4.º da LC), acesso ilegítimo (art.º 6.º da LC), intercepção ilegítima (art.º 7.º da LC) ou mesmo de reprodução ilegítima de programa protegido (art.º 8.º da LC).

Como tal, a perfilhar-se tal entendimento, para além de uma interpretação *contra legem* do preceito em causa, acabaria por se semear o pânico entre os operadores

---

[289] Neste mesmo sentido TEIXEIRA, Carlos Adérito, *Escutas Telefónicas: a mudança*…, p. 284.

[290] De entre decisões judiciais que fomentam a aplicabilidade do art.º 189.º do CPP, sustentando a inadmissibilidade de intercetação de comunicações eletrónicas e obtenção dos respectivos dados de tráfego para prova dos crimes de injúrias, de ameaças, de coação e de devassa da vida privada, cometidos por meio de correio eletrónico - *Vide* Ac. do TRE, de 13 de Novembro de 2012, proferido sob o Processo n.º 315/11.2PBPTG-A.E1, estabelecendo que "*Estando em causa investigação por crime de difamação através da internet, não é admissível o acesso a dados de tráfego, por via de autorização judicial, dado que tal ilícito não consta, nem do catálogo previsto no art. 187.º do CPP, nem da definição de crime grave do art. 2.º, n.º 1, alínea g), da Lei n.º 32/2008, de 17.07*". Disponível *online* no endereço http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/d147ed8908009d4980257de10056f9c9?OpenDocument [acedido em 19 de Maio de 2017]

[291] RAMOS, Armando Dias, *A Prova Digital …,* 1.º ed., p. 42. De realçar que, não obstante o Autor ter atualizado esta obra em 2017, manteve a sua posição.

judiciários, dada a inadmissibilidade de, na sua esmagadora maioria, se poder intercetar um elevado tipo de crimes informáticos tipificados na Lei do Cibercrime e, assim, obter prova digital que se revelasse indispensável à descoberta da verdade material.

É certo que os hábitos impuseram um recurso sistemático ao art.º 189.º do CPP, e que o seu abandono, bem como aceitação da ideia de que esta disposição passa a ser praticamente dispensável, é difícil de aceitar. Todavia, de forma profundamente assumida, é a fina leitura da própria redação da norma, espelhada, de resto, na própria exposição de motivos da sua consagração, que nos confirmam o silogismo do legislador.

Assim, desde logo, é patente que no art.º 18.º, n.º 1, al. a), da LC, a interceção não está dependente ou condicionada a uma moldura penal abstrata ou de enumeração num qualquer catálogo. De resto, isso mesmo se depreende pelo facto do legislador ter autonomizado as alíneas a) e b), do aludido preceito, separando-os com recurso a uma sistematização disjuntiva, contemplando a existência de dois catálogos: os crimes previstos na LC e os crimes tipificados no art.º 187.º do CPP, quando cometidos por meio de um sistema informático ou relativamente aos quais seja necessário recolher a prova em suporte eletrónico[292]. Depois, porque a remissão da al. b), do n.º1, do art.º 18.º da LC, para o catálogo de crimes decorrente do art.º 187.º do CPP, deverá incluir os crimes de injúria, ameaça, coação ou devassa da vida privada cometidos por via de sistemas informáticos[293], operando-se a uma adaptação da investigação ao mundo do crime digital, o que contraria a tese preconizada por PEDRO VERDELHO e PAULO PINTO DE ALBUQUERQUE, que pugnam pela impossibilidade de intercetar as comunicações eletrónicas de ilícitos desta natureza. De resto, como destaca JOÃO CONDE CORREIA, o *"sigilo das comunicações eletrónicas não foi concedido para, a seu coberto, se poder insultar, ameaçar ou coagir outrem ou para se poder devassar a sua vida privada. Neste casos, apesar da sua reduzida relevância penal, o Estado deve ter legitimidade para intervir. Nada justifica, por isso,*

[292] Neste sentido, vide CORREIA, João Conde, *Prova Digital: as leis que temos e a lei que devíamos ter…*, p. 45.

[293] Idêntico entendimento foi perfilhado no Ac. do TRG, de 12 de Abril de 2010, proferido sob o Processo n.º 1341/08.4TAVCT, e Ac. do TRP, de 05-04-2017, proferido sob o Processo n.º 671/14.0GAMCN.P1, disponíveis *online*, respetivamente, nos endereços: http://www.dgsi.pt/jtrg.nsf/-/045285606F260EF2802577180050FDF9 [acedido em 25 de Junho de 2017] e http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/16ebc99e65fc19038025810c0051991a?OpenDocument [acedido em 1 de Junho de 2017].

destacar as ofensas cometidas por telefone, conferindo-lhes uma tutela processual penal muito superior às cometidas por via informática."[294].

Ora a verdade é que, recorrendo-se, mais uma vez, à exposição de motivos da proposta de Lei n.º 289/X, somos desafiados, num confessado reconhecimento, a abonarmos que os propósitos do legislador foram, precisamente, permitir a "*realização de interceção de comunicações eletrónicas e sobretudo a obtenção de dados de tráfego*" nos "*processos-crime em que se investiguem crimes cometidos por via das redes de comunicações*"[295], sendo que, o sentido da remissão da al. b), do n.º1, do art.º 18.º da LC, para o art.º 187.º do CPP, visa legitimar o recurso à interceção de comunicações em processos relativos a crimes *"cometidos por meio de um sistema informático ou em relação aos quais seja necessário proceder à recolha de prova em suporte electrónico*", caindo assim o argumento que apenas, e tão só, os crimes elencados no art.º 187.º do CPP podem ser intercetados.

E se dúvidas ainda imperassem, a verdade é que a recente nota prática n.º 8/2016[296], de 18/02, emitida pelo Gabinete do Cibercrime, relativa a pedidos de dados a operadores de telecomunicações, sendo objetiva na parte em que reconhece que é exigido um "*esforço adicional do intérprete*" na conciliação do CPP, da Lei nº 32/2008, de 17/07 e da Lei do Cibercrime, é também perentória ao consolidar que "*por aplicação das regras gerais da sucessão de leis no tempo, tem que concluir-se que o Artigo 189º do Código de Processo Penal foi parcelarmente revogado pela Lei do Cibercrime*". De resto, conforme ali consignado, apenas subsiste a aludida disposição na parte relativa ao n.º 2, do art.º 189.º, designadamente, na interpretação que apenas o juiz pode ordenar ou autorizar a obtenção de dados de tráfego ou, no contexto telefónico, da chamada faturação detalhada, em que se processa a solicitação de registos guardados pelos operadores de comunicações,

---

[294] CORREIA, João Conde, *Prova Digital: as leis que temos e a lei que devíamos ter…*, p. 45.

[295] Conforme decorre da exposição de motivos da proposta de Lei n.º 289/X. "*A recente (2007) revisão do Código de Processo Penal optou pela limitação, em abstracto, da possibilidade de realização de intercepções de comunicações telefónicas e electrónicas, não tendo incluído normas especiais para a área da cibercriminalidade. Assim, não está prevista a obtenção de dados de tráfego nem a realização de intercepção de comunicações electrónicas na investigação de crimes não previstos no artigo 187.º do Código de Processo Penal*". Disponível *online* no endereço http://www.parlamento.pt/Actividade Parlamentar/Paginas/DetalheIniciativa.aspx?BID=34566 [acedido em 04 de Junho de 2017]

[296] Disponível *online* no endereço http://cibercrime.ministeriopublico.pt/destaque/nota-pratica-no-82016 [acedido em 05 de Junho de 2017]

motivo pela qual os dados de conteúdo apenas são possíveis de obter por via da interceção de comunicações eletrónicas, em tempo real, do art.º 18º da LC, e não por via do art.º 189.º do regime geral.

