Universidade do Minho
Escola de Direito

José Pedro Coutinho Barreiros de Freitas

Os Meios de Obtenção de Prova Digital na Investigação Criminal: o Regime Jurídico dos Serviços de Correio Eletrónico e de Mensagens Curtas

Outubro de 2017

Os Meios de Obtenção de Prova Digital na Investigação Criminal: o Regime Jurídico dos Serviços de Correio Eletrónico e de Mensagens Curtas
José Pedro Freitas

UMinho | 2017

Universidade do Minho
Escola de Direito

José Pedro Coutinho Barreiros de Freitas

Os Meios de Obtenção de Prova Digital na Investigação Criminal: o Regime Jurídico dos Serviços de Correio Eletrónico e de Mensagens Curtas

Dissertação de Mestrado

Mestrado em Direito e Informática

Trabalho efetuado sob a orientação do

Professor Doutor Alexandre Júlio Teixeira Santos

Professor Doutor Pedro Miguel Fernandes Freitas

Outubro 2017

DECLARAÇÃO

Nome: José Pedro Coutinho Barreiros de Freitas

Endereço eletrónico: jose.pedrocbfreitas@gmail.com

Número do Cartão de Cidadão: 14384323 0 ZY8

Título dissertação: Os Meios de Obtenção de Prova Digital na Investigação Criminal: o Regime Jurídico dos Serviços de Correio Eletrónico e de Mensagens Curtas

Orientadores:

Professor Doutor Pedro Miguel Fernandes Freitas

Professor Doutor Alexandre Júlio Teixeira Santos

Ano de conclusão: 2017

Designação do Mestrado: Mestrado em Direito e Informática

Universidade do Minho, __/__/____

Assinatura:

_____

AGRADECIMENTOS

Porque a investigação e redação da presente dissertação seria completamente impossível sem o apoio e a ajuda prestados por várias pessoas, desde já, um enorme e especial obrigado. No entanto, antes de começar a exposição, cumpre agora individualizar todos aqueles que contribuíram, de forma notória, para a realização da presente investigação, fazendo com que este caminho não fosse trilhado solitariamente.

Primeiramente, aos meus pais e irmão por toda a ajuda, paciência, apoio, conforto e carinho incondicional, seria injusto da minha parte não prestar o maior dos agradecimentos.

Em segundo lugar, gostava de agradecer à minha família e amigos, por serem de e para a vida, que direta ou indiretamente contribuíram para a realização deste trabalho e por todos os bons momentos.

Aos meus colegas e amigos da N-ADVOGADOS – Nuno Albuquerque, Deolinda Ribas – Sociedade de Advogados, RL, por toda a paciência, conselhos, conversas e ensinamentos transmitidos tanto a nível profissional como pessoal.

Last but not least, gostaria de deixar um reconhecimento público de agradecimento aos Professores Doutores Pedro Freitas e Alexandre Santos pela persistência, rigor, exigência e disponibilidade em ajudar e orientar a presente dissertação, desde o primeiro dia. Sem este contributo este trabalho seria completamente impossível.

Um obrigado a todos aqueles que fizeram desta jornada de seis anos na Universidade do Minho os melhores anos da minha vida.

MODO DE CITAR

Na presente dissertação optamos por referenciar toda a bibliografia de acordo com as normas portuguesas da série 405 sobre referências bibliográficas, publicadas pelo I.P.Q. (Instituto Português da Qualidade). Assim, ao referenciar-se uma obra, pela primeira vez, utilizaremos o nome do autor (o último apelido em maiúsculas e o(s) primeiro(s) nome(s) em minúsculas), seguido do título da obra, em itálico, edição e suas características, volume, publicação (local: nome do editor, ano e páginas), sendo que, nas posteriores identificações da mesma obra utilizar-se-á a expressão "*op. cit*". Por outra banda, ao fazer-se a referência a mais do que uma obra do mesmo autor, para além da expressão *supra* identificada (nos casos em que a obra já foi previamente mencionada), utilizaremos as primeiras palavras do título seguida de reticências (por exemplo, RODRIGUES, Benjamim Silva*, Da Prova Penal, Tomo IV..., op. cit.*). Na bibliografia final será incluído o ISBN.

No caso de capítulos e/ou artigos científicos de livros e/ou revistas também serão referenciados pelo nome do autor, título do capítulo e/ou artigo, nome do organizador, número de edição (se aplicável), ano e páginas. Na respetiva bibliografia final indicaremos a primeira e última página do respetivo capítulo e/ou artigos científico.

Se estivermos perante o caso de uma obra com mais de 3 autores, indicaremos o nome do primeiro autor seguido da expressão "*et al.*".

Já noutra senda, quando a referência for exatamente igual à que antecede, ou seja, quando estivermos perante o mesmo autor e a mesma obra/capítulo/artigo, em notas de rodapé seguidas, utilizaremos a expressão "*idem*". Se estivermos perante o mesmo autor, a mesma obra e a mesma página, empregaremos o termo "*idem, ibidem*".

Ao referenciar jurisprudência indicaremos o tribunal emissor, data de prolação e *website* onde se encontra disponível.

Por fim, na bibliografia final, a ordenação das obras do mesmo autor assentará num critério meramente alfabético.

RESUMO

"Os Meios de Obtenção de Prova Digital na Investigação Criminal: o Regime Jurídico dos Serviços de Correio Eletrónico e de Mensagens Curtas"

O presente estudo resume-se à análise dos problemas decorrentes da nova realidade digital, nomeadamente, a cibercriminalidade, que, por sua vez, vem reclamar uma particular interpretação, adaptação e adequação por parte do Direito, ao nível do enquadramento e tratamento jurídico-processual penal. Este trabalho tem como principal propósito o esclarecimento acerca das dificuldades sentidas com a prova digital, o caso concreto das comunicações eletrónicas e da sua obtenção que, pela sua natureza volátil, em nada facilita o expediente dos órgãos de polícia criminal.

Numa sociedade cada vez mais célere e digital, em boa verdade, parece mentira que o fenómeno da cibercriminalidade seja uma realidade tão pouco abordada na doutrina e jurisprudência portuguesa e até mesmo pelo próprio curso de Direito. Pelo que, hoje, se impõe, não só a investigação sobre aquele que é um dos principais meios de excelência na prática de um crime, como ainda uma visão histórica na sua consagração legislativa.

Assim, num primeiro capítulo deste estudo, pretendemos enquadrar juridicamente o passado e presente dos meios de obtenção de prova no regime processual penal português, distinguindo-se da prova e dos meios de prova.

Posteriormente, abordaremos a realidade do cibercrime e toda a sua consagração legislativa, desde o Código Penal, à Lei do Cibercrime, não deixando de lado a Lei da Criminalidade Informática, nem a Convenção sobre a Cibercriminalidade. De seguida, numa perspetiva informática, avaliaremos principalmente a arquitetura dos serviços de *e-mail* e *SMS*.

Finalmente, dedicar-nos-emos ao principal objetivo da presente dissertação, ou seja, à apreensão e interceção dos serviços de correio eletrónico e de mensagens curtas, não esquecendo a sua envolvente e complexa teia legislativa.

Palavras-chave: cibercrime, meios de obtenção de prova, correio eletrónico e mensagens curtas.

ABSTRACT

"The Methods of Obtaining Digital Evidence in Criminal Investigation: The Legal Regime of E-mail and Short Message Services"

This study concerns the analysis of the problems arising from the new digital reality, namely the cybercrime, which, in turn, demands a suitable interpretation and adaptation by the Law, at the level of the legal framework and criminal procedure treatment. The main purpose of this work is to clarify the difficulties experienced by the digital evidence, the specific case of electronic communications and its acquisition, which, due to its volatile nature, increases the level of difficulty for the criminal police agencies.

In an increasingly fast and digital society, indeed, it seems to be a lie that the phenomenon of cybercrime is a reality so poorly approached in the Portuguese doctrine and jurisprudence, and even in the law degree itself. Therefore, nowadays, it is necessary to investigate one of the main means in the practice of a crime, but also its legislative historical vision.

Thus, in the first chapter of this study, we intend to legally frame the past and the present of the methods to obtain evidence in the Portuguese criminal procedure, distinguishing itself from the evidence and the means of proof.

Following the study, it will be addressed the reality of cybercrime and all its legislative consecration, from the Penal Code to the Cybercrime Law, without leaving aside neither Law on Computer Crime, or the Convention on Cybercrime. Afterwards, from an informatic perspective, we will mainly assess the architecture of electronic mail and short message services.

Finally, we will focus on the main purpose of this dissertation, that is the seizure and interception of electronic mail and short message services, not forgetting its complex legislation.

Keywords: cybercrime, methods of obtaining evidence, e-mail and short message services.

ÍNDICE

LISTA DE SIGLAS E ABREVIATURAS

Al. – Alínea

AR – Assembleia da República

Art.º – Artigo

Cfr. – Confrontar

CP – Código Penal

CPP – Código de Processo Penal

CRP – Constituição da República Portuguesa

DL – Decreto-Lei

E.g. – Exempli gratia, «por exemplo»

E-mail – Electronic mail, «correio eletrónico»

Et al. – Et alii, «e outros»

EUA – Estados Unidos da América

I.e. – Id est, «isto é»

Ipsis Verbis – literalmente, «pelas mesmas palavras»

JIC – Juiz de Instrução Criminal

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

MMS – Multimedia Messaging Service, «serviço de mensagens multimédia»

MP – Ministério Público

N.º – Número

Op. cit. – Opus citatum, «obra citada»

OPC – Órgãos de Polícia Criminal

P. – Página

P. e p. – Previsto e punido

PC – Personal Computer

PJ – Polícia Judiciária

PKI – Public Key Infrastructure, «Infraestruturas de Chaves Públicas»

PP. – Páginas

PR – Presidente da República

RGIT – Regime Geral das Infrações Tributárias

SMS – Short Message Service, «serviço de mensagens curtas»

Ss – Seguintes

STJ – Supremo Tribunal de Justiça

Vd – Vide, «veja-se em»

INTRODUÇÃO

A comunicação pressupõe uma relação entre duas ou mais entidades cujo principal objetivo se traduz na transmissão de uma mensagem que poderá ser feita "cara a cara", ou seja, pessoalmente, ou efetuada sem a copresença de um emissor e recetor, i.e., à distância. Neste último caso, ou seja, quando a transmissão da mensagem deixa de ser realizada num único momento, o ato comunicacional só se torna perfeito no momento em que o destinatário receciona a mensagem, apesar de a comunicação iniciar-se no momento em que o emissor pressiona a opção enviar/*send* [1].

É comumente sabido que a evolução tecnológica provocou na sociedade mundial variadíssimas transformações sendo possível constatar uma evolução tão frenética e célere que, por sua vez, obrigou à restruturação do pensamento da sociedade do séc. XXI, diante da atual realidade digital. É neste contexto que as novas tecnologias de informação e comunicação consentem a conceção de diversas modalidades de negócio e centros de discussões envolvendo tanto empresas, como os próprios cidadãos, na utilização de novos meios digitais.

É nesta transformação da sociedade em que vivemos, cada vez mais digital e eletrónica, que o estudo que se pretende levar avante se mostra pertinente no quadro jurídico da investigação criminal em concreto que, por sua vez, vem reclamar um novo manuseamento e especiais cautelas ao nível do enquadramento e tratamento jurídico-processual penal. Melhor dizendo, porque não podemos, enquanto juristas e profissionais do Direito, fechar os olhos a esta nova realidade social, globalizada e informatizada, cuja influência se estende, como não podia deixar de ser, aos meios de obtenção de prova digital, bem como à própria prova, modificando assim o paradigma das ciências jurídico-criminais, a própria atuação dos órgãos de polícia criminal, do Ministério Público, dos Magistrados e dos advogados em geral. Pelo que, sendo o Direito uma ciência, tudo aquilo que ele engloba terá sempre de se readaptar ao tempo e ao espaço vigente sob pena de se tornar desajustado e insuficiente face às necessidades da atualidade.

[1] A este propósito, NEVES, Rita Castanheira, *As ingerências nas comunicações electrónicas em processo penal: natureza e respectivo regime jurídico do correio electrónico enquanto meio de obtenção de prova*, Coimbra, Coimbra Editora, julho 2011, p. 15 e ss.

Assim, se no séc. XX fenómenos como a Internet, correio eletrónico, mensagens curtas, redes sociais, entre outros, eram trilhos pouco explorados e sem grande relevância na comunidade em geral e na criminalidade em concreto, hoje, graças à crescente adaptação e utilização das Tecnologias de Informação e Comunicação, tal contacto tornou-se verdadeiramente indissociável do comum cidadão, influenciando todos os aspetos da vida corrente. Portanto, a prova digital passou a ser um assunto da ordem do dia, na medida em que os dispositivos eletrónicos, ou a própria *web*, são as ferramentas mais utilizadas para o armazenamento de dados e de informação.

É com base na crescente utilização da informática que novas questões têm vindo a ser colocadas e consequentemente se reclamam respostas rápidas e eficientes por parte do Direito, que vão desde a apreensão e/ou interceção de realidades imateriais à desterritorialização do fenómeno do cibercrime[2] que ultrapassa as fronteiras geográficas e envolve múltiplas perspetivas. Nas doutas palavras de PEDRO VERDELHO "A fronteira que delimita o crime não é consistente nem foi ainda suficientemente interiorizada pela comunidade cibernética. E, neste contexto, criminalidade rima com criatividade"[3].

É por demais evidente que o cibercrime (criminalidade gerada especificamente através do auxílio informático) é uma tendência real e concreta e que este tipo de crimes representa hoje uma grande parcela dos crimes investigados em Portugal, assistindo-se à sua constante proliferação[4], nas mais diferentes modalidades de crime e sob as mais variadíssimas formas[5]. A verdade é que a criminalidade informática inclui não só os crimes previstos na Lei do Cibercrime, Lei n.º 109/2009, de 15 de setembro, mas também outros crimes que não se encontram previstos *ipsis verbis* nesta lei, mas sim noutros preceitos legais como, por exemplo, o crime de devassa por meio de informática, ou o crime de burla informática e nas comunicações, p. e p., nos termos dos artigos 193.º e 221.º do CP. Para além destes, ainda a

---

[2] Sobre esta temática, SOUSA, Miguel Teixeira de, "*O valor probatório dos documentos electrónicos*", Direito da Sociedade da Informação – Volume II, FDUL – Faculdade de Direito da Universidade de Lisboa / APDI – Associação Portuguesa de Direito Intelectual, Coimbra, Coimbra Editora, 2001, pp. 171 e 172.

[3] Cfr. VERDELHO, Pedro, "*A obtenção de prova no ambiente digital*", Revista do Ministério Público, Ano 25.º, nº 99 julho-setembro 2004, p. 119.

[4] Neste sentido, Relatório Anual de Segurança Interna – Ano 2016, p. 33, disponível em http://app.parlamento.pt/webutils/docs/doc.pdf?path=6148523063446f764c324679626d56304c334e706447567a4c31684a53556c4d5a5763765130394e4c7a464451554e4554456376524739 6a6457316c626e52766330567564476c6b5957526c6330563464475679626d467a4c7a557a595455304e5463784c546b784d5449744e4451774d6931685a6a41784c5751315a545269596a45335954646b4d7935775a47593d&fich=53a54571-9112-4402-af01-d5e4bb17a7d3.pdf&Inline=true [Consultado em 10.09.2017].

[5] Notícia "Cibercrime com maior crescimento no crime económico", disponível em https://www.noticiasaominuto.com/tech/377668/cibercrime-com-maior-crescimento-no-crime-economico [Consultado em 10.09.2017].

título meramente exemplificativo, podemos destacar aquele tipo de crimes cujo meio informático não é absolutamente necessário para a consumação do crime mas que, em todo caso, começa a ser cada vez mais recorrente o recurso à tecnologia informática, por exemplo, os crimes de ameaça, difamação, ou injúrias, p. e p., nos artigos 153.º, 180.º e 181.º do CP.