Naturalmente, sempre permaneceriam por resolver algumas das contradições aparentemente existentes entre as Leis 32/2008 e 109/2009, designadamente, no que concerne à recolha, tratamento e conservação dos dados de tráfego e de localização, sendo aqui de realçar as duas correntes doutrinais que se entrechocam: De um lado, a doutrina que defende que o conjunto normativo dos art.ºs 11.º, 12.º, 13.º, 14.º, 16.º e 18.º da LC, revogou o art.º 9.º, da Lei 32/2008, subsistindo apenas a Lei 32/2008 no que respeita ao estabelecimento dos deveres dos fornecedores de serviços de conservação desses mesmo dados, no que a crimes graves diz respeito[297]; do outro, a tese que pugna pela relação de coexistência e complementaridade entre ambas as Leis numa harmonia possível[298]. Embora manifestando a nossa propensão para creditar que o art.º 9.º se mostra revogado e substituído pelo regime processual contido na Lei nº 109/2009, não podemos deixar, também aqui, de destacar o tremendo e complexo exercício de interpretação jurídico a que o legislador submeteu o intérprete, agora, ainda mais emaranhado face à orientação da aludida nota prática n.º 8/2016[299].

[297] MESQUITA, Paulo Dá, *Processo Penal, Prova e Sistema Judiciário*…, p. 123; NEVES, Rita Castanheira, *As Ingerências nas comunicações eletrónicas*…,p. 220-280. No mesmo sentido Ac. do TRE, de 06 de Janeiro de 2015, proferido sob o Processo n.º 6793/11.2TDLSB-A.E1. Disponível *online* no endereço http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/847dae6b85353cb880257de10056ff4c?OpenDocument [acedido em 08 de Junho de 2017].

[298] Tal entendimento é sustentado com o argumento que a complementaridade entre Leis foi solenemente consagrada por parte do legislador no art.º 11.º, n.º 2, da LC. Neste sentido *vide* ALBUQUERQUE, Paulo Pinto, *Comentário do Código de Processo Penal*…, 2011, p. 549; RODRIGUES, Benjamim Silva, *Da Prova Penal – Tomo II, Bruscamente…,* p. 519; MILITÃO, Renato, *A propósito da prova digital no processo penal*…, p. 275. CORREIA, João Conde, *Prova Digital: as leis que temos…,* p. 36-37.

[299] De acordo com a nota prática, o pedido de acesso aos dados de tráfego é da competência do JIC, podendo ser feito a partir dos art.ºs 187.º e 189.º, n.º2, do CPP (para os crimes do catálogo do art.º 187.º do CPP), e dos art.ºs 3.º, 6.º e 9.º da Lei 32/2008 (para o catálogo de crimes desta Lei). Já no que diz respeito à obtenção de dados de identificação do cliente e endereço de IP, nos termos do art.º 14.º, n.º 4, da LC, o GC reconhece-se competência ao MP, relativamente a todos os crimes, para proceder ao seu pedido.

9.3. As Buscas *Online*

Por via das buscas *online* é possível pesquisar os dados de conteúdo de um determinado sistema informático, sem que os órgãos de polícia criminal necessitem de se deslocar ao local onde se encontra o computador, o *smartphone*, entre outros equipamentos. Esta pesquisa é realizada a partir de outro terminal informático, com recurso a *worms* ou *spyware* (métodos idênticos aos utilizados pelos *hackers*), sem que ao visado seja concedida a possibilidade de controlar os limites legais da diligência[300].

Como método oculto de investigação que é, tal diligência representa uma agressiva intromissão nos processos de interação e comunicação das pessoas visadas (suspeitos), não tendo consciência de que ela está a ser realizada. De tal modo, nas palavras de COSTA ANDRADE, continuarão os cidadãos *"a agir, a interagir, a expressar-se e a comunicar de forma `inocente´, fazendo ou dizendo coisas de sentido claramente auto – incriminatório ou incriminatório daqueles que com elas interagem ou comunicam*", acabando por "vomitar", no profundo da sua intimidade, autênticas "*confissões larvadas*" que colocam a nu a sua privacidade.[301]

Nesta sequência, é inolvidável representar-se hoje o computador, conforme ilustra HASSEMER, como uma espécie de "armazém" ou "compartimento", assumindo-se, nas palavras de BENJAMIM SILVA RODRIGUES, como *"o domicílio informático ou a casa digital onde mora a nossa alma digital. Nele estão armazenados os nossos "anseios e receios, gostos e desgostos, prazeres e haveres, amores e desamores, inclinações ou orientações"*[302], enfim, todo um conjunto de dados que identificam a nossa "*essência humana*" e nos tornam facilmente identificáveis.

Como é consabido, os métodos ocultos de investigação sacrificam bens jurídicos e direitos fundamentais pessoais do cidadão. De tal forma, as potenciais lesões à privacidade/intimidade, à imagem, à palavra, à inviolabilidade do domicílio, à confidencialidade e integridade dos sistemas técnico – informacionais, bem como à própria autoderminação – informacional, apenas podem ser justificadas mediante a verificação cumulativa de um exigente conjunto de pressupostos materiais e requisitos formais-

[300] ANDRADE, Manuel da Costa, *Comentário Conimbricense…,* p. 1103.
[301] ANDRADE, Manuel da Costa, *Bruscamente no verão passado…*, p 106.
[302] RODRIGUES, Benjamim Silva, "*Da Prova Penal – Tomo II – Bruscamente*…p. 472 e 473.

procedimentais, sob pena de inadmissibilidade e invalidade da prova recolhida. Desde logo, é pressuposto, *sine qua non,* a verificação do princípio da reserva de lei, sob a imaculada veste segundo o qual só a lei pode legitimar a autorização de qualquer método oculto de investigação criminal. Complementarmente, exigir-se-á a seleção e eleição de um restrito catálogo de crimes, suficientemente gravosos, que justifique tal invasão à esfera privada, submetendo-se a recolha de prova ao crivo do princípio da proporcionalidade (*strictu* senso), necessidade e salvaguarda pela inviolabilidade da área nuclear da intimidade. De outra sorte, não deverá deixar de se exigir que em causa esteja uma fundada suspeita, consubstanciada em factos concretos, devendo o meio oculto utilizado na investigação revelar-se subsidiário em relação a outros meios menos gravosos, circunscrito no tempo, bem como sujeito ao controlo do JIC, enquanto garante dos direitos, liberdades e garantias.[303]

Para mágoa de alguma doutrina (atendendo que permitiria abonar as taxas de eficiência da investigação em matéria de cibercriminalidade), este método oculto de investigação não tem expressa consagração no ordenamento jurídico português, dada a inexistência de regulamentação específica de procedimentos e meios técnicos a utilizar pela investigação, situando-se fora da categoria e tutela da inviolabilidade das telecomunicações (porquanto não configura qualquer intromissão na transmissão do processo comunicativo), e propriamente das tradicionais buscas, reconduzindo-se a uma distinta forma de intromissão e abuso nos sistemas informáticos[304]. Assim, por força dos art.ºs 18.º, n.º 2, 34.º, n.º 4 e 35.º, n.º 4, todos da CRP, somente com a adoção de uma lei clara, expressa e específica, dada a elevada danosidade nos direitos fundamentais do cidadão, estaria aferida a legitimidade de recorrer-se a tal método de obtenção de prova[305].

---

[303]RODRIGUES, Benjamim Silva, *Da Prova Penal – Tomo II – Bruscamente*…p. 63-66;

[304] Neste sentido *Vide*, ANDRADE, Manuel da Costa, *Bruscamente…,* p. 166-169; NEVES, Rita Castanheira, *As ingerências*…, p. 284. RAMOS, Armando Dias, *A Prova Digital*...,2.º Ed., p. 102. RODRIGUES, Benjamim Silva, "*Da Prova Penal – Tomo II – Bruscamente*…, p. 474. Neste conspecto, o Tribunal Constitucional Federal Alemão avançou com a sugestão de decantar e institucionalizar um novo direito fundamental: a integridade e confidencialidade dos sistemas informáticos – cfr. decisão do 1.º senado do *BVerfG*, de 27.03.2008 - *Apud* ANDRADE, Manuel da Costa, *Bruscamente no verão passado*…, p. 168.

[305] O legislador Alemão, fazendo *jus* às exigências de proporcionalidade, e obrigando a medida a níveis de exigência mínimos, circunscreve a utilização das buscas *online* em casos de terrorismo internacional (Lei para a defesa face aos perigos do terrorismo internacional através do *Bundeskriminalamt*) e sob condição da iminente perigosidade de lesão de concretos bens jurídicos essenciais para o Estado. *Vide* ANDRADE, Manuel da Costa, *Bruscamente*…, p. 165 e 166 e RODRIGUES, Benjamim Silva, *Da Prova Penal – Tomo II – Bruscamente…,* p. 475.

De tal modo, será errado ver-se no art.º 15.º, n.º 5, da LC, conforme o vem fazendo alguma doutrina, nomeadamente PAULO PINTO ALBUQUERQUE[306] e PEDRO VERDELHO[307], a consagração expressa das buscas *online,* ainda que pugnando pela inconstitucionalidade de tal preceito. O que está aqui em causa é apenas a extensão *online* de uma pesquisa de dados informáticos em curso, não se tratando de uma diligência oculta e feita à revelia do visado. De resto, o acesso informático ao segundo sistema, estando sempre dependente da prévia autorização a partir do primeiro, compromete, desde logo, o secretismo deste meio de obtenção de prova, permitindo ao visado o controlo da sua legalidade[308]. Doutro passo, conforme adianta RITA CASTANHEIRA NEVES, a presença da autoridade durante a pesquisa de dados informáticos (art.º 15.º, n.º1, da LC), bem como as formas de apreensão de dados informáticos dispostas na LC (art.º 16.º, n.º 7, al. a) a d)), por si só, são também procedimentos que comprometem a realização de buscas *online*.[309]

Assim, sendo um facto que se desafia o sistema processual penal português a disciplinar os campos de legitimação da utilização de tal método oculto de investigação, a verdade é que, na legislação vigente, foi o legislador luso incapaz de dotar a investigação deste poderoso meio de obtenção de prova, ainda que razoavelmente justificado a circunscritas formas extremas de criminalidade, como sucede no caso alemão. Não obstante, por se tratar também de um meio preventivo, facto é que permanece a incógnita quanto à concreta utilização de tal meio por parte da investigação no ordenamento jurídico português, permanecendo sérias dúvidas relativamente à sua efetiva utilização, ainda que à margem da legalidade e dos princípios estruturantes do processo penal.

[306] ALBUQUERQUE, Paulo Pinto, *Comentário do Código de Processo Penal*….p. 502.
[307] VERDELHO, Pedro, *Lei do Cibercrime*, in AA. VV., *Enciclopédia de Direito e Segurança*…p. 261.
[308] CORREIA, João Conde, *Prova Digital: as leis que temos e a lei que devíamos ter…,* p. 42.
[309] NEVES, Rita Castanheira, *As ingerências nas comunicações eletrónicas*…, p. 284

Conclusão

Como pudemos verificar, o correio eletrónico, enquanto prova digital, vê-se emaranhado numa arrevesada teia legislativa no processo penal português, acabando a diversidade de diplomas que o regulam por criar dissimetrias conceptuais, nem sempre se alcançando os desideratos do legislador, circunstância que contribui para a insegurança jurídica, acabando por fragilizar direitos individuais.

As respostas às questões jurídicas relacionadas com as comunicações eletrónicas, designadamente, as condições processuais de admissibilidade da apreensão e interceção de dados informáticos no correio eletrónico, convocam o intérprete a um complexo exercício interpretativo, tal a quantidade de fontes normativas que é necessário mobilizar na procura de soluções, essencialmente, dispersas no Código de Processo Penal, na Lei 32/2008, de 17/07, e na Lei 109/2009, de 15/09.

A superficial inclusão que fizemos ao mundo digital, permitiu-nos, desde logo, concluir que as particulares características da prova digital, tornaram-na numa prova ímpar e carente de interpretação especializada, fazendo sentido falar-se hoje da ciência forense digital, não apenas como o conjunto de regras, procedimentos e princípios que assegurem a integridade, fiabilidade e inalterabilidade desta prova, mas também no reconhecimento pelos direitos constitucionais que é necessário salvaguardar.

Sendo um facto que os suportes informáticos são o "espelho da alma", tal a quantidade de informação pessoal e profissional que aí é depositada, julgámos de primordial importância destacar que os meios de obtenção de prova dispostos no Código de Processo Penal estão talhados para a prova física, não aprazados à recolha e obtenção dos dados informáticos, que, no fundo, se reconduzem a codificações binárias de *bits* e *bytes*.

A difícil encruzilhada a que vinha sendo submetida a regulação do correio eletrónico, particularmente, as condições processuais de admissibilidade da recolha dos dados informáticos, aconselhavam que o legislador, na reforma operada ao CPP de 2007, tivesse a audácia necessária para assumir uma mudança de paradigma, concretamente, acolhido no CPP os influentes contributos da timoneira CCiber e da Decisão-Quadro 2005/222/JAI, eliminando a manta de retalhos em que o art.º 189.º do CPP se tinha transformado. Porém, este não foi o caminho seguido pelo legislador, acabando esta

cláusula de extensão, para além de avolumar dissimetrias conceptuais, por semear o caos processual entre os operadores judiciários ao regular, a partir do regime das escutas, indistintamente, quer a interceção e registo das mensagens de correio eletrónico, ainda em transmissão, e, portanto, enquanto comunicação, quer a apreensão destas mensagens já armazenadas, enquanto ficheiro digital resultante de uma comunicação.

Não obstante a Lei 32/2008, de 17/07, ter contribuído para regular a conservação de dados gerados e tratados no contexto de oferta de serviços de comunicações eletrónicas, caberia à Lei n.º 109/2009, de 15/09, a virtuosidade de rasgar com a matriz e os efeitos hipnóticos do art.º 189.º do CPP, designadamente, reconhecendo os desequilíbrios de proteção constitucional a que o correio eletrónico, por via dos dois momentos do ato comunicacional, pode estar submetido: o momento de transmissão, em que a mensagem reclama a proteção inerente ao estatuto de comunicação, e o momento posterior ao cumprimento do ato de levar ao destinatário o teor comunicacional, elevado ao estatuto aproximado de um ficheiro digital armazenado.

Neste seguimento, num estilhaçar de aparências, e no que ao correio eletrónico concerne, não obstante a promiscuidade das constantes remissões para a lei penal adjetiva, é imperioso considerar que o art.º 17.º da LC, disciplinando autonomamente as mensagens de correio eletrónico que se encontram armazenadas nos sistemas informáticos, parte do profundo reconhecimento que tais ficheiros, embora já não sendo comunicação, têm, em nome da salvaguarda constitucional do direito à autoderminação informacional, por via da utilização da informática, uma proteção adicional em relação a outros ficheiros e documentos arquivísticos. Neste esteio, reconhecendo a opção legislativa as desigualdades existentes entre o correio eletrónico e o correio tradicional, desde logo, percetível à lupa da própria natureza jurídica da prova digital, bem como os riscos a que está exposta por parte da ingerência de terceiros, deve prevalecer o entendimento que, efetivamente, somente com a autorização ou ordem do juiz é possível proceder à apreensão de mensagens de correio eletrónico, assim como deverá ser o juiz a primeira pessoa a tomar conhecimento do conteúdo dos *e-mails* apreendidos.