Importa sobretudo fazer um pequeno mas importante parêntesis, ora, para que seja possível falar deste novo fenómeno apelidado de "cibercrime" terá sempre que se ter em conta que a informática também pode ser considerada um bem jurídico-penal[6]. Isto é, para além de ser inicialmente vista como um bem jurídico lato e indeterminado que, consequentemente, acaba por ser um "simples" meio que auxilia a prática de um crime, também pode ser vista como uma realidade ofendida[7]. Assim, um dispositivo eletrónico pode não só constituir-se como um instrumento de um crime, como pode ser alvo do mesmo, ou um simples repositório de prova.

E porque ninguém está protegido neste âmbito, apesar de ser uma realidade tão atual que ninguém a pode negar, não é menos verdade que se multiplicam os processos-crime em torno destas matérias e, com eles, se revela muitas vezes a "ciberignorância" de muitos dos agentes que têm como profissão zelar pela boa administração e aplicação da Justiça, o que não deixa de constituir um verdadeiro entrave no desenvolvimento de estudos e meios que permitam uma eficaz luta contra o cibercrime.

Assim, juntamente com o desconhecimento e da falta de preparação *de quem de Direito*, uma das matérias que efetivamente necessita de ser avaliada e estudada, daí a escolha deste tema, são os meios de obtenção de prova na investigação cibercriminal. É portanto sob esta problemática, e porque cremos na sua utilidade prática, que estudaremos, para além da realidade do cibercrime, os meios de obtenção da prova digital, em específico a utilização do correio eletrónico e do serviço de mensagens curtas.

---

[6] De entre a pluralidade de definições e ausência do mínimo consenso, podemos afirmar que o bem jurídico é aquele bem que necessita de ser particularmente protegido, sendo esta a primacial função do direito penal. Neste sentido, COSTA, José de Faria, "*Sobre o objecto de protecção do direito penal: o lugar do bem jurídico na doutrina de um direito penal não iliberal*", Revista de Legislação e de Jurisprudência, ano 142.º, n.º 3978, Coimbra, Coimbra Editora, janeiro-fevereiro 2013, pp. 158 e 159.

[7] A título de exemplo, atente-se ao crime de reprodução ilegítima de programa protegido, p. e p. nos termos do art.º 8.º da LCiber, no qual o bem jurídico a proteger é o *software*, ou seja, um verdadeiro bem jurídico de cariz informático. Através deste tipo de ilícito podemos constatar a evolução da legislação portuguesa que atribui uma moldura penal com pena de prisão até três anos, ou com pena de multa, para aquele que reproduzir, divulgar ou comunicar ao público ilegitimamente um programa informático, bastando para tal sanção a mera tentativa.

A restrição no que toca ao objeto de estudo desta dissertação, mais concretamente ao setor das telecomunicações, como correio eletrónico e as mensagens curtas, deve-se ao facto de este tipo de comunicações se encontrarem totalmente inseridas na vida do comum utilizador e à primazia na sua utilização, apesar de todas as atualizações que têm sido feitas neste setor (resultado da enorme evolução tecnológica), permanecem ainda como um dos principais meios de comunicação.

Se, por um lado, podemos caracterizar o correio eletrónico como o sistema rápido e multifuncional que permite a troca de correspondência a partir de equipamentos ligados em rede, como um computador, telemóvel ou *tablet*, que podem ser acedidos em qualquer parte do mundo, através da Internet[8]. Por outro lado, o serviço de *SMS* define-se como o serviço eletrónico que consente o envio de mensagens de texto curtas (até 160 caracteres), entre telemóveis, e apesar de ser um serviço banalmente utilizado entre a generalidade das pessoas, tanto para comunicar com familiares e amigos como profissionalmente, caracteriza-se também por ser um meio de divulgação de campanhas comerciais, um meio de utilização de serviços de subscrição de meteorologia e/ou notícias, ou até mesmo um meio coadjuvante na consumação de um crime.

Tanto uma comunicação, como a outra, são realidades banais do quotidiano de qualquer cidadão, utilizadas a qualquer hora e em qualquer lugar, com uma enorme rapidez e eficácia. Se assim é, no âmbito jurídico-penal, estas comunicações eletrónicas também constituem um auxílio para a eficiente reprodução de ilícitos criminais informáticos, como ainda noutro tipo de ilícitos como, por exemplo, no âmbito do tráfico de droga/crianças/armas, ou até mesmo o crime de perseguição, e tantos outros que hoje em dia é quase indissociável a prática de qualquer crime da utilização dos meios de comunicação eletrónica.

A verdade é que o cibercrime reavivou a problemática da prova, não deixando de lado os meios de obtenção de prova e, como se não bastasse, falamos aqui de bens que não são suscetíveis de apreensão material, ou seja, bens que não passam de sequências binárias e que, por isso, justificam a novidade dos meios de obtenção de prova nesta sede. Enquanto que um meio de prova é um meio através do qual o julgador se vai auxiliar para formar a convicção

[8] Nesta senda, RAMOS, Armando Dias, *A prova digital em processo penal: o correio eletrónico*, 2.ª edição atualizada e ampliada, Chiado Editora, Lisboa, fevereiro 2017, versão *e-book*, pp. 23 e 24.

sobre um determinado facto[9] , o meio de obtenção de prova, por seu turno, é um instrumento utilizado pelas autoridades judiciárias na investigação e recolha do meio de prova, ou seja, é "o caminho" que as entidades competentes têm de percorrer para alcançar a real prova e serve para obter declarações/coisas acerca de um determinado acontecimento, sempre de acordo com o princípio da dignidade da pessoa humana[10].

Foi face à necessidade de tratamento diverso, concretamente, em termos de obtenção da prova digital que surgiu a LCiber que, pese embora estabeleça aspetos substantivos, também regula as medidas que têm como objetivo a descoberta da verdade material e preservação dos elementos de prova digital.

Assim, o presente estudo, como certamente as passagens anteriores já revelaram, iniciar-se-á com a mais elementar contextualização através de um breve enquadramento jurídico revelador da verdadeira estrutura acusatória do direito processual penal português. Aqui, discutiremos qual a diferença entre a prova, os meios de prova e os meios de obtenção de prova, distinção essa que graças à sua tenuidade, nem sempre é clara e percetível.

De seguida, iremos abordar o fenómeno do cibercrime e a constante dependência informática por parte da sociedade da informação. Quem é que são os seus principais agentes? Será que todo o *malware* é aquilo a que geralmente apelidamos de "vírus" e será que todos os piratas informáticos têm em vista a prática de um crime? Afinal quais são as principais conceções metodológicas do fenómeno do Cibercrime e quais as suas diferenças? Será que essas diferenças têm algum relevo prático? Por fim, qual é a verdadeira consagração legislativa do cibercrime?

Por sua vez, o terceiro capítulo será reservado para as questões técnicas relativas aos serviços de correio eletrónico e de mensagens curtas, bem como às duas definições. Salientamos, desde já, que não pretendemos com a presente dissertação discorrer sobre todas as questões informáticas interligadas com este tipo de comunicações eletrónicas, tendo em conta que o nosso objetivo passa por trilhar por caminhos do foro jurídico e de Direito. Contudo,

[9] JESUS, Francisco Marcolino, *Os Meios De Obtenção Da Prova Em Processo Penal*, 2ª edição rev., at. e amp, Coimbra, Almedina, março 2015, p. 179 e ss.

[10] Apesar de a verdade ser sempre bem-vinda, não nos podemos esquecer que foi uma pessoa que praticou o crime, logo não podemos ter como princípio da investigação que "os meios justificam os fins".

tendo em conta a abertura de horizontes técnico-informáticos que aqui se reclama, seria limitador da nossa parte não fazer uma correta menção à arquitetura destes serviços.

Por fim, iremos entrar no núcleo duro deste estudo e será aqui que, novamente, tentaremos responder a uma variedade de questões provocadas pela atual encruzilhada legislativa do direito processual penal português, no âmbito das comunicações eletrónicas. Será que devemos aplicar o mesmo regime jurídico ao correio eletrónico, às mensagens curtas, às escutas telefónicas e à correspondência tradicional? Será que a LCiber veio revogar as consagrações relativas aos meios de obtenção de prova previstos no CPP? O que é necessário para a apreensão e/ou interceção de uma comunicação eletrónicas? Qual a sua diferença e sob pena de que consequência?

Ora, em virtude do tema escolhido para a elaboração da Dissertação de Mestrado em Direito e Informática destacamos a imprescindibilidade, para a cientificidade desejada, que nos afastemos de considerações e de pré-conceitos mais íntimos e procuraremos, para o efeito, alicerçar todas as ilações com a melhor sabedoria dos nossos *mui* doutos doutrinários das áreas de Direito Penal e Processual Penal, com especial enfoque nos estudos versados nos meios de obtenção de prova digital, nomeadamente, o regime jurídico dos serviços *e-mail* e *SMS*.

Os novos meios tecnológicos de informação e comunicação alteraram definitiva e drasticamente o quotidiano social. No entanto, apesar da sua relevância e pertinência atual, o tratamento dado aos meios de obtenção de prova digital, e à prova com essas caraterísticas, especificamente, o correio eletrónico e as mensagens curtas, continuam a dar azo a interessantes e controversas discussões na doutrina portuguesa e na jurisprudência.

Entende-se, pois, que o que motiva à investigação desta temática sejam as constantes questões que se levantam em torno do regime aplicado aos serviços e-*mail* e *SMS* e, será nestes termos, que munidos do conhecimento necessário e pertinente, que procuraremos indagar sobre esta temática, levantando questões que cremos por oportunas para que, quiçá, se consiga fazer um contributo útil, porque científico e desinteressado, sobre a problemática que se apresenta a estudo.

CAPÍTULO I

O PASSADO E O PRESENTE DOS MEIOS DE OBTENÇÃO DE PROVA NO REGIME PROCESSUAL PENAL PORTUGUÊS

Neste primeiro capítulo pretendemos fazer uma breve e concisa abordagem de algumas especificidades e conceitos jurídicos que, tendo em conta a sua utilidade para os capítulos posteriores, não merecem o esquecimento.

Uma vez que, em regra, uma análise, ainda que breve, do passado dissipa de uma melhor forma as dúvidas do presente[11], é necessário fazer um enquadramento jurídico do que são os meios de obtenção de prova (distinguindo-os da prova e dos meios de prova) e os problemas que estes enfrentam face à sociedade da informação do séc. XXI, baseada na aquisição de informação através das redes comunicacionais.

1. Breve Enquadramento Jurídico

A Constituição caracteriza-se por ser a lei suprema de cada país, sendo a ordem fundamental das comunidades políticas[12] que todos os cidadãos têm o dever, obrigação e necessidade de respeitar. Na sua aceção mais clássica podemos afirmar que a Constituição de cada país é a ordem fundamental da comunidade política que responde aos problemas vitais que o tecido coletivo coloca[13].

[11] Neste sentido, VERDELHO, Pedro, *"Técnica no Novo C.P.P.: Exames, Perícias e Prova Digital"*, Revista CEJ, nº 9 (especial) – Jornadas sobre a Revisão do Código de Processo Penal, 1º Semestre 2008, p. 148.

[12] A este propósito, AMARAL, Maria Lúcia*, A Forma da República - Uma Introdução ao Estudo do Direito Constitucional*, Reimpressão, Coimbra, Coimbra Editora, outubro 2012, p. 11.

[13] Nas palavras da autora, as relações sociais carecem de princípios constitucionais que, no fundo, vêm responder a três principais problemas, nomeadamente: quem é que na comunidade é titular do poder; quem é que pertence ou está excluído da sociedade e, por fim, por que valores constitucionais é que uma comunidade se deve reger. Neste mesmíssimo sentido, AMARAL, Maria Lúcia, *op. cit.*, p. 19.

No interior de cada ordem jurídica estabelece-se uma hierarquia normativa, sendo as normas constitucionais aquelas que alcançam o lugar cimeiro na ordem legislativa e, por isso, é que a Constituição é a lei fundamental de cada Estado[14]. Se em Portugal a CRP é a fonte superior do ordenamento jurídico português, no qual o direito se sustenta – nas palavras de KELSEN[15], a *Grundnorm* – então qualquer norma é direta ou indiretamente reconduzida por esta fonte de direito. Isto é, pensando numa hierarquia, a Constituição sempre será o vértice superior e todas as demais fontes se desenvolvem com base nela e a partir dela.

Nas palavras mais eruditas de MARIA LÚCIA AMARAL, "(...) a unidade do ordenamento jurídico positivo é realizada, isto é, construída e reconstruída, tendo sempre a Constituição como ponto de partida e como ponto de chegada"[16]. Acresce ainda que é a própria CRP que no seu artigo 3.º expõe a sua primazia hierárquica segundo a qual a validade dos vários preceitos normativos depende da sua harmonização constitucional.

É através da unidade, concordância e adequação funcional que o sistema normativo complexo a que apelidamos de CRP vai exercer o seu impacto na teia legislativa, sendo os próprios Código Penal e Código de Processo Penal, que neste texto daremos mais relevância, exemplos disso mesmo.

Por um lado, o direito penal[17] é a ciência jurídica constituída por um conjunto de normas que definem os crimes e as respetivas sanções e regras para a sua aplicação, tendo como principal fundamentação e legitimação o comportamento criminoso e a respetiva consequência jurídica[18]. É a área do direito que vai refletir o equilíbrio da sociedade e das instituições políticas de cada momento[19]. O direito penal é o direito substantivo que se apresenta como um conjunto

---

[14] Ainda neste sentido, AMARAL, Maria Lúcia, *op. cit.*, p. 13.

[15] A este propósito, relembramos KELSEN, Hans, *Pure theory of law*, 5th printing, Univ. of California Press., p. 8, disponível em https://books.google.pt/books?redir_esc=y&hl=pt-PT&id=6XQNJe8-OdEC&q=gr#v=onepage&q=gr&f=false [Consultado em 17/09/2017].

[16] Porém, isto não significa que todo o direito seja Direito Constitucional e que todas as soluções são apresentadas e "sufocadas" por este. Cfr. AMARAL, Maria Lúcia, *op. cit.*, p. 94.

[17] Importa referir que, historicamente, era dada preferência ao designativo "direito criminal", contudo com a reforma das Faculdades de Direito de 1972 (DL 364/72, de 28 de setembro), as designações "pena" e "penal" (derivadas da expressão latina *poena*) ganharam cada vez mais preponderância prevalecendo, desde então, o vocábulo "direito penal". A este propósito, DIAS, Jorge de Figueiredo, *Direito Penal - Parte Geral - Tomo I - Questões Fundamentais; A Doutrina Geral do Crime*, 2.ª Edição - 2.ª Reimpressão, Coimbra, Coimbra Editora, outubro 2012, p. 4.

[18] FREITAS, Pedro Miguel Fernandes, *Determinação da medida da pena privativa de liberdade: um olhar crítico a partir do direito anglo-saxónico*, Braga, Universidade do Minho – Escola de Direito, setembro 2015, p. 48.