Doutro passo, não obstante a LC não ter revogado expressamente o art.º 189.º do CPP, não há que deixar de considerar que, com a vigência desta Lei extravagante, ficam esclarecidas muitas das questões que se levantavam em sede de interceção e registo do correio eletrónico. Assim, é essencial notar que o art.º 189.º do CPP, por via do art.º 18.º da

LC, ficou vazio de conteúdo, passando a ser a disposição especial a trave mestra que regula a interceção e registo de comunicações eletrónicas – em tempo real – por parte da investigação, abrangendo, quer os crimes tipificados na LC, quer os crimes do art.º 187.º do CPP, quando cometidos por meio de um sistema informático ou em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico, encontrando-se quer os dados de conteúdo, assim como os dados relacionados com a comunicação, protegidos pelo direito à privacidade e a coberto da garantia constitucional do direito à inviolabilidade das comunicações plasmado no art.º 34.º da CRP.

A precipitação legislativa, aliada à frenética conceção de diplomas, não têm contribuído para que o legislador português estabilize as regras processuais quanto à recolha e obtenção de dados informáticos, originando uma colisão normativa, por via da multiplicação e sobreposição das regras processuais dispostas no CPP, na Lei n.º 32/2008, e na Lei Cibercrime, muito embora se reconheça este último diploma como a "pedra angular" e o "sagrado altar" no que diz respeito à recolha da prova digital.

Em derradeiro, mal ficaríamos se, no que à regulação da prova digital diz respeito, não fossemos apologistas que o legislador português, contrariamente aos modelos adotados, não tivesse aproveitado o soprar dos ventos para compatibilizar, globalmente, e numa única fonte, a prova digital. Ao ter deixado escapar a oportunidade de "recodificar" o Código de Processo Penal, assegurando a sua centralidade normativa (colocando de pé capítulos novos e regimes novos), reconduzindo à Lei geral os meios de obtenção de prova consagrados na Lei do Cibercrime (à semelhança, de resto, do que sucede noutros ordenamentos jurídico – processuais), então, à giza de reflexão, o panorama convidaria que a legislação especial, em exclusivo, regulamentasse a recolha e obtenção da prova digital, cortando umbilicalmente com as remissões para a lei geral.

Cientes dos nefastos danos que uma lei mal concebida pode trazer à administração da justiça, é nossa convicção que o conhecimento e experiência adquiridos pelos operadores e aplicadores do direito, contribuirão para desconstruir enigmas que minam o campo do direito e da informática, sobretudo numa área tão complexa, evoluída e perigosa, como é a cibercriminalidade, sempre se assegurando que a realização da justiça, não ocorra à margem do esquecimento dos direitos, liberdades e garantias das pessoas. Afinal, porque não o diríamos melhor, razão assistia ao Ilustre Professor Conimbricense FIGUEIREDO

DIAS, na singela, mas tão emblemática afirmação de que "*Diz-me como tratas o arguido, dir-te-ei o processo penal que tens e o Estado que o instituiu.*"[310].

[310] DIAS, Jorge de Figueiredo, *Direito Processual Penal*, 1ª Ed. 1974, Coimbra Editora, p. 428.

Bibliografia

- ALBARRÁN LOZANO, Irene, PABLOS HEREDERO, Carmen e MONTERO NAVARRO, Antonio, *Uso del correo electrónico: un análisis empírico en la Universidad Complutense de Madrid,* Documentos de Trabajo de la Facultad de Ciencias Económicas y Empresariales, nº 09, 1999, ISSN: 2255-5471. Conteúdo disponível *online* no endereço http://eprints.sim.ucm.es/6676/1/9909.pdf;

- ALBUQUERQUE, Paulo Pinto, *Comentário do Código de Processo Penal à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem*, 2.ª Edição, Universidade Católica, Lisboa, 2008;

- _____, Paulo Pinto, *Comentário ao Código de Processo Penal*, 4º Edição Atualizada, Universidade Católica Editora, Lisboa 2011;

- _____, Paulo Pinto, *Comentário do Código Penal à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem*, 3.ª Edição, Universidade de Católica Editora, 2015;

- ALBRECHT, Hans-Jörg, "*Vigilância das telecomunicações. Análise teórica e empírica da sua implementação e efeitos"*, *Que futuro para o direito processual penal? Simpósio em Homenagem a Jorge de Figueiredo Dias, por ocasião dos 20 anos do Código de Processo Penal Português*, Coord. Mário Ferreira Monte, Trad. Inês Fernandes Godinho, Coimbra Editora, 2009;

- AMBOS, Kai, *Derecho penal del enemigo,* trad. por Gómez Jara Díez e Miguel Lamadrid, Bogotá, Universidad Externato de Colombia, 2007.

- ANDRADE, José Carlos Vieira de, *Os direitos fundamentais na Constituição portuguesa de 1976*, 5. ed. Coimbra, Edições Almedina, 2012;

- ANDRADE, Manuel da Costa, *Sobre as proibições de Prova em Processo Penal*, Reimpressão, Coimbra Editora, 2006;

- _____, Manuel da Costa, *As Escutas Telefónicas como meio de obtenção de prova no novo Código de Processo Penal de Macau,* in Revista Jurídica de Macau, Volume IV, n.° 1, 1997;

- _____, 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, ISBN 978-972-32-1726-1;

- _____, Manuel da Costa, *Comentário Conimbricense do Código Penal: parte especial*, Dir. Jorge de Figueiredo Dias, Américo Taipa de Carvalho, 2ª edição, Coimbra, Coimbra Editora, 2012, ISBN 9789723220612;

- _____, Manuel da Costa, *Sobre as Proibições de Prova em processo Penal*, Coimbra Editora, 1.ª Edição, Reimpressão, Outubro, 2013, ISBN 978-972-32-2196-1;

- ASCENSÃO, José de Oliveira, *Teoria Geral do Direito Civil*, Vol. I, Faculdade de Direito de Lisboa, Lisboa, 1996;

- _____, José Oliveira, *Direito da Sociedade da Informação*, Vol. VIII, Coimbra Editora, ISBN 978-972-32-1710-0;

- _____, José de Oliveira, *Estudos sobre Direito da Internet e da Sociedade da Informação*, Livraria Almedina, Coimbra, 2001, ISBN 163116/01;

- BACHMAIER WINTER, Lorena, *Investigación criminal y protección de la privacidad en la doctrina del Tribunal Europeo de Derechos Humanos*, AA.VV., 2.º Congresso de investigação criminal (org. por Maria Fernanda Palma /Augusto Silva Dias / Paulo de Sousa Mendes), Coimbra, Almedina, 2011;

- BERGMAN, Michael, *The Deep Web: Surfacing Hidden Value*, BrightPlanet, Volume 7, Issue 1: *Taking License*, August, 2001;

- BLASCO, Andrés, *Qué Es Internet?*, Principios de Derecho de Internet, Prainter, Tirant lo Blanch, Valencia, 2002;

- BRAVO, Rogério Bravo, *Da não equiparação do correio - eletrónico ao conceito tradicional de correspondência por carta, Polícia e Justiça*, Revista do Instituto Superior de Polícia Judiciária e Ciências Criminais, III Série, n.º 7, Coimbra Editora, Janeiro - Junho 2006;

- CABO, Ana Isabel, *Nova lei facilita investigação da Criminalidade Informática*, Boletim da Ordem dos Advogados, n.º 65, Abril 2010;

- CABRAL, Santos, Código de Processo Penal Comentado, A.A. VV., Almedina Editora, 2.ª edição, 2016;

- CANOTILHO, Gomes e MOREIRA, Vital, *Constituição da República Portuguesa Anotada*, Coimbra Editora, 1993;

- _____, Gomes, *Direito Constitucional e Teoria da Constituição*, 7. ed. Coimbra, Almedina, 2010;

- CASEY, Eoghan, *Digital Evidence and Computer Crime, Forensic Science, Computers and the Internet*, Academic Press, 2000;

- CASTELLS, Manuel, *A Galáxia Internet, Reflexões sobre a Internet, Negócios e Sociedade, Serviço de Educação e Bolsas,* Fundação Calouste Gulbenkian, Lisboa, 2004;

- CASTRO, Catarina Sarmento, *Direito da Informática, Privacidade e Dados pessoais*, Coimbra, Edições Almedina, 2005, ISBN: 9789724024240;

- _____, Catarina Sarmento, *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;

- COMER, Douglas, *Internetworking with TCP/IP*, Volume 1: Principles, Protocols, and Architectures, Fourth Edition, Prentice Hall PTR, Upper Saddle River, NJ, 2000;

- CONCEIÇÃO, Ana Raquel, Escutas Telefónicas - Regime Processual Penal, Quid Juris Editora, 2009;

- COSTA, Bruto da, e BRAVO, Rogério, *Spam e Mail Bomb, Subsídios para uma perspectiva criminal*, Quid Juris, 2005;

- COSTA, José de Faria, *O direito penal, a informática e a reserva da vida privada, Direito Penal da Comunicação – Alguns escritos*, Coimbra, Coimbra Editora, 1998;

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

- _____, José de Faria, *Algumas Reflexões sobre o Estatuto Dogmático do Chamado ´Direito Penal Informático´*, Direito Penal da Comunicação, Coimbra Editora, 1998;

- _____, José de Faria e MONIZ, Helena, "*Algumas Reflexões sobre a Criminalidade Informática em Portugal*" in BFDUC, Vol. LXXIII, 1997;

- CORREIA, João Conde, *Prova Digital: as leis que temos e a lei que devíamos ter*, Revista do Ministério Público, ISSN 0870-6107, Ano 35, n.º 139, 2014;

- CORREIA, Miguel Pupo, *Retenção de dados de comunicações*, Universidade Lusíada de Lisboa, n.º 7, 2010;

- CRATO, Nuno Teixeira, *The Walking Virtually Dead: Entre uma Algoritmocracia Jus Constituendum e um Homem Virtual Transparente, Existe Espaço para o Direito a uma Identidade Informacional?,* Dissertação de Mestrado em Segurança da Informação e Direito no Ciberespaço, Universidade de Lisboa, Out. 2016;

- DIAS, Jorge de Figueiredo, *Temas Básicos da Doutrina Penal – Sobre os Fundamentos da Doutrina Penal*, sobre a Doutrina Geral do Crime, Coimbra Editora, 2001;

- _____, Figueiredo, *Sobre a Revisão de 2007 do Código de Processo Penal Português*, RPCC, ano 18, n.º 2/3, 2008;

- DIAS, Vera Marques, *A Problemática da Investigação do Cibercrime*, Data Venia, Revista Jurídica Digital, Ano 1, n.º 1, Julho-Dezembro 2012, ISSN 2182-8242;

- DRAY, Guilherme Machado, *Justa causa e esfera privada,* Estudos do Instituto de Direito do Trabalho, Vol. III, Almedina, Coimbra, 2001;

- EIRAS, Agostinho, *Segredo de Justiça e Controlo de Dados Pessoais Informatizados*, Coimbra Editora, Col. Argumentum, 4, 1992;

- FERNÁNDEZ TERUELO, Javier Gustavo, *Cibercrim, Los delitos cometidos a través de Internet*, Constitutio Criminalis Carolina, 2007;

- GARRIGA DOMÍNGUEZ, Ana, *Nuevos retos para la protección de datos personales: en la era del big data y de la computación ubicua*, Editorial Dykinson, 1ª ed., 2016;

- GASPAR, António Henriques, *As exigências da investigação no processo penal durante a fase de instrução*, *Que futuro para o direito processual penal? Simpósio em Homenagem a Jorge de Figueiredo Dias, por ocasião dos 20 anos do Código de Processo Penal Português,* Coord. Mário Ferreira Monte, Trad. Inês Fernandes Godinho, Coimbra Editora, 2009;

- GONÇALVES, Pedro, *Direito das Telecomunicações,* Almedina, Coimbra, 1999;

- JÚDICE, José Miguel, *Escutas telefónicas: a tortura do século XXI*, Revista da Ordem dos Advogados, Ano 64, Vol. I/II, Novembro, 2004;

- KERR, Orin S., *Digital Evidence and the New Criminal Procedure*, Columbia Law Review 279, GWU Law School Public Law Research Paper No. 108, 2005;

- LEITE, André Lamas, *Entre Péricles e Sísifo: o novo regime legal das escutas telefónicas*, Revista Portuguesa de Ciência Criminal, Ano 17, n.º 4, Out.- Dez. 2007;

- LÉVY, André, CASANOVA, Catarina, GASPAR, Augusto e VIEIRA, António Bracinha, *Homem: Origem e evolução*, 2.ª edição, Edição Glaciar, Maio de 2015, ISBN: 978-989-8776-21-1;

- LOBO, Fernando Gama, *Código de Processo Penal Anotado*, Almedina Coimbra, 2015;

- LOPES, José Mouraz e CABREIRO, Carlos Antão, *A Emergência da Prova Digital na Investigação da Criminalidade Informática, in* Sub Judice — Justiça e Sociedade, n.º 35, Coimbra, Almedina, 2006;

- MADISON, Michael, *Law as Design: Objects, Concepts, and Digital Things*, Case Western Reserv Law Review, v.56, 2005;

- MADUREIRA, Raquel Castro, DUARTE, A. Manuel e FONSECA, Raquel Matias, *133 anos de Histórias das Comunicações em Portugal*, Electrónica e Telecomunicações, Revista da Universidade de Aveiro, vol. 5, n.º 3, Junho 2011;

- MARQUES, Garcia e MARTINS, Lourenço, *Direito da Informática*, 2ª Edição, Almedina, Coimbra, 2006;

- _____, Garcia e MARTINS, Lourenço, *Direito da Informática*, Lições de Direito da Comunicação, Almedina, 2000;

- MARQUES, Pedro P. Leitão da Costa, *Informática Forense - Recolha e Preservação da Prova Digital*, Dissertação de mestrado em Segurança em Sistemas de Informação, Universidade Católica Portuguesa Faculdade de Engenharia, Maio, 2013;

- MARTINS, Lourenço, MARQUES, Garcia e DIAS, Pedro, *Ciberlaw em Portugal – O direito das tecnologias da informação e comunicação*, Centro Atlântico, 1.ª Edição, Setembro de 2004;

- MAURÍCIO, Pedro, *O Correio Eletrónico – Aspectos importantes para a investigação criminal*, Área de Documentação e Tradução da Policia Judiciária, Lisboa, 2006;

- MCCULLAGH, Noel, *Securing E-Mail with Identity Based Encryption*, IT Pro, May June, EUA, 2005;

- MESQUITA, Paulo Dá, *Processo Penal, Prova e Sistema Judiciário,* Wolters Kluwer, Coimbra Editora, 1.ª Edição, Set. 2010;

- MILITÃO, Renato Lopes, *A propósito da prova digital no processo penal,* Revista da Ordem dos Advogados – ROA, (Ano 72), n.º 1, 2012;

- MONIZ, Helena, *Notas sobre a proteção de dados pessoais perante a informática (o caso especial dos dados pessoais relativos à saúde),* Separata da Revista Portuguesa de Ciência Criminal, Ano 7, Fasc. 2.º, Coimbra Editora, Abril – Junho 1997;

- MONTEIRO, Edmundo e BOAVIDA, Fernando, Engenharias de Redes Informáticas, FCA, 7.ª edição, Agosto de 2000;

- NETO, João Monteiro, *Crimes informáticos uma abordagem dinâmica ao direito penal informático*, Pensar Fortaleza, vol. 8, n.º 8, Fevereiro, 2003.