[19] Nesta senda, COSTA, José de Faria, *Noções Fundamentais De Direito Penal: (Fragmenta Iuris Poenalis): Introdução – A Doutrina Geral Da Infração [A Ordenação Fundamental Da Conduta (Facto) Punível; A Conduta Típica (O Tipo); A Conduta Ilícita (O Ilícito); A Conduta Culposa (A Culpa)]*, 4ª Edição, Coimbra, Coimbra Editora, setembro 2015, p. 139.

de normas que obedecem a uma intencionalidade procurando fazer com que todos os seus destinatários não pratiquem determinadas condutas criminosas, caso contrário, o Estado, através dos órgãos jurisdicionais, ver-se-á obrigado a aplicar as respetivas penas. O crime é a ação humana típica, ilícita e culposa punida por Lei, com sanção criminal[20]. O direto penal é um direito negativo, um direito que *não se cumpre*, é o direito de *não dever fazer*, no fundo, é a área do direito que indica como é que os agentes não se devem comportar e realiza-se quando cumpre as suas funções preventivas e protecionistas[21]. Poder-se-á afirmar que o direito penal tem como ponto de partida, e também de chegada, a realização da justiça penal historicamente situada, construindo-se como um ordenamento de paz, visando a defesa e proteção dos bens jurídicos que têm dignidade penal[22].

É a CRP que indica tudo o que é vital para a manutenção da sociedade, bem como do Estado de Direito, que deve ser condignamente protegido (bens jurídicos como a vida, a integridade física, saúde, património, a honra, segurança[23]). É na CRP que o direito penal encontra os seus verdadeiros fundamentos e limites[24], encontrando-se sempre vinculado a esta, *nullum crimen sine lege, nulla poena sine lege*[25]...

O direito penal é uma área jurídica teórica e abstrata como um verdadeiro direito substantivo deve ser, regulada mormente pelo CP e que só terá aplicabilidade prática através do direito processual penal, ou seja, através do direito adjetivo, principalmente instrumentado pelo CPP.

Deste modo, o Direito Processual Penal é o ramo do direito que indaga a ocorrência de um determinado crime, que tipo de crime, e averigua a necessidade de aplicação de uma determinada consequência jurídica a um agente criminoso. Quando ocorre um determinado

[20] JESUS, Francisco Marcolino, *op. cit.*, p. 11.

[21] Com isto pretendemos dizer que o direito penal visa a resolução de comportamentos ilícitos tidos como insuportáveis, pela sociedade em geral, prevenindo, deste modo, eventuais futuros crimes. Veja-se MONTE, Mário Ferreira, *Direito Processual Penal Aplicado*, Braga, AEDUM - Associação de Estudantes de Direito da Universidade do Minho, 2017, p. 44.

[22] A este propósito, COSTA, José de Faria, *Noções Fundamentais De Direito Penal..., op. cit.,* p. 11 e ainda MONTE, Mário Ferreira, *op. cit.*, p. 42.

[23] Neste sentido, COSTA, José de Faria, *Noções Fundamentais De Direito Penal..., op. cit.,* p. 14.

[24] Neste mesmo sentido, JESUS, Francisco Marcolino, *op. cit.*, p. 12.

[25] Do latim, "não há crime sem lei, não há pena sem lei", ou seja, o direito penal rege-se por critérios de estrita legalidade, cujo conteúdo essencial se reflete nas eruditas palavras de Figueiredo Dias "(...) não pode haver crime, nem pena que não resultem de uma lei prévia, escrita, estrita e certa". Cfr. DIAS, Jorge de Figueiredo, *op. cit.*, p. 177. Como tal só poderemos assistir a uma condenação se, e só se, tais factos forem previamente punidos por lei. COSTA, José de Faria, *Noções Fundamentais De Direito Penal..., op. cit.,* p. 119.

crime urge saber quem foi o seu autor[26]. Só podemos afirmar que ocorreu um crime quando, terminado o processo, conseguimos apurar a ocorrência de determinado facto criminoso e, o mais importante, quem é que foi o seu responsável. Apesar da sua independência teleológica, o direito processual penal realiza, complementa e disciplina o direito penal, fortificando essa mesma relação.

De acordo com o STJ[27], a finalidade do processo penal prende-se com a reposição da verdade e a realização da justiça[28] e será através destes dois pilares estruturais que se conseguirá averiguar que tipo de crime é que está em causa, quem é que o cometeu e se esse agente deve ser punido ou absolvido pela sua prática, com todas as garantias que isso implica.

O processo penal de hoje visa a descoberta da verdade material[29], a realização da justiça, bem como a proteção dos direitos fundamentais revelando, no seu todo, o conflito existente entre Homem/Estado[30]. Sendo o direito processual penal uma das várias ramificações do direito constitucional, i.e., direito constitucional aplicado[31], então o primeiro deve respeitar o segundo, como se de um ente querido se tratasse. Contudo, não nos podemos esquecer que

---

[26] Conforme a posição de MONTE, Mário Ferreira e LOUREIRO, Flávia Noversa, *Direito Processual Penal – Roteiro de Aulas*, 2.ª ed. revista e atualizada, Braga, AEDUM – Associação de Estudantes de Direito da Universidade do Minho, 2014, p. 26.

[27] Cfr. Acórdão do Supremo Tribunal de Justiça de 18-02-2009, disponível em http://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/8e0a119937ab01188025757c0052bba3?OpenDocument [Consultado em 17.09.2017].

[28] Tal asserção prende-se com o facto que o direito processual penal não pode existir se não tiver em vista a verdade material e a aspiração da justiça ideal e teoreticamente justificável de acordo com o direito substantivo. No entanto, não podemos afirmar que o processo penal conduzirá sempre a absolvições ou condenações materialmente justas. Assim o refere, com inteira razão, DIAS, Jorge de Figueiredo, *Clássicos Jurídicos – Direito Processual Penal (Reimpressão da 1ª Edição de 1974)*, Coimbra, Coimbra Editora, junho 2004, pp. 43 e 44.

[29] O princípio da verdade material orienta o processo penal, enquanto que o princípio da verdade formal orienta o processo civil. A verdade do processo civil é uma verdade formal, ou seja, a verdade no processo civil é unicamente alcançada através dos elementos que são levados pelas partes para o processo (factos e provas), no entanto, no processo penal é o próprio juiz que pode investigar e carrear para o processo todos os meios de prova que julgue necessários. O juiz tem o poder de investigar autonomamente, podendo ordenar a produção de uma prova para a descoberta da verdade e da boa e criteriosa decisão da causa. A verdade material não é uma verdade obtida a qualquer preço, mas sim uma verdade judicial prática que apesar de não ser "absoluta" ou "ontológica" é processualmente válida, ou seja, é uma convicção de que certa alegação é aceitável por ter sido obtida por meios processualmente válidos. Neste sentido, MONTE, Mário Ferreira e LOUREIRO, Flávia Noversa, *op. cit.*, p. 32.

[30] Neste sentido, CORREIA, João Conde, *"Qual o significado de Abusiva Intromissão na Vida Privada, no Domicílio, na Correspondência e nas Telecomunicações (art. 32.º, n.º 8, 2ª parte da C.R.P.)?"*, Revista do Ministério Público, Ano 20.º, n.º 79, julho-setembro, 1999, p. 45.

[31] Formulação apresentada numa dupla dimensão: por um lado, os fundamentos do processo penal são os alicerces constitucionais do Estado, por outro lado a regulamentação dos problemas processuais tem uma conformação prevista constitucionalmente. O processo penal não só é a área do direito mais sensível às flutuações político criminais, como ainda a CRP vai ser sempre um ponto de referência direto ou indireto do direito processual penal. A este propósito, DIAS, Jorge de Figueiredo, *Clássicos Jurídicos..., op. cit.,* p. 74. Para mais desenvolvimentos sugere-se a leitura de ROXIN, Claus, *Derecho procesal penal/ Strafverfahrensrecht*, trad. de la 25ª ed. alemana de Gabriela E. Córdoba y Daniel R. Pastor; Rev. por Julio B. J. Maier, Buenos Aires, Editores del Puerto, s.r.l., 2001, p. 10. e, ainda, em sentido idêntico, MONTE, Mário Ferreira, *Direito Processual Penal Aplicado..., op. cit.,* pp. 53 – 61.

esta área do direito também tem as suas características e objetivos próprios principalmente no domínio da prova e dos seus meios de obtenção. Daí que parte do estudo que nos propusemos a fazer parta precisamente da medida em que será possível estabelecer um equilíbrio entre a CRP, e os seus princípios basilares e norteadores de todo o ordenamento jurídico, e a prossecução dos objetivos tutelados pelo Direito Processual Penal, ainda que limitados pela Lei Fundamental.

2. A estrutura acusatória do direito processual penal português

É com base no princípio da investigação[32] que o processo penal português tem, seguramente, uma estrutura acusatória sustentada pela prova, sob pena de a pretensão não ser acolhida por *quem de direito*. A investigação jamais poderá ficar dependente de uma possível confissão dos factos pelo arguido, devendo ser sempre que possível eficaz e inequívoca[33].

A prova nada mais é do que um meio através do qual são revelados factos significativos para a ocorrência de determinado crime, punibilidade do criminoso e determinação da pena, ou medida de segurança, consistindo na demonstração da sua realidade em juízo[34]. Para além dessa demonstração de verdade, a prova deve também criar uma real convicção de factos juridicamente relevantes que, simplesmente, não são graduáveis, ou existem, ou não existem.

Para que haja a condenação de um sujeito é necessário que seja feita prova dos elementos tipo de crime e que esse agente tenha efetivamente violado a nossa lei. No entanto, mesmo que a prova indicie com quase todas as certezas que determinado sujeito praticou um crime, essas mesmas convicções são extremamente difíceis de concretizar, graças ao simples facto que os órgãos jurisdicionais não estiveram presentes no momento da alegada prática do crime e muito menos têm acesso aos desejos mais profundos do agente criminoso. Imaginando um cenário um pouco grotesco, convidamos a que suponha que determinado sujeito foi vítima de um crime de homicídio, ora se todas as provas indicassem um sujeito como o autor de tal

[32] Princípio que se traduz na investigação autónoma e independentemente dos contributos de acusação e da defesa, por parte dos tribunais. Assim o refere, com inteira razão, ANTUNES, Maria João, *Direito Processual Penal*, Coimbra, Almedina, abril 2016, p. 164.

[33] COELHO, António Manuel Mendes, "*Meios de Prova e Meios de Obtenção de Prova*", Verbo Jurídico, dezembro 2006, p. 4, disponível em http://www.verbojuridico.net/doutrina/penal/penal_meiosprova.pdf [Consultado em 17/09/2017].

[34] A este propósito, JESUS, Francisco Marcolino, *op. cit.*, p. 84.

crime, o certo é que nem sempre se concretiza a existência de uma certeza confortável a fim de ser possível uma condenação. Por vezes, nem mesmo as provas consideradas como mais exatas ou inequívocas permitem lograr descobrir quem foi o autor da prática de um determinado crime dada a multiplicidade de factos que, por vezes, constituem uma realidade e, até mesmo, as várias perceções do que foi "verdade" de testemunhas e outros intervenientes num processo.

Em todo caso, uma vez que a prova pretende demonstrar factos relevantes para a existência de um ilícito e, a consequente, aplicabilidade de uma pena, não podemos deixar de mencionar que esses factos são demonstrados através de meios de prova. Portanto, podemos concluir que os meios de prova são fontes de convencimento legais que se distinguem da própria prova, uma vez que é através destes meios que o legislador se vai servir para gerar a real convicção sobre um determinado facto, introduzindo no procedimento pelo menos um elemento de prova[35]. Melhor dizendo, os meios de prova caracterizam-se por ser o caminho a percorrer e a prova, *strictu sensu*, o destino ou resultado que se ambiciona.

A título de exemplo, perante um tipo de prova pessoal como a testemunhal, o meio de prova será a testemunha; por outro lado, numa prova real que resulta da observação de coisas, como a prova documental, o meio de prova será a coisa/documento[36].

Distintos da prova e dos meios de prova, são os meios de obtenção de prova, que se caracterizam por ser os instrumentos através dos quais as autoridades judiciárias se vão servir para investigar, analisar e obter os meios de prova, como por exemplo os exames, as revistas e buscas, apreensões ou as escutas telefónicas[37]. Nas eruditas palavras de MARIA JOÃO ANTUNES "Na perspetiva técnico-operativa os meios de obtenção de prova caracterizam-se pelo modo e também pelo momento da sua aquisição no processo, em regra nas fases preliminares, sobretudo no inquérito"[38].

---

[35] JESUS, Francisco Marcolino, *op. cit.*, p. 145.

[36] Se o meio de prova é a testemunha, as suas declarações/testemunho serão a prova; na prova documental o meio de prova é o pedaço de papel e a prova propriamente dita é o conteúdo desse papel, o "documento" propriamente dito é apenas uma reprodução reduzida a papel ou a outro elemento físico. Neste mesmo sentido, JESUS, Francisco Marcolino, *op. cit.*, p. 146. Outro exemplo pode ser retirado do Acórdão do Tribunal da Relação do Porto, de 01-06-2016, quando refere que: *As escutas telefónicas são um meio de obtenção de prova, mas as conversações recolhidas através dessas interceções constituem meio de prova; transcrito e inserido no processo o conteúdo das gravações possa a constituir prova documental submetida ao princípio da livre apreciação da prova.* Disponível em http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/1f85e373f004b9fd80257fd5004eda69?OpenDocument [Consultado em 22.10.2017].

[37] Ainda no mesmíssimo sentido, JESUS, Francisco Marcolino, *op. cit.*, p. 179.

[38] Cfr. ANTUNES, Maria João, *op. cit.*, p. 111.

Tendo por base a metáfora previamente mencionada, se os meios de prova são o caminho a percorrer e a prova o destino, os meios de obtenção de prova serão o instrumento usado para percorrer esse caminho. Atendendo ao facto de os meios de obtenção de prova poderem restringir os direitos, liberdades e garantias, os primeiros necessitam de ser adequados e proporcionais com a investigação em curso, devem ser previamente autorizados pela CRP e balizados por esta mesma[39]. A relação dos meios de obtenção de prova com a CRP é tão forte que a sua utilização deve ser sustentada por lei, ou decreto-lei autorizado, deve salvaguardar outros direitos ou interesses constitucionalmente protegidos, bem como encontrar-se prevista de forma geral e abstrata.

Claro está que nem sempre os preceitos constitucionais vão coincidir com a busca incessante da prova, gerando, por vezes, um mal-estar legislativo. Por exemplo, se protegermos em demasia os direitos fundamentais podemos colocar em causa a descoberta da verdade, mas se por outro lado, realizarmos uma busca pela verdade a todo custo podemos cair no risco de eliminar os mais elementares direitos[40]. Será na ponderação entre a salvaguarda de direitos e interesses fundamentais e o objetivo primordial da descoberta da verdade material do direito processual penal português que iremos encontrar as maiores dificuldades em conseguir equilibrar, de forma harmoniosa, os pratos da balança da justiça.

Apesar de existir uma certa abertura e simplificação no que concerne às investigações, traduzindo-se num fortalecimento dos poderes dos OPC[41] e fragilizando os princípios fundamentais como oralidade ou a publicidade, devemos ter presente que os meios de obtenção de prova só podem ser utilizados quando a prova é extremamente difícil, ou praticamente impossível, de se obter de outra forma. Por isso é que os meios de obtenção de prova como as escutas telefónicas são considerados a ultima *ratio* da investigação, tendo em conta o facto de serem bastante intrusivas na vida privada dos cidadãos, portadoras de uma elevada danosidade social, sendo, por esse motivo, alvos de grandes debates jurisprudenciais[42], violando vários direitos como a reserva da vida privada, ou o direito à intimidade.

---

[39] Veja-se, ABREU, Carlos Pinto de, "*Prova e meios de obtenção de prova, breve nota sobre a natureza e o regime dos exames no processo penal*", disponível em http://carlospintodeabreu.com/public/files/CPA_prova_meios_obtencao_prova.pdf [Consultado em 17/09/2017].

[40] Nesta senda, CORREIA, João Conde, *op. cit.*, p. 46.

[41] MILITÃO, Renato Lopes, "*A Propósito da Prova Digital no Processo Penal*", Revista da Ordem dos Advogados - ROA, 2012 (Ano 72), n° 1, p. 254..