- NETO, Luísa, *O Direito Fundamental à disposição sobre o próprio corpo (A relevância da vontade na configuração do seu regime),* Coimbra: Coimbra Editora, 2004;

- NEVES, Rita Castanheira, *As Ingerências nas Comunicações Eletrónicas em Processo Penal – Natureza e respectivo regime jurídico do correio electrónico enquanto meio de obtenção de prova*, Coimbra Editora, 1.ª Edição, Junho de 2011, ISBN 978-972-32-1942-5;

- _____, Rita Castanheira e CORREIA, Hélder Santos, *A lei do cibercrime e a colaboração do arguido no acesso aos dados informáticos,* Actualidad Jurídica Uria Menéndez, n.º 38, 2014;

- OLIVA LEÓN, Ricardo, *La Prueba Electrónica Envenenada*, in *La Prueba Electrónica – Validez y Eficacia procesal*, Coord. Ricardo Oliva León Sonsoles Valero Barceló, Colección Desafíos Legales, 1º edição, Setembro de 2016;

- PEREIRA, Joel Timóteo, *Compêndio Jurídico da Sociedade da Informação – Notas Práticas, Legislação e Jurisprudência*, Quid Juris, Sociedade Editora, Lisboa, Outubro 2004;

- PÉREZ LUÑO, Antonio Enrique, *Manual de Informática y Derecho*, Ariel Derecho, Barcelona, 1996;

- PINHEIRO, Alexandre Sousa, *Privacy e Protecção de Dados Pessoais: A Construção Dogmática do Direito à Identidade Informacional*, Associação Académica da Faculdade de Direito de Lisboa, AAFDL Editora, Janeiro, 2015;

- PINTO, Paulo da Mota, *A limitação voluntária do direito à reserva sobre a intimidade da vida privada*, in Estudos em homenagem a Cunha Rodrigues, Vol. II, Coimbra Editora, Coimbra, 2001;

- PORTELA, Irene, *A intercepção legal de comunicações em redes IP,* Revista de Estudos Politécnicos, Vol VI, nº 9, 2008, ISSN: 1645-9911;

- RAMALHO, David Silva, *A investigação criminal na Dark Web*, Revista da Concorrência e Regulação, Ano IV, n.º 14/15, Almedina, Abril/Setembro 2013;

- _____, David Silva, *A Recolha de Prova Penal em Sistemas de Computação em Nuvem*, Revista de Direito Intelectual, n.º 2, 2014.

- _____, David Silva e COIMBRA, José Duarte, *A Declaração de Invalidade da Diretiva 2006/24/CE: Presente e futuro da regulação sobre a conservação de dados por parte de fornecedores de serviços de comunicações eletrónicas*, Abril, 2014, Disponível *online* no endereço http://www.servulo.com/xms/files/publicacoes/Updates_2014/Update_TI_DSR_JDC_A_declaracao_de_invalidade_da_diretiva_2006_24_CE_10_04_2014.pdf;

- RAMOS, Armando Dias, *A Prova Digital em Processo Penal*, Chiado Editora, 1.º ed., Novembro 2014;

- _____, Armando Dias, *A Prova Digital em Processo Penal*, Chiado Editora, 2.º ed., Fevereiro de 2017, ISBN: 978-989-51-2383-4;

- RAMOS, Vânia Costa, *Âmbito e Extensão do Segredo das Telecomunicações*, Revista do Ministério Público, n.º 11, Out./Dez. 2007;

- RODRIGUES, Benjamim Silva, *Das Escutas Telefónicas – A Monitorização dos Fluxos Informacionais e Comunicacionais*, Tomo I, Coimbra, Coimbra Editora, 2008;

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

- _____, Benjamim Silva, *Da Prova Penal – Tomo IV, Da Prova - Electrónico - Digital e da Criminalidade Informático – Digital*, Rei dos Livros, Lisboa, 2011, ISBN 9789898305183;

- _____, Benjamim Silva, *Da Prova Penal – Tomo II, Bruscamente… A(s) Face(s) Oculta(s) dos Métodos Ocultos de Investigação Criminal*, 1.ª Edição, Editora Rei dos Livros, Abril, 2010;

- _____, Benjamim Silva, *Das Escutas Telefónicas à Obtenção da Prova [em ambiente digital]*, Tomo II, Coimbra, 2009;

- _____, Benjamim Silva, *A Monitorização dos Fluxos Informacionais e Comunicacionais* - (*Contributo para a Superação do "Paradigma da Ponderação Constitucional e Legalmente Codificado" em Matéria de Escutas Telefónicas),* Vol. II, Coimbra, Coimbra Editora, 2009, ISBN 9789899577978;

- _____, Benjamim Silva, *Da Prova Penal - Tomo II, Métodos Ocultos de Investigação Criminal*, Rei dos Livros, 2010;

- _____, Benjamim Silva, *Da Prova Penal – Tomo IV, Da prova – Electónico – Digital e da Criminalidade Informático-Digital*, 1.º edição, 2011;

- ROGALL, Klaus, *A nova regulamentação da vigilância das telecomunicações na Alemanha*, 2.º Congresso de Investigação Criminal, Coord. Científica de Maria Fernanda Palma, Augusto Silva Dias e Paulo de Sousa Mendes, Almedina, Out. 2010;

- ROMEO CASABONA, Carlos María, *La protección penal de los mensajes de correo eletrónico y de outras comunicaciones de carácter personal a través de Internet*, Derecho y Conocimiento, Vol. 2, 2006;

- ROVIRA DEL CANTO, Enrique, *Delincuencia Informática y Fraudes Informáticos*, Estúdios de Derecho Penal dirigidos por Carlos María Romeo Casabona, 33, Editorial Comares, Granada, 2002;

- SALOM CLOTET, Juan, *Delito Informático y su Investigación*, Cuadernos de Derecho Judicial, III, Consejo General Del Poder Judicial, Centro de Documentación Judicial, 2006;

- SANTOS, André Teixeira, *Os novos desafios do Direito Penal no século XXI*, Scientia Ivridica, n.º 316, 2008;

- SANTOS, Cristina Máximo, *As novas tecnologias da informação e o sigilo das telecomunicações*, Revista do Ministério Público – Lisboa, Sindicato dos Magistrados do Ministério Público, A. 25, n.º 99, 2004;

- SANTOS, Paulo, BESSA, Ricardo e PIMENTEL, Carlos, *Ciberwar – O Fenómeno, as Tecnologias e os* Actores, FCA – Editora de Informática, Janeiro 2008, ISBN: 978-972-722-597-2;

- SANTOS, Rita Coelho, *O Tratamento Jurídico-Penal da Transferência de Fundos Monetários Através da Manipulação Ilícita dos Sistemas Informáticos*, Coimbra Editora, 2005;