[42] A título de exemplo veja-se a seguinte passagem do Acórdão do Supremo Tribunal de Justiça de 27-05-2009: *As escutas telefónicas, não constituindo meios de prova, mas meios de obtenção de prova, devem ser encaradas como um meio de obtenção de prova de ultima ratio e*

No entanto, em certas situações, são previstas e autorizadas limitações e restrições aos direitos fundamentais relacionados com a reserva da intimidade da vida privada quando os bens a proteger se traduzem na defesa e segurança pública e do Estado, bem-estar económico, prevenção e repressão criminais... Portanto, os direitos fundamentais não podem ser totalmente absolutos, podendo ser restringidos em algumas situações, *vd* art.º 18.º n.º 2 e 3 e 34.º n.º 4 da CRP. Este princípio da proibição do excesso demarca expressamente a autorização que o legislador tem de poder limitar, em algumas circunstâncias especificas, os direitos fundamentais, restrições essas que têm de constar obrigatoriamente na lei ou DL autorizado, têm de ter carácter geral e abstrato, sem efeitos retroativos, sendo crucial a sua justificação, adequação, necessidade e apropriação aos fins que se pretendem atingir[43].

Para que haja uma justiça cada vez mais eficiente e uma política ao serviço do povo é necessário que a sociedade democrática crie canais de informação sobre os seus cidadãos. No entanto, vamos sempre desabar no problema da reserva da intimidade da vida privada que se vai gladiar com a necessidade sentida pelos "organismos sociais" de recolher e processar as mais variadas informações. Importa, portanto, ter sempre presente o carater não absoluto da reserva da intimidade pessoal e a própria relatividade do seu conteúdo com as exigências práticas do caso em concreto.

A questão da restrição dos direitos fundamentais supõe um conflito positivo de normas constitucionais e, de acordo com RENATO LOPES MILITÃO, a regra para a solução deste mesmo conflito passa pela máxima observância dos direitos fundamentais em causa e da sua mínima restrição, compatível com a ressalva de um outro direito fundamental[44]. Nessa linha de pensamento e seguindo os ensinamentos de GOMES CANOTILHO e VITAL MOREIRA[45], em caso de dúvida, prevalece a interpretação segundo a qual se deve restringir o mínimo possível os direitos fundamentais, atendendo à especial atenção que os direitos fundamentais carecem e

---

nunca de prima ou sola ratio ou para se obter o flagrante delito; por essa razão, tem-se salientado a natureza excecional das escutas telefónicas no contexto dos diversos meios de obtenção da prova, por se ter presente a danosidade social elevada, já que fere o mais íntimo dos segredos do ser humano, cuja proteção emerge do direito à reserva da intimidade da vida privada e familiar. Disponível em http://www.pgdlisboa.pt/jurel/stj_mostra_doc.php?nid=27558&codarea=2 [Consultado em 17.09.2017].

[43] Ainda a este propósito, CORREIA, João Conde, *op. cit.*, p. 59.

[44] MILITÃO, Renato Lopes *op. cit.*, p. 270.

[45] Sobre esta temática, CANOTILHO, J. J. Gomes e MOREIRA, Vital, *Fundamentos da Constituição*, Coimbra, Coimbra Editora, novembro 1991, p. 134. Significa isto que a necessidade de intervenção legislativa para acomodar e balizar os diversos direitos, perante o Estado de Direito, é uma realidade. Em sentido idêntico, sugere-se a leitura de SOUSA, Marcelo Rebelo de e ALEXANDRINO, José de Melo, *Constituição da República Portuguesa Comentada – Introdução Teórica e Histórica, Anotações, Doutrina e Jurisprudência, Lei do Tribunal Constitucional*, Lisboa, Lex, 2000, p. 98.

que conferem uma maior proteção ao indivíduo, ampliando o seu âmbito sempre que possível, conforme os casos.

3. Os meios de obtenção de prova no séc. XXI

A função de balança que o legislador ordinário exerce entre as leis penais e constitucionais complica-se principalmente no séc. XXI, uma vez que se tem vindo a assistir a uma proliferação de violações dos direitos fundamentais graças aos desenvolvimentos tecnológicos, fruto da sociedade da informação e de um *modelo de capitalismo neoliberal global*[46]. As novas tecnologias romperam com tudo o que era certo e irrefutável, criando um novo mundo de possibilidades e experiências, contudo trouxeram também alguns riscos e perigos no que toca aos direitos fundamentais[47].

Para além da violação dos direitos fundamentais, é também consequência da revolução da sociedade da informação e das evoluções tecnológicas a eficiente difusão informacional num curto espaço de tempo e lugar[48], onde os sistemas comunicacionais são poderosos instrumentos de negócios, não se associando, de todo, ao amadorismo dos finais do séc. XX[49]. Apesar deste novo paradigma tecnológico, certo é que o direito processual penal só poderá ser considerado eficaz, certo, seguro e eficiente quando compatibilizado com os direitos fundamentais e conseguindo acompanhar as novas exigências do mundo tecnológico em que vivemos.

Hodiernamente, fruto da revolução tecnológica, o Direito Penal substantivo e adjetivo têm sido sobejamente marcados pelas Novas Tecnologias, resultando na *neo-criminalização*. Desde a invenção dos computadores que a própria sociedade começou a questionar-se acerca do advento de perigos que as NTIC trouxeram, atendendo à exploração das potencialidades

[46] Neste sentido, MILITÃO, Renato Lopes, *op. cit.*, p. 248.

[47] A este propósito, LEITÃO, Maria Da Glória, "*A Admissibilidade como meio de prova em processo disciplinar das mensagens de correio eletrónico enviadas e recebidas por trabalhador a partir de e na caixa de correio fornecida pela entidade empregadora*", Colóquio no STJ, Lisboa, 10 outubro de 2012, p. 1, disponível em http://www.stj.pt/ficheiros/coloquios/coloquios_STJ/V_Coloquio/maria_glria_leito.pdf [Consultado em 17/09/2017].

[48] MARTINS, António Gomes Lourenço / MARQUES, J. A. Garcia / DIAS, Pedro Simões, *Cyberlaw em Portugal – O Direito das Tecnologias da Informação e Comunicação*, Famalicão, Edições Centro Atlântico, 2004, p. 364.

[49] Nesta senda, ASCENSÃO, José de Oliveira, *Estudos sobre Direito da Internet e da Sociedade de Informação*, Coimbra, Almedina, 2001, p. 85.

destes mesmos bens e à facilitação da sua desleal utilização diária (cada vez mais intrusiva), assistindo-se, deste modo, ao nascimento do Direito Penal substantivo e adjetivo neoliberal. Acresce ainda o facto de as Novas Tecnologias de Informação e Comunicação terem vindo a apropriar-se de informação e de produtos privados, ou seja, para além de deterem um efeito libertador têm também um efeito constitucionalmente perturbador de elevada danosidade para os indivíduos.

Quem não vai escapar aos novos paradigmas digitais do atual milénio serão a prova e os meios de obtenção de prova, traduzindo-se, agora, num ambiente eletrónico-digital, onde se exige a aplicação de novas técnicas de investigação com peculiaridades e controlos estreitos, sob pena de não serem admissíveis em juízo[50]. Hoje, constata-se a vigência da prova digital, traduzida numa imaterialidade e vulnerabilidade, transmitindo-se binária e digitalmente, i.e., em "*bits*", facilmente dissimuláveis através dos meios de suporte de informação[51] e que em nada se compara às "provas tradicionais". Este tipo de prova raramente se encontra no local da prática de um crime e só é suscetível de apreensão imaterial que, por sua vez, exige um aprofundado *cyber knowledge*, sendo, por isso, propensa a erros provenientes das máquinas, ou até mesmo da ação humana. Como conclui ARMANDO DIAS RAMOS "destas características resulta que a rapidez na sua obtenção, aliada a uma correta recolha de prova, são essenciais para o êxito da investigação e imputação dos factos ao suspeito do crime" [52].

RENATO LOPES MILITÃO chega mesmo a colocar para debate uma certa simplificação e ampliação do regime processual penal referente à prova digital, bem como uma especificação referente aos seus meios de obtenção, tendo em conta as novas necessidades da investigação, que deveriam ser realizados em período temporal útil e eficaz, o que nem sempre se verifica[53].

A necessidade da celeridade e eficiência da investigação é um reflexo de uma sociedade em cujo fluxo informativo simplesmente não cessa, fruto das tecnologias de ponta e de todos os avanços científicos. Hoje a mudança é uma constante, o conhecimento está à distância de um *click* acessível a qualquer cidadão, e a própria informação é, tão só, instantânea. A sociedade da

---

[50] A este propósito, RODRIGUES, Benjamim Silva, *Da Prova Penal, Tomo II – Bruscamente... A(s) face(s) oculta(s) dos Métodos Ocultos de Investigação Criminal*, Lisboa, Rei dos Livros, abril 2010, p. 329.

[51] Neste sentido, MILITÃO, Renato Lopes, *op. cit.*, p. 261.

[52] Cfr. RAMOS, Armando Dias, *op. cit.*, p. 102.

[53] Face à nova realidade digital o autor reivindica uma ampliação e facilitação do regime processual penal, tendo em conta não só a eficácia da investigação criminal, mas também o seu desenvolvimento sem grandes esforços nem riscos para os agentes. MILITÃO, Renato Lopes, *op. cit.*, p. 266.

informação em que hoje vivemos fica marcada pela rapidez na modificação e circulação de informações, traduzindo-se numa rutura com aquilo que era certo e irrefutável.

As telecomunicações são um dos grandes motores da sociedade da informação e, provavelmente, um dos seus maiores marcos, tendo em conta que o ser humano sempre comunicou de forma oral, escrita, ou até gestual, no entanto, nunca o fez com a facilidade, eficiência e produtividade das comunicações eletrónicas de hoje. Fazendo uma análise histórica é surpreendente a rapidez com que esta área cientifica evoluiu, tendo em conta que há cerca de cinquenta anos atrás o simples telemóvel não existia, nem tampouco os *e-mails.* Mas afinal o que é que são as telecomunicações?

Nas palavras de BENJAMIM SILVA RODRIGUES as telecomunicações são "(...) o agrupamento de todos os meios de comunicação através das redes de "comunicações electrónicas""[54] que se encontram protegidas pela tutela da inviolabilidade do sigilo das comunicações privadas, prevista no art.º 34.º da CRP[55], bem como pelo direito à reserva da vida privada a familiar, previsto no art.º 26.º da CRP. Este tipo de comunicação é operado digitalmente através de operadoras telefónicas e/ou rede de Internet, sendo que o utilizador servir-se-á deste serviço na espectativa de que os "dados trocados" se mantenham sigilosos dentro do ciclo comunicacional, esperando ainda a não divulgação daqueles que têm acesso ao fluxo informacional, graças ao exercício das suas profissões. Tendo por referência o princípio da proteção da vida privada é imposto às medidas de vigilância das telecomunicações um controlo especial *pós facto* e *ante facto*, como também um controlo político, legal e normativo[56], no entanto, é irrealista sequer considerar-se que os operadores telefónicos e/ou rede de Internet não gozam de um domínio extremo sobre as comunicações tidas entre os particulares[57].

Não obstante a confidencialidade entre os interlocutores, certo é que a inviolabilidade do sigilo das comunicações visará a proteção das redes e dos sistemas comunicacionais eletrónicos

[54] Cfr. RODRIGUES, Benjamim Silva, *op. cit.*, p. 344.

[55] Neste sentido, RODRIGUES, Benjamim Silva, *Das Escutas Telefónicas, Tomo I – A Monitorização dos Fluxos Informacionais e Digitais*, Coimbra, Coimbra Editora, maio 2008, p. 431.

[56] Para melhor desenvolvimento, 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 Figueiredo Dias, por ocasião dos 20 anos do Código de Processo Penal Português, Coord. MÁRIO FERREIRA MONTE, Trad. INÊS FERNANDES GODINHO, Coimbra, Coimbra Editora, 2009, pp. 731 e 732.

[57] RODRIGUES, Benjamim Silva, *Da Prova Penal, Tomo II...*, *op. cit.,* p. 347.

"à distância", respeitando os dados de conteúdo[58] (aqueles que respeitam o conteúdo de uma mensagem e que só podem ser intercetados em tempo real), os dados de tráfego[59] (aqueles dados técnicos ou informáticos que foram originados e se relacionam com o envio de uma comunicação eletrónica, ou seja, são dados gerados pelo percurso de determinada comunicação, indicando a sua origem, por exemplo, dados relativos à data e hora inicial – *log in* – e final – *log out* – da sessão, bem como a duração dos serviços subjacente, ou até mesmo o n.º de identidade e morada do assinante, entre outros) e, ainda, os dados de localização[60] (dados que indicam a posição geográfica do equipamento do utilizador de serviço de comunicação eletrónica).

É graças à utilização massiva das telecomunicações e ao facto de os dados eletrónicos permanecerem nas redes para além do seu período temporal originário, surgindo "(...) "um tempo de não comunicação e relativo à comunicação ocorrida noutro tempo""[61], i.e., um rasto de marcas e sinais, que o processo penal português não ficou alheio, criando meios para conseguir ter acesso e utilizar em juízo essas mesmas comunicações. Ora, desde logo se pode constatar que, neste prisma, o processo penal português atendeu às necessidades do advento digital e ao facto que nem todas as provas são físicas, necessitando, por isso, de tratamento diferenciado.

É graças a esta nova realidade probatória digital e, consequentemente, aos novos meios de informação e comunicação que os tribunais se têm visto obrigados a depreender novas matérias, cuja compreensão exige específicos conhecimentos[62]. É racional que seja exigido um grande desenvolvimento do direito processual penal, bem como das suas técnicas de investigação com vista à investigação cibercriminal, numa linha muito mais vanguardista e adequada às novas necessidades do novo milénio[63].

---

[58] Nesta senda, RODRIGUES, Benjamim Silva, *Da Prova Penal, Tomo IV – Da Prova-Electrónico-Digital e da Criminalidade Informático-Digital*, Lisboa, Rei dos Livros, abril 2011, p. 420.

[59] A este propósito, VEIGA, Armando e RODRIGUES, Benjamim Silva, *"A monotorização de dados pessoais de tráfego nas comunicações eletrónicas"*, Raízes Jurídicas, Curitiba v. 3, n.º 2, jul./dez. 2007, p. 73.

[60] *Vd* a al. e) do n.º 1 do artigo 2.º da Lei n.º 41/2004, de 18 de agosto: *«Dados de localização» quaisquer dados tratados numa rede de comunicações eletrónicas ou no âmbito de um serviço de comunicações eletrónicas que indiquem a posição geográfica do equipamento terminal de um utilizador de um serviço de comunicações eletrónicas acessível ao público.*

[61] Cfr. RODRIGUES, Benjamim Silva, *Da Prova Penal, Tomo II..., op. cit.,* p. 355.

[62] Neste sentido, VERDELHO, Pedro, *"Técnica no Novo C.P.P..."*, *op. cit.*, p. 146.

[63] MILITÃO, Renato Lopes, *op. cit.*, p. 262.

Apesar de todo o desenvolvimento tecnológico, certo é que as necessidades vivenciadas pelos investigadores ficaram aquém com a redação do CPP de 2007, uma vez que do mesmo não resultou uma regulação assumida no que toca à recolha e análise da prova digital. MANUEL DA COSTA ANDRADE acusa o legislador de tapar os olhos e os ouvidos aos "ruídos dos media" e das novas tecnologias de informação e comunicação[64], chegando mesmo a intitular de penosa a atitude do mesmo que simplesmente não deu sinais de direção, nem de sentido, face a esta nova odisseia digital. Esta abstenção levou a que se deixasse por resolver questões práticas constatáveis em sede de audiência e discussão de julgamento.

Nesta linha, é constatável que um dos principais véus que não foi levantado com a redação do CPP 2007 foi o regime dos meios de obtenção de prova digital previsto no art.º 189.º do CPP[65], atendendo à analogia que o mesmo convida entre o regime das escutas telefónicas e as restantes comunicações eletrónicas, como o *e-mail*, ou as *SMS*. Portanto, este regime de proteção alargada das escutas telefónicas, para além das conversações efetuadas através de telemóveis, também se vai traduzir nas conversações efetuadas através de *PCs* ou outros sistemas, desde que detenham armazenamento em suporte digital. Seja através de uma escuta telefónica, *SMS*, ou *e-mail*, a verdade é que o elemento de prova é o próprio conteúdo dessas comunicações, ou seja, a conversa que indicie a prática de um crime.

Este meio de obtenção de prova previsto nos artigos 187.º e ss do CPP, tal como já foi supramencionado, é considerado a ultima *ratio* da investigação não só por causa da abundância de direitos fundamentais que exacerbadamente viola, mas também devido ao facto de a sua "teia de investigação" não deter limites. Com este tipo de investigação o contágio de terceiros é um verdadeiro risco, reproduzindo, desta forma, conhecimentos furtuitos, ou seja, conhecimentos casualmente descobertos e que nem sequer eram objeto de investigação. A título de exemplo podemos imaginar um caso em que certo sujeito é alvo de escutas telefónicas devido a inúmeros indícios da prática do crime de tráfico de estupefacientes. Através deste meio

---

[64] Neste sentido, ANDRADE, Manuel da Costa, *"Bruscamente no Verão Passado", a Reforma do Código de Processo Penal: Observações Críticas sobre uma Lei que podia e devia ter sido diferente*, Coimbra, Coimbra Editora, julho 2009, p. 144.

[65] Pode ler-se o regime do art.º 189.º do CPP:

1 - O disposto nos artigos 187.º e 188.º é correspondentemente aplicável às conversações ou comunicações transmitidas por qualquer meio técnico diferente do telefone, designadamente correio eletrónico ou outras formas de transmissão de dados por via telemática, mesmo que se encontrem guardadas em suporte digital, e à interceção das comunicações entre presentes.

2 - A obtenção e junção aos autos de dados sobre a localização celular ou de registos da realização de conversações ou comunicações só podem ser ordenadas ou autorizadas, em qualquer fase do processo, por despacho do juiz, quanto a crimes previstos no n.º 1 do artigo 187.º e em relação às pessoas referidas no n.º 4 do mesmo artigo.

de obtenção de prova podemos não só descobrir os clientes deste sujeito, como possíveis "companheiros de negócios", ou seja, *drug dealers* e todos os esquemas que estão por detrás da prática do ilícito[66]. Podemos também assistir à situação em que os dados segregados pelas comunicações vão-se revelar mais significativos que o próprio conteúdo da comunicação, contudo, nem todos os dados produzidos no contexto da comunicação conseguem ser protegidos pela ordem jurídica[67].

É em função dos riscos constitucionais que a própria letra da lei afirma que este tipo de investigação somente será autorizada durante a fase de inquérito e quando é absolutamente indispensável para a descoberta da verdade material, através de despacho fundamentado do JIC, em que este autorize a interceção, gravação ou registo de conversações ou comunicações, mediante requerimento prévio do MP, quanto aos crimes previstos no n.º 1 e 2 do art.º 187.º.

Independentemente do titular do meio de comunicação utilizado, o art.º 187.º n.º 4 do CPP[68] vem discriminar que os suspeitos ou arguidos da prática dos crimes previstos nos números anteriores; a 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 a vítima de crime, mediante o respetivo consentimento, podem ser alvos de escutas telefónicas.

Por outro lado, em relação à duração da medida, a interceção de conversações é autorizada pelo prazo máximo de três meses, renovável por períodos sujeitos ao mesmo limite, contanto que os requisitos de admissibilidade se mantenham, nos termos do n.º 6 do art.º 187.º

O n.º 5 do art.º 187.º apresenta uma das restrições deste tipo de investigação, mais propriamente a interceção e a gravação de conversações ou comunicações entre o advogado e o seu constituinte, atendendo à necessidade de preservação dos direitos de defesa do arguido. Não obstante, essa restrição poderá não se aplicar caso o JIC entenda que as gravações constituam objeto ou elemento de crime.

Conclui-se que as escutas têm um prazo máximo de 3 meses, de 15 em 15 dias os OPC levam ao conhecimento do MP todos os autos relatórios das mesmas. Mais tarde, será o MP que

[66] E o problema levanta-se quando nos questionamos sobre o que fazer com esse conhecimento, abrimos um novo processo crime sobre esses elementos? Mas essa prova poderá ser válida?

[67] Nesta senda, ANDRADE, Manuel da Costa, *op. cit.*, p. 156.

[68] JESUS, Francisco Marcolino, *op. cit.*, p. 290.

dará conhecimento ao JIC, num prazo de 48 horas, todos os autos relatórios conseguidos pelos OPC e, num prazo de 24 horas, o JIC poderá fazer cessar este meio de obtenção de prova, ou mantê-lo por um prazo não superior a 3 meses[69]. A confidencialidade das escutas deve ser sempre garantida mesmo que o prazo das interceções se tenha concluído, sendo que as conversações ou comunicações que poderão valer como prova serão as previstas no n.º 9 do art.º 188.º do CPP.

Ademais, o regime das escutas telefónicas tem obrigatoriamente de atender a todos os pressupostos formais e materiais sob pena de nulidade. Assim, a violação dos pressupostos formais desencadeará um desvalor da ação, mas que não se traduz obrigatoriamente numa "detenção ilícita da informação". Por outro lado, violando os pressupostos materiais, i.e., aqueles que legitimam a aquisição e detenção informativa, bem como a sua utilização probatória, desencadear-se-á num desvalor do resultado, logo tal informação não será aprovada pela ordem jurídica e, consequentemente, não poderá ser utilizada[70].

Todavia, a extensão do regime das escutas telefónicas aos casos das *SMS* ou *e-mails*, prevista no art.º 189.º, trouxe alguns inconvenientes, uma vez que, desde logo, as telecomunicações, como hoje as conhecemos, abrangem um espectro que à data da entrada em vigor do CPP era totalmente inimaginável, deixando para trás, em muito, os procedimentos anteriormente disponíveis. É esta uma das razões que leva a que COSTA ANDRADE apelide o regime do art.º 189.º de "casa dos horrores hermenêuticos", atendendo às confusões e desequilíbrios inexplicáveis que este regime reclamou para si[71].

Acresce ainda que, graças ao Código de Processo Penal que trouxe consigo um regime precipitado e desatualizado, face a um novo ambiente eletrónico-digital, e por força da necessidade de transposição das obrigações internacionais por parte do Estado português, veio a introduzir-se no nosso ordenamento jurídico mais dois regimes que regulam um conjunto de importantes normas dedicadas à obtenção de prova digital. Assim, no âmbito de monotorização das comunicações eletrónicas podemos ter três regimes que vêm regular a intromissão nas comunicações privadas eletrónicas, a saber: os artigos 187.º a 190.º do CPP; por outro lado, a Lei n.º 32/2008, de 17 de julho (Lei da Conservação de Dados Gerados ou Tratados no Contexto Oferta de Serviços de Comunicações Eletrónicas); ou até mesmo a Lei n.º 109/2009,

[69] A este propósito, JESUS, Francisco Marcolino, *op. cit.*, p. 299.

[70] ANDRADE, Manuel da Costa, *op. cit.*, p. 143.

[71] Neste sentido, ANDRADE, Manuel da Costa, *op. cit.*, p. 185.

de 15 de setembro (Lei do Cibercrime), refletindo, por isto, um desnecessário atropelo legislativo[72].

Perante esta encruzilhada legislativa, são várias as opiniões e soluções apontadas, desde logo, um pequeno exemplo passa, por um lado, pela teoria de RENATO LOPES MILITÃO cujas normas referentes à obtenção da prova digital deveriam integrar-se no CPP porque só desta forma é que subsistirá uma harmonia com o regime geral de obtenção das provas e até mesmo porque este regime só se diferencia do "regime tradicional" em alguns aspetos[73], por outro lado, com vista à eliminação do art.º 189.º do CPP, MANUEL DA COSTA ANDRADE defende a criação de um regime mais amplo e compreensivo no próprio CPP relativamente às diferentes formas de intromissão nas telecomunicações[74].

Ora, independentemente de as telecomunicações serem um campo de liberdade à margem do direito que possibilita diversos tipos de comunicações através dos mais diversos suportes técnicos e, por sua vez, da dificuldade de o direito processual penal português as conseguir considerar devidamente, sem indecisões ou indagações desnecessárias, o certo é que não faltam doutrinas com "desfechos milagrosos" totalmente distintos para poderem auxiliar o legislador português na criação de um regime mais consistente, exigente e seletivo face à atual realidade informática.

[72] Nesta senda, RODRIGUES, Benjamim Silva, *Da Prova Penal, Tomo II..., op. cit.*, pp. 387 e 388.

[73] MILITÃO, Renato Lopes, *op. cit.*, pp. 273 e 274.

[74] A este propósito, ANDRADE, Manuel da Costa, *op. cit.,* p. 184.

CAPÍTULO II

O CIBERCRIME: UMA CRESCENTE REALIDADE

Expostas algumas das principais especificidades do regime processual penal português e, consequentemente, dos meios de obtenção de prova, importa agora fazer uma análise de uma realidade que, apesar de já não ser novidade, continua a revelar-se num verdadeiro quebra-cabeças para os profissionais da área da justiça, graças à sua constante mutabilidade e imaterialidade, i.e., o "fenómeno" do cibercrime, outrora denominado de criminalidade informática.

Assim, no presente capítulo, debruçar-nos-emos sobre a atividade criminosa levada a cabo por meios/objetos informáticos penalmente relevantes, obrigando a ciência do direito a "mergulhar de cabeça" na era digital. É graças à dependência informática sentida pela sociedade da informação e graças ao facto de o direito ser uma ciência, estando constantemente obrigado a evoluir e reinventar-se (contudo, de forma muito mais rigorosa e ponderada), que têm nascido preceitos e soluções legais totalmente inovadoras e capazes de apaziguar os crimes cibernéticos.

1. A dependência informática por parte da sociedade da informação

Enquanto inicialmente a revolução tecnológica modificou apenas alguns setores da sociedade, hoje são raras as atividades que não dependem de métodos informáticos especializados e, em particular, da Internet. Numa sociedade como aquela em que vivemos, é absolutamente impensável sobreviver sem qualquer meio técnico ou informático de relevo, como os computadores, telemóveis, *GPS*, ou *tablets*, tendo em conta que estes se encontram

praticamente enraizados em quase todos os setores da vida em sociedade[75], seja no âmbito profissional, ou até mesmo pessoal. É caricato o facto de este tipo de *gadgets* ser solução para todos os nossos problemas e é constatável que quando, por exemplo, perdemos o sinal de rede dos telemóveis/alcance da rede *wifi*, ou até mesmo quando falha a eletricidade no local em que nos encontramos e necessitamos de aceder ao "mundo virtual", não sabemos muito bem como é que havemos de reagir face à eterna dependência deste tipo de instrumentos. Hoje, é absolutamente impensável o retrocesso informático, não só em Portugal, como na generalidade dos países ocidentais.

Contudo, apesar de todos os benefícios e auxílios que estes instrumentos têm trazido para o quotidiano de qualquer cidadão, o certo é que também catalisam algumas vulnerabilidades e não estamos a referir-nos às eventuais avarias destes equipamentos. De facto, tem-se assistido a um constante jogo do "gato e do rato" quando falamos da interligação entre a área jurídica e a área informática, tendo em conta que a primeira se tem visto completamente impossibilitada de apresentar soluções céleres e eficazes face à vertiginosa evolução da segunda[76], principalmente na área criminal, uma vez que de dia para dia têm progredido e emergido cada vez mais delitos relacionados com o recurso às novas tecnologias, colocando em risco a utilização quotidiana dos meios informáticos. A realidade informática é tão celeremente mutável que dificulta o papel do legislador que, por sua vez, vê o seu trabalho tornar-se obsoleto e ultrapassado num pequeno período de tempo.

Dúvidas não devem subsistir que, independentemente dos vários fatores como a ganância, inveja ou exibicionismo, existirão sempre indivíduos orientados para a intromissão e produção de danos em bens alheios, procurando vantagens patrimoniais com esses mesmos atos, principalmente quando nem sequer necessitam de se deslocar fisicamente ao local da prática do crime.

A sociedade da informação surgiu como uma realidade à margem do direito[77], todavia o mesmo não lhe pode ficar eternamente alheado. Assim, no que ao âmbito criminal diz respeito, devemos ter em linha de conta que o Direito irá sempre tentar alcançar um equilíbrio

---

[75] Assim o refere, MARTINS, António Gomes Lourenço, "*Criminalidade Informática",* Direito da Sociedade da Informação – Volume IV, APDI – Associação Portuguesa de Direito Intelectual", Coimbra, Coimbra Editora, 2003, p. 9.

[76] A este propósito, ASCENSÃO, José Oliveira, "*Criminalidade Informática",* Direito da Sociedade da Informação – Volume II, FDUL – Faculdade de Direito da Universidade de Lisboa / APDI – Associação Portuguesa de Direito Intelectual, Coimbra, Coimbra Editora, 2001, p. 228.

[77] VENÂNCIO, Pedro Dias, *Lei do Cibercrime – Anotada e Comentada*, Coimbra, Coimbra Editora, fevereiro 2011, p. 14.

harmonioso entre o combate ao cibercrime e a proteção dos direitos fundamentais de qualquer cidadão, principalmente pelo facto de as instituições, cidadãos e Estado dependerem em tão larga escala dos meios informáticos e principalmente da Internet.

2. O que é Cibercrime e quem são os seus principais agentes?

Foi graças à Internet e aos novos meios de informação e comunicação que a criminalidade para além de crescer exponencialmente, moldou-se a um novo contexto e a uma nova realidade. Se no séc. XIX e meados do séc. XX as únicas formas conhecidas de praticar crimes se resumiam ao pleno contacto físico e pessoal com as vítimas, com o aparecimento das NTIC surgiu uma nova realidade.

A informática é reguladora dos mais variadíssimos setores sociais como a energia, transportes, justiça, saúde e educação, contudo também pode ser tida como um instrumento de ataque à própria sociedade de informação. Foi desta forma que se assistiu à evolução da ciência criminal, bem como do comportamento do criminoso que por sua vez se tornou muito mais perigoso, eficaz e internacional. Hoje, através das mais recentes potencialidades informáticas, assiste-se à proliferação e ao aumento generalizado de novos delitos[78] que permitem a verdadeira dissimulação dos intervenientes[79], dificultando a identificação dos criminosos por *quem de direito*[80]. É por estas razões que a informática, ultimamente, tem sido alvo de atenções legislativas, não só no âmbito nacional, mas também europeu e internacional.

Assim, fruto da evolução tecnológica e através das redes informáticas surgiu uma nova forma de praticar crimes, i.e., o cibercrime. O cibercrime, ou também ainda denominado de criminalidade informática, apesar de não deter nenhuma definição consagrada expressamente na legislação portuguesa, nem se encontrar 100% assente em todos os ordenamentos jurídicos, pode definir-se como todas e quaisquer "(...) condutas danosas para a sociedade concretizadas

[78] Neste sentido, Relatório Anual de Segurança Interna – Ano 2016, *op. cit.*, p. 31.

[79] Atendendo ao facto que a reconstituição de práticas criminosas, no contexto *web*, é uma tarefa muito mais dificultada e imprecisa graças à facilidade de transferência de informação para outros pontos *web* ou até mesmo através da disponibilização de anonimizadores.