- SANTOS, Simas e HENRIQUES, Leal, *Código de Processo Penal Anotado*, 2.ª Edição, I Vol., Editora Rei dos Livros, 1999;

- SIEBER, Ulrich, *Legal Aspects of Computer – Related Crime in the Information Society – Comcrime – Study*, 1998;

- SILVA, Germano Marques, *Curso de Processo Penal, I Volume – Noções Gerais, Elementos do Processo Penal*, 6.ª Edição, Lisboa, Verbo, 2010;

- TEIXEIRA, Angelina, *A Chave para a Regulamentação da Proteção de Dados*, Data Venia, Revista Jurídica Digital, n.º6, Novembro 2016;

- TEIXEIRA, Carlos Adérito, *Escutas Telefónicas: a mudança de paradigma e os velhos e novos problemas* – Jornadas sobre a revisão do Código de Processo Penal, Revista CEJ, 1.º semestre, número 9 (Especial), 2008;

- VALENTE, Manuel Guedes, *Escutas Telefónicas - Da Excepcionalidade à Vulgaridade*, 2.ª edição, Coimbra, Edições Almedina, 2008;

- VEIGA, Armando e RODRIGUES, Benjamim Silva, *Escutas telefónicas, rumo à monitorização dos fluxos informacionais e comunicacionais digitais*, Coimbra Editora, 2ª Edição, 2007;

- _____, Armando e RODRIGUES, Benjamim, *A Monitorização de dados pessoais de tráfego nas comunicações electrónicas*, Revista Raízes Jurídicas, Curitiba, v. 3, n. 2, Jul./Dez. 2007;

- VEIGA, Pedro, *Direito a Pensar Tecnologicamente*, revista científica sobre *cyberlaw* do centro de investigação jurídica do ciberespaço – CIJIC – da faculdade de direito da universidade de lisboa, Edição n.º II, Junho de 2016;

- VEIGA, Pedro e DIAS, Marta, *A Governação da Internet*, Janus.Net, e-journal of International Relations, Vol. 1, n.º 1, 2010, ISSN: 1647-7251;

- VENÂNCIO, Pedro Dias, *Lei do Cibercrime – Anotada e Comentada*, Coimbra Editora, Janeiro 2011;

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

- VERDELHO, Pedro, *Cibercrime*, in AA.VV., *Direito da Sociedade da Informação*, APDI (Associação Portuguesa de Direito Intelectual), volume IV, Coimbra Editora, 2003;

- _____, Pedro, *Apreensão do Correio Eletrónico em processo Penal,* Revista do Ministério Público, Lisboa, Ano 25, n.º 100, Out./Dez, 2004;

- _____, Pedro, A *Técnica no novo C.P.P.: Exames, Perícias e Prova Digital*, Revista do CEJ, Lisboa, 1. º Semestre, n. 9, 2008;

- _____, Pedro, *A nova Lei do Cibercrime, in Scientia Ivridica,* Revista de Direito Comparado Português e Brasileiro, Tomo LVIII, N.º 320, Out. – Dez. de 2009, ISSN 0870-8185;

- _____, Pedro, BRAVO, Rogério e ROCHA, Manuel Lopes, *Leis do Cibercime – Volume I*, Centro Atlântico, 1ª edição, Julho de 2003, ISBN: 972-8426-69-0;

- _____, Pedro, *Lei do Cibercrime*, in AA. VV., *Enciclopédia de Direito e Segurança*, Coord. Jorge Bacelar Gouveia e Sofia Santos, Almedina, 2015;

- WARREN, Samuel e BRANDEIS, Louis, *The right to privacy*, Harvard Law Review, Vol. IV, n.º 5, *December* 15, 1890.

Jurisprudência, Pareceres e Outros Recursos Bibliográficos

Jurisprudência

- Acórdão do Tribunal da Relação de Guimarães, de 10.01.2005, proferido sob o processo n.º 2013/04-1, disponível *online* no endereço http://www.dgsi.pt/jtrg.nsf/86c25a698e4e7cb7802579ec004d3832/0acea33f67fe0e2980256fe3003d53b8?OpenDocument [acedido em 28 de Novembro de 2016];

- Acórdão do Tribunal da Relação de Coimbra, de 03.10.2012, proferido sob o processo n.º 84/11.6JAGRD-A.C1, acessível *online* no endereço http://www.dgsi.pt [acedido em 16 de Dezembro de 2016];

- Acórdão do Tribunal da Relação de Évora, de 5.06.2012, proferido sob o processo n.º 12/12.1YREVR, acessível *online* no endereço http://www.dgsi.pt [acedido em 16 de Dezembro de 2016];

- Acórdão do Tribunal da Relação de Lisboa, de 19.06.2014, proferido sob o processo n.º 1695/09.5PJLSB.L1-9, acessível *online* no endereço http://www.dgsi.pt [acedido em 16 de Dezembro de 2016];

- Acórdão do Tribunal da Relação de Lisboa, de 15.07.2008, proferido sob o processo n.º 3453/2008-5, acessível *online* no endereço http://www.dgsi.pt/jtrl.nsf/0/9182245992c7c5d18025749000503b8c?OpenDocument [acedido em 18 de Dezembro de 2016];

- Acórdão do Tribunal da Relação de Guimarães, de 12.10.2009, proferido sob o processo n.º 1396/08.1PBGMR – A.G1, acessível *online* no endereço http://www.dgsi.pt/jtrg.nsf/86c25a698e4e7cb7802579ec004d3832/4c03909839f95d5f8025767e004f83fe?OpenDocument [acedido em 18 de Dezembro de 2016];

- Acórdão do Tribunal da Relação do Porto, de 27.01.2010, proferido sob o processo n.º 896/07.5JAPRT.P1, acessível *online* no endereço: http://www.dgsi.pt/jtrp.nsf/c3fb530030ea1c61802568d9005cd5bb/68fdcdf35dc62b6e802576c40041c7 9 [acedido em 19 de Dezembro de 2016];

- Acórdão do Segundo Senado do Tribunal Constitucional Federal Alemão, de 02.03.2006, *apud* RAMOS, Vânia Costa, Âmbito e Extensão do Segredo das Telecomunicações, Revista do Ministério Público, n.º 11, Out./Dez. 2007, p. 147;

- Acórdão do Tribunal de Justiça da União Europeia, de 08.04.2014;

- Acórdão do Tribunal Constitucional n.º 210/2017, de 27.04.2017, disponível *online* no endereço http://www.tribunalconstitucional.pt/tc//tc//tc/acordaos/20170210.html [acedido em 11 de Maio de 2017];

- Acórdão do Tribunal da Relação do Porto, de 24.04.2013, proferido sob o processo n.º 585/11.6PAOVR.P1, disponível *online* no endereço: http://www.dgsi.pt/jtrp.nsf/d1d5ce625d24df5380257583004ee7d7/872f3063233d8de480257b78003e60f3?OpenDocument [acedido em 05 de Abril de 2017];

- 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* no endereço: http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/d10c400a16882e9e80257853005d65c1?OpenDocument [acedido em 05 de Abril de 2017];

- 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* no endereço http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/e5ed1936deb44eb180257824004ab09d?OpenDocument [acedido em 02 de Janeiro de 2017];

- Acórdão do Tribunal da Relação de Guimarães, de 29.03.2011, proferido sob o processo n.º 735/10.0GAPTL – A.G1, disponível *online* no endereço http://www.dgsi.pt/jtrg.nsf/86c25a698e4e7cb7802579ec004d3832/6aa96edf91e899b2802578a00054631f?OpenDocument [acedido em 05 de abril de 2017];