[80] Assim o refere, VENÂNCIO, Pedro Dias, *"Breve Introdução à Questão da Investigação e Meios de Prova na Criminalidade Informática",* Verbo Jurídico, dezembro 2006, p. 6.

na utilização de um computador, ou sistema de tratamento de dados, que funciona como objecto e/ou instrumento da acção, e que atenta contra bens jurídico-penais, como a esfera privada do indivíduo ou o seu património, através do acesso, recolha, armazenamento, introdução, alteração, destruição, intercepção ou transmissão informática (ou telemática) de dados"[81].

No fundo, o cibercrime pode ser definido como aquele tipo de crime cujos sistemas informáticos podem servir de instrumento para a perpetração de crimes, ou cujos instrumentos informáticos são alvo desses mesmos ataques, pelo que o ilícito praticado através de equipamentos informáticos não se assemelhará aos tradicionalmente previstos pelo legislador penalista. Perante o fenómeno do cibercrime, cujos principais problemas subsumem-se a celeumas imateriais e internacionais cuja facilidade de deslocação de conteúdos ou até mesmo o anonimato do criminoso são uma constante, só com os melhores e mais recentes equipamentos informáticos, bem como a constante formação de *quem de direito*, é que o sucesso por parte das autoridades policiais poderá ser uma realidade.

O certo é que se tem vindo a assemelhar o cibercrime à criminalidade organizada, atendendo à sua propagação estonteante numa esfera sem fronteiras geográficas. De mais a mais, existe quem[82] associe este tipo de criminalidade aos *white collar crimes*[83], uma vez que estes ilícitos se caracterizam pelo não uso da violência física, têm em vista a obtenção de vantagens patrimoniais ou de ocultação de perdas que, geralmente, ultrapassam em larga escala as decorrentes dos crimes "tradicionais".

De facto, toda a realidade digital tem potenciado uma deslocalização massiva da criminalidade para a *web*, dificultando a tarefa do processo penal ao combate eficaz contra o cibercrime, desde logo porque as principais normas penais assentam em fatores como a

[81] Contudo, não podemos julgar que serão única e simplesmente alvo destas condutas os bens jurídicos *supra* explanados. Basta refletir que a própria segurança dos bens informáticos também pode ser alvo de cibercrime. Cfr. MACEDO, João Carlos Cruz Barbosa, *"Algumas considerações acerca dos crimes informáticos em Portugal",* Direito Penal Hoje - Novos desafios e novas respostas, Organiz. MANUEL DA COSTA ANDRADE e RITA CASTANHEIRA NEVES, Coimbra, Coimbra Editora, 2009 p. 224.

[82] Neste sentido, MARTINS, António Gomes Lourenço, "*Criminalidade Informática...", op. cit.,* p. 12.

[83] Em português, crimes de colarinho branco. São aqueles crimes que não dependem do uso da violência física ou ameaça, associando-se, em regra, a todo o tipo de fraudes, burlas, ocultações, ou violações de confiança. Por norma, a principal motivação desta espécie de crimes é de natureza financeira, com vista a vantagens pessoais ou empresariais. Disponível em https://www.fbi.gov/investigate/white-collar-crime [Consultado em 15.04.2017].

materialidade e territorialidade[84], não se coadunando com o caráter global e digital da realidade informática[85]. Independentemente das campanhas[86] cujo objetivo passa pelo combate ao cibercrime e do auxílio por parte dos gigantes da Internet (como por exemplo, *Google*, *Facebook*, *Amazon*)[87], dúvidas não devem subsistir quanto ao aumento e sofisticação da cibercriminalidade, tanto no contexto nacional, como internacional[88].

Relativamente aos agentes que executam este tipo de ilícitos, se em 1990, subdividia-se os delinquentes informáticos em apenas duas categorias[89], nomeadamente, os *Cibercriminosos Acidentais* (aqueles apaixonados pelas NTIC, que se divertiam a descobrir códigos e dados de acesso das diversas empresas e organizações governamentais, resumindo os seus atos a verdadeiros "truques informáticos") e os *Reais Cibercriminosos* (aqueles que apostavam em verdadeiros ganhos financeiros, extremamente competentes, sendo que aquilo que os motivava, na esmagadora maioria das vezes, eram os possíveis lucros económicos), o certo é que face ao ritmo alucinante a que a informática evoluiu, consequentemente, houve a necessidade de se fazer uma distinção que refletisse e denominasse, com maior rigor, as verdadeiras motivações criminosas.

Nessa sequência, surgiram denominações como *hacker* ou *cracker* que julgamos não serem totalmente desconhecidas do público em geral, contudo a verdade é que nem sempre estas designações são corretamente empregues. Portanto, antes de tudo, tendo em vista uma melhor compreensão, e atendendo à taxonomia maioritariamente aceite, importa fazer uma distinção elucidativa entre aquilo a que apelidamos de *hackers* e as suas diversas categorias, ou seja, os *hackers* de chapéu branco, cinzento, azul ou preto e, num plano mais "inocente", os *script kiddies*.

---

[84] O princípio da territorialidade caracteriza-se por ser um princípio base do nosso ordenamento jurídico que se traduz na aplicação do direito penal português a todos os factos juridicamente relevantes que se reproduziram em Portugal, não fazendo quaisquer distinções por quem ou contra quem tais factos foram cometidos. DIAS, Jorge de Figueiredo, *Direito Penal..., op. cit.*, p. 208.

[85] Neste mesmíssimo sentido, VENÂNCIO, Pedro Dias, *Lei do Cibercrime..., op. cit.,* p. 16.

[86] Disponível em http://www.apav.pt/cibercrime/ [Consultado em 15.10.2017].

[87] Disponível em https://pplware.sapo.pt/internet/cibercrime-portugal-fez-8-mil-pedidos-ao-facebook/ [Consultado em 15.04.2017].

[88] 12 de maio de 2017 ficou marcado por um dos maiores ataques informáticos a nível nacional e internacional. Nas palavras de Carlos Cabreiro (diretor da Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica da Polícia Judiciária) tratou-se de "*uma campanha de distribuição de ransomware, que se caracterizou pela encriptação dos dados dos computadores com pedido de resgate para o seu desbloqueio*". Apesar de os principais alvos terem sido as empresas de telecomunicações, também os bancos, empresas de consultoria e hospitais foram vítimas deste ciberataque. A notícia está disponível na íntegra em https://www.publico.pt/2017/05/12/tecnologia/noticia/ataque-informatico-internacional-afecta-empresas-e-hospitais-1771939 [Consultado em 12.05.2017].

[89] O autor baseia-se na distinção acolhida pelo Relatório do Comité Europeu para os Problemas Criminais, do Conselho da Europa de 1990, face à realidade da época. Neste sentido, MARTINS, António Gomes Lourenço, "*Criminalidade Informática...", op. cit.,* p. 13.

Ora, importa desde já esclarecer, que o termo *hacker* nem sempre é utilizado de modo pejorativo, mas sem dúvida alguma que será sempre aquele indivíduo que utiliza o seu *know-how* informático para aceder legítima ou ilegitimamente a um sistema informático. Assim, os *white hat hackers*[90] são aqueles *hackers*, autorizados por empresas, que promovem a difusão do conhecimento, a ética de entreajuda e promoção de segurança dos sistemas informáticos, sem intenções maliciosas; os *grey hat hackers*[91] são aqueles especialistas que chegam a violar alguns padrões ético-legais, tendo em conta que apesar de não deterem uma intenção puramente maliciosa acabam por pedir recompensas pelos erros informáticos descobertos; os *blue hat hackers*[92] são especialistas informáticos contratados por empresas com a função de encontrar vulnerabilidades ou *bugs*[93] nas próprias infraestruturas das empresas; os *black hat hackers* ou também conhecidos por *crackers*[94] são aqueles que se dedicam ao *hacking* com objetivos unicamente maliciosos, como por exemplo, ganhos financeiros[95], sendo vistos como autênticos criminosos[96]; por fim, os *Script Kiddies*[97] são aqueles que, apesar da sua inexperiência

---

[90] Adaptação nossa traduzida do texto original: *A white hat hacker is a computer security specialist who breaks into protected systems and networks to test and asses their security. White hat hackers use their skills to improve security by exposing vulnerabilities before malicious hackers (known as black hat hackers) can detect and exploit them. Although the methods used are similar, if not identical, to those employed by malicious hackers, white hat hackers have permission to employ them against the organization that has hired them.* Disponível em https://www.techopedia.com/definition/10349/white-hat-hacker [Consultado em 15.04.2017].

[91] Adaptação nossa traduzida do texto original: *A gray hat hacker (also spelled grey hat hacker) is someone who may violate ethical standards or principles, but without the malicious intent ascribed to black hat hackers. Gray hat hackers may engage in practices that seem less than completely above board, but are often operating for the common good. Gray hat hackers represent the middle ground between white hat hackers, who operate on behalf of those maintaining secure systems, and black hat hackers who act maliciously to exploit vulnerabilities in systems.* Disponível em https://www.techopedia.com/definition/15450/gray-hat-hacker [Consultado em 15.04.2017].

[92] Adaptação nossa traduzida do texto original: *A blue hat hacker is someone outside computer security consulting firms who bug tests a system prior to its launch, looking for exploits so they can be closed. Blue Hat Hacker also refers to the security professional invited by Microsoft to find vulnerabilities in Windows. The term has also been associated with th annual security conference by Microsoft, the unofficial name coming from the blue color associated with Microsoft employee badges.* Disponível em https://definitions.uslegal.com/b/blue-hat-hacker/ [Consultado em 15.04.2017].

[93] Vocábulo geralmente utilizado no âmbito informático quando é descoberto algum erro num programa, ou quando esse mesmo sistema apresenta alguma falha inesperada.

[94] Adaptação nossa traduzida do texto original: *A cracker is one who breaks into or otherwise violates the system integrity of remote machines with malicious intent. Having gained unauthorized access, crackers destroy vital data, deny legitimate users service, or cause problems for their targets. Crackers can easily be identified because their actions are malicious.* Disponível em http://searchenterprisedesktop.techtarget.com/tip/The-difference-between-hackers-and-crackers [Consultado em 15.04.2017].

[95] *Vd* http://www.computerworld.com.pt/2017/03/17/hacker-suspeito-de-danos-acima-de-400-mil-euros/ [Consultado em 15.04.2017].

[96] Neste sentido, MARTINS, António Gomes Lourenço / MARQUES, J. A. Garcia / DIAS, Pedro Simões, *op. cit.*, p. 446.

[97] Adaptação nossa traduzida do texto original: *The lowest form of cracker; script kiddies do mischief with scripts and programs written by others, often without understanding the exploit they are using. Used of people with limited technical expertise using easy-to-operate, pre-configured, and/or automated tools to conduct disruptive activities against networked systems. Since most of these tools are fairly well-known by the security community, the adverse impact of such actions is usually minimal. People who cannot program, but who create tacky HTML pages by copying JavaScript routines from other tacky HTML pages. More generally, a script kiddie writes (or more likely cuts and pastes) code without either having*

informática, visam a busca de falhas e vulnerabilidades informáticas através de *scripts*[98] programados por terceiros, tendo por objetivo ganhos patrimoniais, bem como obtenção de benefícios ou vantagens ilegítimas.

Se, inicialmente, maioria destes *hackers* começam a sua "carreira" de forma totalmente inocente, o certo é que rapidamente tendem a obter lucro através do anormal funcionamento dos sistemas informáticos, i.e., através de *malware*[99] (criados por eles próprios), como *os trojan horses*[100], *worms*[101], *vírus*[102], *spyware*[103], *ransomware*[104], tornando-se em verdadeiras fontes de rendimento.

Independentemente da utilização dos vocábulos corretos para a situação em concreto, uma coisa é certa, graças aos novos instrumentos informáticos facilmente se pode constatar que a prática de cibercrimes é fomentada pelos pequenos riscos que estão a si associados, aliados ao anonimato do criminoso e ao facto de serem ilícitos que podem ser praticados sem qualquer contacto físico com a pessoa e/ou local da prática do crime[105].

---

or desiring to have a mental model of what the code does. Vide RAYMOND, Eric S., "The New Hacker's Dictionary", disponível em http://www.proselex.net/Documents/The%20New%20Hacker's%20Dictionary.pdf [Consultado em 15.04.2017].

[98] Do inglês, roteiro em código, ou seja, é uma linguagem em computador que executa algumas funções, como por exemplo, o *JavaScript*. Disponível em http://searchenterpriselinux.techtarget.com/definition/script [Consultado em 15.04.2017].

[99] Do inglês, *malicious software*, ou seja, software malicioso, ou software com objetivos maliciosos, é um conjunto de variantes de software intruso, ou hostil, que ao danificar os arquivos do equipamento informático, vai interferir no normal funcionamento do seu sistema, tornando-o completamente inoperante. Disponível em https://techterms.com/definition/malware [Consultado em 15.04.2017].

[100] Do inglês, "Cavalo de Troia", ou seja, é aquele tipo de programa aparentemente inofensivo, mas que deixa o atacante assumir o controlo do computador remotamente, registando tudo o que o utilizador digita e, assim, o controlador remoto tem acesso às passwords, ou até mesmo os dados bancários do utilizador. Disponível em http://searchsecurity.techtarget.com/definition/Trojan-horse [Consultado em 15.04.2017].

[101] Do inglês, "minhoca", é o software capaz de se disseminar pelo computador e por toda a rede, sem qualquer intervenção humana. Disponível em http://malware.wikia.com/wiki/Worm [Consultado em 15.04.2017].

[102] Traduz-se num conjunto de parasitas informáticos introduzidos num programa, suscetíveis de provocar diversas perturbações no funcionamento do computador. Disponível em https://pplware.sapo.pt/microsoft/windows/seguranca-informatica-malware-virus-spyware-trojans/ [Consultado em 15.04.2017].

[103] É aquele *malware* que, como o próprio nome indica, tem a capacidade de vigiar e roubar, remotamente, as informações pessoais do computador do utilizador, como por exemplo, informações bancárias. Disponível em https://support.microsoft.com/pt-pt/help/129972/how-to-prevent-and-remove-viruses-and-other-malware [Consultado em 15.04.2017].

[104] Advém do inglês, "resgate", é aquele malware que visa a obtenção de lucros através da infeção de um sistema informático e encriptação dos dados pessoais presentes no mesmo. Disponível em https://pplware.sapo.pt/informacao/ransomware-jogar-desbloquear-ficheiros/ [Consultado em 15.04.2017].

[105] MACEDO, João Carlos Cruz Barbosa, *Idem, ibidem*.

3. Diferentes conceções metodológicas do fenómeno do Cibercrime

O certo é que o território *virgem e inexplorado* é extremamente apreciado por aqueles que desejam deixar a sua "marca", acolhendo sempre novas sistematizações e, como não poderia deixar de ser, o conceito de cibercrime é um exemplo claro desta afirmação.

Assim, no lapidar dizer de PEDRO DIAS VENÂNCIO[106], o cibercrime pode ter duas naturezas completamente distintas, havendo a necessidade de fazer uma distinção entre os casos em que a informática não passa de um meio para praticar um crime e, por outro lado, os casos em que a informática é uma componente do tipo legal de crime.

Deste modo, por um lado, podemos ter a cibercriminalidade em sentido amplo que se vai traduzir naquelas atividades criminosas que podem, ou não, ser executadas através de meios informáticos. Nestes casos, a prática do ilícito pode ser levada a cabo por meios informáticos, contudo estes meios não são estritamente necessários para a sua consumação. Posto isto, conclui-se que os meios informáticos simplesmente não integram os tipos legais de crime tendo em conta que os mesmos crimes podem ser praticados através de outros instrumentos. Como exemplo de cibercrimes em sentido amplo podemos identificar os crimes de difamação, injúrias ou ofensas que, na maioria dos casos, são proferidos verbalmente, contudo também podem ser cometidos por meios informáticos, através de redes sociais, agravando-se assim a moldura abstrata do tipo legal de crime[107].