- Acórdão do Tribunal da Relação do Porto, de 07.06.2016, proferido sob o processo n.º 2039/14.0JAPRT.P1, disponível *online* no endereço http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/cffe710b2cb8d91e8025800500475ea9?OpenDocument [acedido em 03 de Março de 2017];

- Acórdão do Tribunal da Relação de Lisboa, de 22.01.2013, disponível *online* no endereço http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/7bd2dd8af10b34c380257b27003a5697?OpenDocument [acedido em 15 de abril de 2017];

- Acórdão do Tribunal da Relação de Évora, de 06.01.2015, proferido sob o processo n.º 6793/11.2TDLSB-A.E1, disponível *online* no endereço http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/847dae6b85353cb880257de10056ff4c?OpenDocument. [acedido em 11 de Maio de 2017];

- Acórdão do Tribunal da Relação de Lisboa, de 22.01.2013, proferido sob o processo n.º 581/12.6PLSNT-A.L1-5, disponível *online* no endereço http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/7bd2dd8af10b34c380257b27003a5697?OpenDocument [acedido em 13 de Maio de 2017];

- Acórdão do Tribunal da Relação de Coimbra, de 04.02.2015, proferido sob o processo n.º 73/14.9JALRA-A.C1, disponível *online* no endereço http://www.dgsi.pt/jtrc.nsf/8fe0e606d8f56b22802576c0005637dc/85a30a1f50f67a2780257de8004fd90b?OpenDocument [acedido em 15 de Maio de 2017];

- Acórdão do Tribunal da Relação de Évora, de 13.11.2012, proferido sob o processo n.º 315/11.2PBPTG-A.E1, disponível *online* no endereço

http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/d147ed8908009d4980257de10056f9c9?OpenDocument [acedido em 20 de Maio de 2017];

- Acórdão do Tribunal da Relação de Guimarães, de 29.03.2011, proferido sob o processo n.º 735/10.0GAPTL – A.G1, disponível *online* no endereço www.dgsi.pt [acedido em 21 de Maio de 2017];

- 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* no endereço www.dgsi.pt [acedido em 21 de Maio de 2017];

- Acórdão do Tribunal da Relação de Évora, de 13.11.2012, proferido sob o processo n.º 315/11.2PBPTG-A.E1, disponível *online* no endereço http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/d147ed8908009d4980257de10056f9c9?OpenDocument [acedido em 19 de Maio de 2017];

- Acórdão do Tribunal da Relação de Guimarães, de 12.04.2010, proferido sob o processo n.º 1341/08.4TAVCT, disponível *online* no endereço http://www.dgsi.pt/jtrg.nsf/-/045285606F260EF2802577180050FDF9 [acedido em 25 de Junho de 2017];

- Acórdão do Tribunal da Relação do Porto, de 05.04.2017, proferido sob o processo n.º 671/14.0GAMCN.P1, disponível *online* no endereço http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/16ebc99e65fc19038025810c0051991a?OpenDocument [acedido em 1 de Junho de 2017].

Pareceres e Notas Práticas

- Parecer n.º 21/2000, de 16/06, do Conselho Consultivo da Procuradoria Geral da República, disponível *online* no endereço http://www.dgsi.pt/pgrp.nsf/7fc0bd52c6f5cd5a802568c0003fb410/58101f7b2b6fb7818025689e00501437?OpenDocument&Highlight=0,P000212000 [acedido em 3 de Dezembro de 2016];

- Parecer n.º 16/94/complementar, de 24.06.1994, disponível *online* no endereço http://www.dgsi.pt/pgrp.nsf/6be0039071f61a61802568c000407128/9bd8d477f5dbc3fd80256617004225d4?OpenDocument [acedido em 3 de Dezembro de 2016];

- Nota prática n.º1/2012, da Procuradoria-Geral da República (Gabinete do Cibercrime), disponível *online* no endereço http://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/nota_pratica_1_pedido_de_ip.pdf [acedido em 18 de Dezembro de 2016];

- Nota prática n.º 8/2016, de 18/02, da Procuradoria-Geral da República (Gabinete do Cibercrime), disponível *online* no endereço http://cibercrime.ministeriopublico.pt/destaque/nota-pratica-no-82016 [acedido em 05 de Junho de 2017]

Links Relevantes

- Intervenção de Bill Gates no *World Economic Forum* - disponível *online* no endereço https://www.microsoft.com/presspass/ofnote/01-03davos.mspx [acedido em 25 de Agosto de 2016];

- Estudo da *Bareme Internet (Grupo Marktest)* - disponível *online* no endereço http://www.marktest.com/wap/a/n/id~209b.aspx [acedido em 5 de Setembro de 2016];

- Comunicação da Comissão ao Parlamento Europeu, ao Conselho e ao Comité das Regiões: *Rumo a uma política geral de luta contra o Cibercrime* - disponível *online* no endereço http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=URISERV:l14560 [acedido em 25 de Setembro de 2016];

- Publicação da EUROPOL, *High Tech Crimes Within The EU: Old Crimes New Tools, New Crimes New Tools, Threat Assessment, High Tech Crime Centre* - disponível

online no endereço https://www.enisa.europa.eu/topics/nationalcsirtnetwork/files/eventfiles/ENISA_Europol_threat_assessment_2007_Dileone.pdf [acedido em 25 de Setembro de 2016].

- Procedimentos avançados pelo Scientific Working Group on Digital Evidence (FBI) - Informação disponível *online* em https://archives.fbi.gov/archives/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm [acedido em 23 de Novembro de 2016];

- Missão, valores, atribuições e poderes da ANACOM - disponível *online* no endereço http://www.anacom.pt/render.jsp?categoryId=381611#.VSkKANzF9yU [acedido em 05 de Janeiro de 2017];

- Exposição de Motivos da Proposta de Lei n.º289/X - disponível *online* no endereço http://app.parlamento.pt/webutils/docs/doc.pdf?path=6148523063446f764c3246795a5868774d546f334e7a67774c336470626d6c7561574e7059585270646d467a4c31677664475636447397a4c334277624449344f5331594c6d527659773d3d&fich=ppl289X.doc&Inline=true [acedido em 4 de Março de 2017];

- Informação sobre as Cartas da Nigéria - disponível *online* no endereço http://www.apav.pt/cibercrime/ [acedido em 25 de Março de 2017];

- Informação sobre o *malware Mirai* - disponível *online* no endereço http://www.acriacao.com/sexta-feira-dyn-e-o-inicio-da-guerra-cibernetica/ [acedido em 30 de Março de 2017].

- Informação relativa à leitura dos *e-mails* dos utilizadores por parte da Google - disponível *online* no endereço https://www.google.pt/intl/en/policies/terms/regional.html [acedido em 15 de abril de 2017];

- Artigo publicado no jornal "Sol" no dia 08.03.2017 - disponível *online* no endereço https://sol.sapo.pt/artigo/552582/processo-penal-verdades-indiziveis [consultado a 16 de Abril de 2017];

- Informação que a encriptação é possível em determinados *Webmails* - disponível *online* no endereço http://exameinformatica.sapo.pt/noticias/internet/2014-03-21-Google-passa-a-encriptar-todas-as-mensagens-do-Gmail [consultado a 3 de Junho de 2017].

Figura (s)

- Fig.1 – Figura alusiva ao processo de envio/receção de uma mensagem de correio eletrónico da autoria de Pedro Penha Leitão da Costa Marques, retirada da Dissertação de Mestrado em Segurança em Sistemas de Informação, intitulada "*Informática Forense - Recolha e Preservação da Prova Digital*", Universidade Católica Portuguesa Faculdade de Engenharia, Maio, 2013, p. 81.