---

[106] VENÂNCIO, Pedro Dias, *Lei do Cibercrime...*, *op. cit.*, p. 17.

[107] A título de exemplo, denote-se o Acórdão do Tribunal da Relação do Porto de 30-10-2013 que condenou o arguido que através de um *post* na rede social Facebook conseguiu propalar factos inverídicos, capazes de ofender o prestígio da pessoa coletiva em causa. O Acórdão em causa tem o seguinte sumário: *Integra o tipo de crime de Ofensa a organismo, serviço ou pessoa coletiva, do artigo 187º, do Código Penal, apenas a afirmação ou propalação de factos inverídicos e ofensivos e não (ao contrário do que se verifica com os crimes de Difamação do artigo 180º, do Código Penal, e de Injúria do artigo 181º do mesmo Código) a formulação de juízos ofensivos. Este é um crime de perigo: basta que os factos em questão sejam capazes de ofender a credibilidade, o prestígio ou a confiança do visado, mesmo que essa credibilidade, esse prestígio, ou essa confiança não tenham sido efetivamente atingidos. Constitui "meio de comunicação social", para o feito do nº 2 do artigo 183º do Código Penal uma página do "Facebook" acessível a qualquer pessoa e não apenas ao grupo de "amigos". Em caso de provimento de um recurso que tem como consequência a condenação do arguido, cabe ao tribunal de segunda instância fixar a pena respetiva, sem que tal implique violação do duplo grau de jurisdição.* Disponível em http://www.dgsi.pt/jtrp.nsf/c3fb530030ea1c61802568d9005cd5bb/0fab00c6a2ab290380257c2200521381?OpenDocument [Consultado em 22.10.2017].

Por outro lado, entende-se por cibercriminalidade em sentido estrito aquele tipo de criminalidade informática cujo elemento digital ou informático surge como componente integrador do tipo legal criminalmente punido, ou seja, a execução do crime vai necessariamente recorrer aos meios informáticos. Nestas situações o bem jurídico a proteger será a segurança nos bens informáticos e, a título de exemplo, podemos destacar o crime de acesso ilegítimo, burla informática e falsidade informática, que podem encontrar-se tipificados no CP, na LCiber, ou até mesmo no RGIT.

Sem embargo da distinção *supra* mencionada, comummente aceite, em 2003, PEDRO VERDELHO[108] distinguiu o cibercrime em três realidades distintas, nomeadamente: os crimes que recorrem a meios informáticos; os crimes referentes à proteção de dados pessoais; e os crimes informáticos propriamente ditos. Os primeiros seriam aqueles crimes que só podiam ser praticados através de meios informáticos, encontrando-se essencialmente previstos no CP, como por exemplo, o crime de burla informática, ou devassa por meio informático. A segunda distinção, como o próprio nome indica, referia-se aos crimes relacionados com a proteção de dados pessoais e à proteção de privacidade no setor das telecomunicações, como por exemplo, o crime de acesso indevido a dados, que, à data, era regulado pela já revogada Lei de Proteção de Dados Pessoais, Lei n.º 67/98, de 26 de outubro. Já os crimes informáticos propriamente ditos englobavam, àquela data, os crimes previstos na revogada Lei da Criminalidade Informática, Lei n.º 109/91, de 17 de agosto, como por exemplo, o crime de falsidade informática, ou acesso ilegítimo.

Por outro lado, BENJAMIM SILVA RODRIGUES optou por fazer uma distinção entre crimes informáticos digitais próprios (ou "puros"), dos impróprios (ou "impuros"), sendo que os primeiros serão aquele tipo de crimes em que estamos perante condutas penalmente relevantes, tendo em conta que são lesivas dos fluxos informacionais, comunicacionais e informático-digitais, contidos ou veiculados a partir dos computadores ou outro sistema informático-digital, tendo como objeto a "(...) integridade, fiabilidade, operacionalidade, originalidade ou genuinidade, secretismo e segurança dos fluxos informacionais e comunicacionais e

[108] Neste sentido, VERDELHO, Pedro, "*Cibercrime*", Direito da Sociedade da Informação – Volume IV, APDI – Associação Portuguesa de Direito Intelectual, Coimbra, Coimbra Editora, 2003, pp. 356 – 370.

informático-digitais (...)"[109]; enquanto os segundos se caracterizam não deter o mesmo objeto, mas antes outros bens jurídicos de natureza pessoal ou coletiva[110].

Todavia, se seguirmos os ensinamentos de RITA COELHO DOS SANTOS[111] a criminalidade informática vai deter uma classificação tripartida, nomeadamente:

- crimes tipicamente informáticos, que são aqueles cujo objeto ou instrumento da ação vital é um computador ou instrumento informático semelhante (em sentido amplo), *conditio sine qua non*[112] o tipo legal de crime não se preencherá, como por exemplo, o crime de sabotagem informática;

- crimes essencialmente informáticos, resumem-se ao tipo de crime cujo bem jurídico ofendido traduz-se numa realidade informática, como por exemplo, um programa de computador, um telemóvel. É o caso do crime de reprodução ilegítima de programa protegido no qual o bem jurídico a proteger é o *software*[113], ou seja, um verdadeiro bem jurídico informático;

- crimes acidentalmente informáticos, são aqueles cuja utilização de um instrumento informático não passa de um novo *modus operandi*[114] para a consumação da prática de um ilícito. Exemplos dessa classificação são os crimes de injúrias ou difamação.

Não obstante as classificações tri ou bipartidas do conceito de cibercrime/criminalidade informática *supra* referidas, uma coisa é certa, todas elas servem para demonstrar que o cibercrime é uma realidade crescente, em permanente evolução, sendo que aquilo que hoje é certo e irrefutável, amanhã pode ser simplesmente ultrapassado e tornar-se obsoleto, não conseguindo acolher, por isto mesmo, o total assentimento doutrinal. Por este motivo existe um receio que o Direito não consiga acompanhar os desenvolvimentos do mundo informático e das comunicações colocando em causa a própria estabilidade jurídica e, por outro lado, assiste-se ainda ao problema de se não regularmos tal realidade então não podem existir respostas

---

[109] Cfr. RODRIGUES, Benjamim Silva, *Direito Penal – Parte Especial, Tomo I – Direito Penal Informático-Digital*, Coimbra, Coimbra Editora, maio 2009, p. 279.

[110] Nesta senda, Benjamim Silva, *Direito Penal – Parte Especial, Tomo I ...*, *op. cit.,* p. 351.

[111] Neste mesmo sentido, SANTOS, Rita Coelho, *O Tratamento Jurídico-Penal Da Transferência De Fundos Monetários Através Da Manipulação Ilícita Dos Sistemas Informáticos*, Studia Iuridica 82, Coimbra, Coimbra Editora, 2005, p. 32 e ss.

[112] Do latim, "condição sem a qual", ou seja, é um requisito fundamental.

[113] Em sentido idêntico ao mencionado *supra* na nota de rodapé n.º 6.

[114] Do latim, "modo de operação", ou seja, é uma forma de agir, de executar.

eficazes por parte dos aplicadores do Direito, face às questões cada vez mais pertinentes, atuais e complexas do mundo e da sociedade atual.

4. Consagração legislativa do Cibercrime

Como já temos deixado adivinhar, perante todo o panorama previamente exposto, não existe margem para dúvidas quanto à dificuldade de gerir e combater o fenómeno do cibercrime. Se por um lado, a complexidade das causas e o anonimato dos seus agentes impulsionam a sua prática, por outra banda, a tarefa das autoridades competentes e da máquina judicial, dificulta-se quando nem sempre o resultado da prática do ilícito é instantâneo e quando o distanciamento geográfico, na maioria das vezes, é um fator chave.

Nesta sequência, importante parece-nos afirmar que nem sempre as ações criminosas praticadas através de instrumentos informáticos chegam a ser detetadas, uma vez que na maioria dos casos são utilizados vários métodos e programas que permitem a invisibilidade dos seus praticantes. Deste modo, é frequente a utilização de "anonimizadores" como por exemplo o *TOR*[115] ou o *AnonymoX* que escondem a verdadeira "identidade" de quem navega na rede *web*, permitindo uma total privacidade e anonimato[116].

Neste âmbito, é constatável a dificuldade de aplicação pura do conceito geral de territorialidade que se encontra previsto no art.º 4.º do CP[117], tendo em conta que os territórios geográficos são, tão só, uma miragem, dando lugar ao crime deslocalizado, sendo que podemos vir a ter elaborados ataques informáticos que podem não produzir os seus efeitos automaticamente podendo, inclusive, vir a repetir-se posteriormente.

Face a esta conjuntura, logicamente que o legislador se vê numa posição delicada porque por muito louvável que seja a sua intenção de tipificar e combater a criminalidade informática, existirão sempre infelizes contratempos. Assim, ele deve atender que uma excessiva

[115] Acrónimo de *"The Onion Router"*.

[116] Aliado a este tipo software e *add-on* posicionam-se as diversas técnicas de encriptação que também acabam por se revelar num obstáculo às autoridades competentes. Neste mesmíssimo sentido, SANTOS, Rita Coelho, *op. cit.*, pp. 51 e 52.

[117] A este propósito, VENÂNCIO, Pedro Dias, *"Breve Introdução..."*, *op. cit.,* p. 8.

regulamentação pode quebrar os mais básicos e imprescindíveis objetivos, sendo unicamente através de princípios claros e exatos que se conseguirá alcançar o equilíbrio ideal, propício ao exercício da liberdade.

Posto isto, no âmbito do combate ao cibercrime, o CP desde cedo estatuiu crimes especificamente praticados através de instrumentos informáticos, contudo foi só com a publicação da Lei n.º 109/91 de 17 de agosto (Lei da Criminalidade Informática) que esta realidade se completou de um modo mais extensivo. Destarte, graças à dispersão de normas criminais potenciadoras do seu próprio desconhecimento, importa fazer uma breve e coerente exposição da aplicabilidade do direito penal português aos diversos crimes informáticos, embora em traços necessariamente largos.

4.1. Código Penal

Antes de mais, importa fazer um pequeno parenteses quanto à ousadia do legislador português no que toca à tipificação dos crimes informáticos na presente lei, uma vez que foi com a revisão de 1995, i.e., finais do séc. XX (período em que a informática começa a ter um peso cada vez maior na sociedade da informação) que passamos a criminalizar condutas praticadas através de esfera digital.

Assim, na presente lei podemos, por um lado, constatar crimes cujo caráter informático é absolutamente claro como a Burla Informática e nas Telecomunicações[118], p. e p. no art.º 221.º do CP, a Violação de Correspondência ou nas Telecomunicações, p. e p. no art.º 194.º n.º 2 do CP, ou o crime de Devassa por Meio de Informática, p. e p. no art.º 193.º CP, decorrente do art.º 35º, n.º 3, da CRP[119], mas também podemos constatar, por outro lado, crimes cujo teor

[118] Introduzido pela revisão de 1995 como crime de "Burla Informática" traduz-se na produção de um engano consciente estabelecido por intermediação da manipulação de um sistema informático e não através da afetação direta em relação a uma pessoa (como o crime de burla p. e p. pelo art.º 217.º do CPC, apesar de prever objetivos materiais e finais idênticos. Acórdão do Tribunal da Relação de Évora de 26-06-2012, disponível em http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/9e4d23e33c93144580257de10056f883?OpenDocument [Consultado em 29.04.2017].

[119] Pode ler-se o regime do n.º 3 do art.º 35.º da CRP:

criminal telemático pode não ser tão explícito, exemplos disso mesmo são os crimes previstos no art.º 225.º (abuso de cartão de garantia ou crédito), o art.º 267.º n.º 1 al. e) (equiparação a moeda dos cartões de garantia ou de crédito)[120], ou os inevidentes crimes previstos nos artigos 153.º (Ameaça); 154.º (Coação); 180.º (Difamação); 181.º (Injúria) e 187.º (Ofensa a Organismo, Serviço ou Pessoa Coletiva), cuja informática poderá tornar-se um meio idóneo na prática de tais delitos.

Não obstante as pequenas contribuições do CP, só o podemos ter como o instrumento legislativo subsidiário no combate ao cibercrime atendendo à posição que é hoje ocupada pela Lei do Cibercrime e/ou Convenção sobre o Cibercrime.

4.2. Lei da Criminalidade Informática, Lei n.º 109/91 de 17 de agosto

Foi o verão de 1991 que ficou marcado pela aprovação da Lei n.º 109/91 de 17 de agosto, também conhecido por Lei da Criminalidade Informática. Foi este o primeiro diploma que, em dezanove artigos, claramente regulou a matéria referente ao cibercrime (na data da sua publicação ainda era designado de crime informático), apresentando o "catálogo" de crimes ligados à informática, as suas penas acessórias e ainda regulou a responsabilidade criminal das pessoas coletivas.

É constatável que este diploma se inspirou de tal modo na Recomendação n.º R (89) 9 do Conselho da Europa, de 13/9[121], normativo elaborado pelo Conselho da Europa, sobre a criminalidade informática, que praticamente não passou de uma tradução literal da mesma. À data da publicação da Recomendação visava-se unicamente a descrição e punição dos crimes informáticos, uma vez que o acesso à Internet era praticamente exclusivo dos âmbitos

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

[120] Neste sentido, MARTINS, António Gomes Lourenço / MARQUES, J. A. Garcia / DIAS, Pedro Simões, *op. cit.*, p. 434.

[121] VERDELHO, Pedro, "*A nova Lei do Cibercrime",* Scientia Iuridica– Revista de Direito Comparado Português e Brasileiro, Tomo LVIII, n.º 320, Braga, Universidade do Minho, outubro/dezembro, 2009, p. 717.

empresariais e académicos, fazendo com que a Lei da Criminalidade Informática não se tornasse muito extensa.

Todavia, como bem sabemos, perante uma realidade cada vez mais galopante e célere como a Informática, rapidamente a Recomendação do Conselho da Europa e Lei da Criminalidade Informática se tornaram obsoletas[122]. Por isso, em 1997, constatou-se a necessidade de reexame à Recomendação n.º R (89) 9 do Conselho da Europa, nascendo, deste modo, o primeiro tratado internacional sobre o cibercrime.

4.3. Convenção do Conselho da Europa sobre a Cibercriminalidade

Assumindo muitas das conceções expressas na Recomendação n.º R (89) 9 do Conselho da Europa, a Convenção sobre o Cibercrime (também denominada por Convenção de Budapeste), como o próprio nome indica, é um tratado internacional com vista ao combate ao Cibercrime, criado por 41 representantes de Estados-membros do Conselho da Europa e 4 Estados exteriores (EUA, Canadá, Japão e África do Sul) adotado em Budapeste, a 23 de novembro de 2001 e ratificado por Portugal através da Resolução da AR n.º 88/2009 e Decreto do PR n.º 92/2009, publicados a 15 de setembro[123]. Apesar de ser um documento elaborado no seio europeu, desde sempre se pretendeu a sua extensão a nível mundial[124], atendendo às repercussões globais do cibercrime.

A Convenção visa a prevenção de todo o tipo de ilícitos informáticos, tais como os atentados à confidencialidade e disponibilidade de sistemas informáticos, bem como o uso fraudulento de tais sistemas, assegurando a respetiva criminalização de tais condutas[125]. Numa realidade tão global e célere como aquela em que vivemos estranho seria se a cooperação internacional não se tornasse numa realidade atendo à necessidade de entreajuda entre os países, à impossibilidade da territorialização do cibercrime e à sua rápida propagação.

---

[122] Neste mesmo sentido, VERDELHO, Pedro, "*A Convenção sobre o Cibercrime do Conselho da Europa – Repercussões na Lei Portuguesa",* Direito da Sociedade da Informação – Volume VI, APDI – Associação Portuguesa de Direito Intelectual, Coimbra, Coimbra Editora, 2006, p. 257.

[123] Neste sentido, VENÂNCIO, Pedro Dias, *Lei do Cibercrime..., op. cit.*, p. 21.

[124] A este propósito, VERDELHO, Pedro, *"Cibercrime..."*, *Idem, ibidem.*

[125] Neste mesmíssimo sentido, MARTINS, António Gomes Lourenço, *Criminalidade Informática..., op. cit.*, pp. 38 e 39.

No lapidar dizer de PEDRO VERDELHO[126], a Convenção caracteriza-se por ser o primeiro grande trabalho, de relevo, à escala global sobre o cibercrime, criando a primeira plataforma de entendimento no âmbito penal, processual penal e cooperação internacional, através de estabelecimentos mínimos comuns aos diferentes ordenamentos jurídicos, pretendendo que, face ao cibercrime, as diversas jurisdições assumam e adotem idênticos instrumentos processuais e de produção de prova, bem como o estabelecimento de medidas ocultas de investigação criminal, em vários meios como o computador, redes, sistemas e/ou serviços informáticos. No fundo, este diploma legal destaca-se pela criação de 3 objetivos principais, nomeadamente:

1) harmonização da legislação sobre o cibercrime;
2) estabelecimento nas diferentes jurisdições determinados instrumentos processuais e de produção de prova modernos e adequados à investigação da cibercriminalidade, ou seja, pretende a adoção de práticas processuais nacionais e internacionais idênticas e suficientes para a investigação do cibercrime;
3) facilitação da cooperação internacional, viabilizando as investigações transfronteiriças.

Dividida em quatro capítulos, a Convenção pretendeu[127]: no Capítulo I (Utilização e Terminologia), abranger as disposições relativas à criminalização dos crimes informáticos, definindo nove infrações, agrupadas em quatro categorias diferentes, versando a responsabilidade acessória e ainda as sanções; no Capítulo II (Medidas a empreender ao nível nacional – direito substantivo e direito processual) visa determinar as condições e salvaguardas gerais processuais (bem como os seus poderes), terminando com as disposições relativas à jurisdição; no Capítulo III (Cooperação Internacional) constataram-se as disposições relativas à assistência mútua em casos de crime informático internacional, bem como regras de extradição; e por último, no Capítulo IV (Disposições Finais), consagrar as cláusulas finais.

Em Portugal, a ratificação da Convenção de Budapeste contemplou unicamente algumas adaptações, que mais não passaram de atualizações, uma vez que Portugal já tinha "transposto" para a legislação nacional a Recomendação n.º R (89) 9 com a Lei da Criminalidade Informática. Assim sendo, em sede substantiva, a Convenção não revelou grandes inovações atendendo ao facto que a lei nacional que se encontrava vigente à data já cobria

[126] VERDELHO, Pedro, *"A Convenção sobre o Cibercrime..."*, *op. cit.,* p. 258.

[127] A este propósito, VERDELHO, Pedro / BRAVO, Rogério / ROCHA, Manuel Lopes, *Leis do Cibercrime - vol. I*, Lisboa, Centro Atlântico, julho 2003, pp. 108 e 109.

substancialmente a maioria dos seus preceitos, no entanto, face à passagem normal do tempo, as realidades previstas já evidenciavam algumas insuficiências e desatualizações, havendo, por isso, a necessidade de adotar conceitos mais abrangentes e atualizados[128].

Por outro lado, quanto ao âmbito processual penal, podemos dizer que a Convenção já trouxe algumas alterações substanciais principalmente ao nível dos instrumentos de investigação, como por exemplo, formas de recolha e conservação de prova, destacando-se, deste modo, a preservação expedita de dados armazenados em computador (aplicável unicamente a todo o tipo de dados guardados num computador ou sistema de computadores) e a revelação expedita de dados de tráfego de forma rápida e urgente (aplicável unicamente aos dados de tráfego)[129].

No âmbito da competência territorial, a Convenção consagrou a competência dos Estados signatários que, por sua vez, se devem declarar competentes "(...) para prosseguir criminalmente os seus cidadãos nacionais, independentemente do local da prática dos factos, em caso de a infração ser punível no local onde foi cometida ou ainda no caso de estes factos não poderem ser conhecidos por nenhuma jurisdição nacional (...)"[130].

Na senda da cooperação internacional, predominou, na Convenção, a referência e a remissão para outros tratados internacionais, não criando novos procedimentos nem novas formas de cooperação. No entanto, face às especificidades e rapidez do ambiente digital em que se insere, este diploma acabou por prever a criação de figuras menos intrusivas e desconhecidas de anteriores tratados a serem utilizadas independentemente do tipo de crime, como por exemplo, a preservação expedita de dados informatizados armazenados, art.º 29.º ou a divulgação expedita dos dados de tráfego conservados, art.º 30.º.

Não é novidade que os dados informatizados são altamente frágeis, atendendo à facilidade com que são apagados, movidos, ou alterados, com um inocente premir de teclas[131]. Assim, é através desta nova modalidade que as autoridades competentes de um Estado signatário solicitam às de outro Estado, que por sua vez deverá assegurar rapidamente a disponibilidade de tais dados (por um período de, pelo menos, 60 dias), de acordo com o seu

[128] Neste mesmo sentido, VERDELHO, Pedro, *"A Convenção sobre o Cibercrime..."*, *op. cit.,* pp. 259 e 260.

[129] Neste sentido, VERDELHO, Pedro, *"A Convenção sobre o Cibercrime..."*, *op. cit.,* pp. 268 – 270.

[130] Cfr. VERDELHO, Pedro, *"A Convenção sobre o Cibercrime..."*, *op. cit.,* p. 273.

[131] Assim o referem, VERDELHO, Pedro / BRAVO, Rogério / ROCHA, Manuel Lopes, *Leis do Cibercrime..., op. cit.,* p. 212.

direito interno, manifestando a intenção de vir a fazer-lhes um pedido formal de cooperação internacional[132]. Qualquer Estado pode negar o pedido de preservação de dados informáticos, tendo por base a imposição da condição da dupla incriminação, ou seja, um Estado signatário pode ver o seu requerimento de conservação negado se o ato "criminoso" não for objeto de censura no Estado requerido, ou quando preenche um dos requisitos previstos no art.º 29.º n.º 5 da Convenção[133].

Já no âmbito da divulgação expedita dos dados informáticos, constatamos que aquando do decurso de um pedido de conservação de dados de tráfego, de acordo com o art.º 29.º, o Estado Requerido descobre que um Estado terceiro participou na transmissão da comunicação, então o Estado requerido deverá transmitir rapidamente ao requerente dados de tráfego suficientes para identificar esse prestador de serviços bem como o trajeto utilizado para a transmissão da comunicação.

Tendo em conta que a revolução nas NTIC conferiu e continuará a conferir novos contornos em quase todos os aspetos da vida em sociedade, consequentemente irá sempre representar novos desafios aos conceitos jurídicos pré-existentes. Assim, atendendo ao constante desenvolvimento e diversas mutações tecnológicas, sociais e morais, urge ao legislador não só a adoção de instrumentos internacionais, bem como a atualização premente da legislação nacional.

4.4. Lei do Cibercrime, Lei n.º 109/2009, de 15 de setembro

Ora, foi face ao decurso do tempo, aos novos desafios tecnológicos, à desatualização da Lei da Criminalidade Informática e aos sucessivos Projetos de Lei[134] e Propostas de Lei[135] [136] que,

[132] Todavia, os dados requeridos poderão não ser expeditamente revelados ao Estado requerente, como acontece internamente, nesta senda, VERDELHO, Pedro, *"A Convenção sobre o Cibercrime…", op. cit.,* pp. 274 e 275.

[133] Neste mesmo sentido, RODRIGUES, Benjamim Silva, *Da Prova Penal, Tomo II…, op. cit.,* p. 428.

[134] Em 2003, no seio da AR, foi discutido o Projeto de Lei n.º 217/IX de 27 de janeiro de 2003 que refletia a criação de um regime jurídico de obtenção de prova digital eletrónica na Internet. Tendo em vista a reserva da intimidade da vida privada e o sigilo das telecomunicações, este Projeto de Lei visava brindar as autoridades competentes de novos meios para a investigação eletrónica, pretendendo que estas acedessem, em tempo útil, a informações que permitissem a identificação dos autores da prática de um crime. Para melhor desenvolvimento sugere-se a leitura de RODRIGUES, Benjamim Silva, *Da Prova Penal, Tomo IV…, op. cit.,* pp. 418 e 419.

em 2009, inspirada pelas novas fontes internacionais como a Convenção de Budapeste ou até mesmo a Decisão-Quadro 2005/222/JAI do Conselho de 24 de fevereiro de 2005 (relativa a ataques contra sistemas de informação)[137], que surgiu a Lei do Cibercrime. Em 2009, uma vez que, com o normal decurso do tempo, a Lei da Criminalidade Informática já apresentava algum desgaste perfeitamente normal, atendendo já à sua longevidade, foi através da LCiber que o legislador português conseguiu transpor para o nosso ordenamento jurídico novos tipos de crimes que ainda não se encontravam previstos na revogada Lei, chegando mesmo a ajustar os ilícitos já previstos, face às novas realidades.

Com esta nova Lei, assistiu-se a pequenas alterações no que respeita ao direito penal substantivo, no entanto, a sua inovação refletiu-se no âmbito do direito penal adjetivo, atendendo às normas processuais específicas que o ordenamento jurídico português passou a prever. Foi assim que, bebendo da Convenção de Budapeste, o legislador português introduziu novos meios de investigação e produção de prova específicos para o combate à criminalidade informática, consagrando normas respeitantes ao direito penal substantivo, adjetivo e ainda normas respeitantes à cooperação internacional, num único diploma.

No que concerne às disposições de direito penal material, nas eruditas palavras de PEDRO VERDELHO[138], a LCiber introduziu alguns conceitos inovadores, desde logo, em algumas definições constantes do art.º 2.º, como por exemplo, as alíneas a), b) c) e d) que passaram a reproduzir conceito mais técnicos e ajustados face à nova realidade digital. Relativamente à al. a) o conceito de "sistema informático", era um conceito que simplesmente não se consubstanciava na pretérita Lei da Criminalidade Informática, havendo, por isso a necessidade de se criar uma noção tecnologicamente neutra e resistente às constantes mutações da realidade digital. Deste modo, foi com vista à inclusão dos tradicionais computadores, dispositivos informáticos e comunicacionais que a LCiber passou a concretizar este novo contexto. Por um lado, relativamente ao conceito de "dados informáticos", o legislador optou por criar um conceito atual e ajustado que visasse incluir, ontologicamente, a definição anterior de menor dimensão. Por

[135] Surgindo no seguimento do Projeto de Lei 217/IX, a Proposta de Lei n.º 155/IX, Regime Jurídico de Obtenção da Prova Digital Eletrónica, de 4 de dezembro de 2004, teve como principal objeção o facto de se prender com classificações de vários tipos de dados que não respeitavam os critérios estabelecidos internacionalmente. Neste sentido, RODRIGUES, Benjamim Silva, *Da Prova Penal, Tomo IV...*, *op. cit.*, pp. 431 – 443.

[136] Contudo tais projetos acabaram por não prosperar. VENÂNCIO, Pedro Dias, *Lei do Cibercrime...*, *op. cit.*, p. 23.

[137] Tem por objetivo fortalecer a cooperação entre as autoridades policiais e outros serviços especializados, mediante a aproximação de disposições de direito penal em matéria de ataques contra os sistemas informáticos. Nesta senda, VENÂNCIO, Pedro Dias, *Lei do Cibercrime...*, *op. cit.*, p. 329 e ss.

[138] Neste mesmo sentido, VERDELHO, Pedro, *"A nova Lei do Cibercrime..."*, *op. cit.*, pp. 719 – 723.

outro lado, os "dados de tráfego" trazidos pela alínea c), distintos dos dados de conteúdo e de localização, refletem praticamente uma transposição clara da al. d) do art.º 1.º da Convenção sobre o Cibercrime, tratando-se de um importante conceito que pode ser objeto de diversas medidas processuais em sede de investigação criminal e graças à obrigação de conservação dos mesmos por parte das operadoras, nos termos da Lei n.º 32/2008, de 17 de julho (Conservação de Dados Gerados ou Tratados no Contexto Oferta de Serviços de Comunicações Eletrónicas). Por fim, no que respeita ao "fornecedor de serviços", a sua introdução visou sobretudo ultrapassar a desatualização cujos antiquados conceitos sofriam.

Acresce ainda que, no âmbito das imposições da Decisão Quadro 2005/222/JAI e da Convenção sobre o Cibercrime, a Lei do Cibercrime consagrou a responsabilização das pessoas coletivas que, por sua vez, são responsabilizadas quanto aos ilícitos previstos a partir do art.º 3.º da mesma lei, no mesmo ponto de vista que o são quanto aos crimes previstos no CP.

Assim, para cabal compreensão da temática da presente dissertação, antes de entrar no real âmago da questão e atendendo ao atual panorama legislativo do cibercrime, a nosso ver, importa fazer uma lacónica referência aos principais crimes que se encontram previstos na Lei n.º 109/2009, fazendo uma breve passagem pelas principais disposições processuais:

4.4.1. Crime de falsidade Informática, art.º 3.º da LCiber

É a primeira definição penal material da Lei do Cibercrime, parcialmente coincidente com o dano informático, tendo por referência o art.º 4.º da Lei da Criminalidade Informática. Foi desta forma que a essência do crime se manteve, sendo-lhe atribuídas matrizes redaccionais mais simples, cujo bem jurídico a tutelar se caracteriza por ser a integridade dos sistemas de informação. As principais alterações refletiram-se nas novas modalidades de atuações ilegítimas como a falsificação de dados registados ou incorporados em cartão bancário de pagamento ou qualquer outro dispositivo de pagamento, tais como os cartões de crédito, débito direto, cartões telefónicos (*SIM Cards – Subscriber Identity Module*[139]) que permitam o acesso a redes de

[139] *Subscriber Identity Module*, em português, "módulo de identificação do assinante". *Vide*: http://searchmobilecomputing.techtarget.com/definition/SIM-card [Consultado em 15.07.2017].

telecomunicações e ainda outros dispositivos que permitam o acesso a serviços condicionados, como por exemplo, um cartão específico de uma empresa.

Neste artigo é também tipificada a conduta cometida por quem "importar, distribuir, vender, ou detiver para fins comerciais qualquer dispositivo"[140] que permita a prática das falsificações previstas no n.º 2, sendo que na maioria das decisões publicadas é feita uma interpretação literal e restrita dos seus elementos constitutivos. Apesar de ser vulgarmente associado à falsificação de cartões bancários[141], contudo, os tribunais portugueses já se pronunciaram quanto a casos mais *sui generis*[142].

4.4.2. Dano relativo a programas ou outros dados informáticos, art.º 4.º da LCiber

Este ilícito já constava no "cardápio" da Lei da Criminalidade Informática, no seu art.º 5.º, que, só por si, já satisfazia na globalidade as exigências da Decisão Quadro e da Convenção do Cibercrime. No fundo, as principais alterações introduzidas visaram unicamente as imposições da Convenção do Cibercrime e a consagração de novas modalidades da ação típica.

No n.º 3 do respetivo artigo é possível constatar um novo objeto do tipo legal de crime, nomeadamente, a tipificação da produção, venda, distribuição, ou disseminação daquilo a que apelidamos de *malware*. Neste artigo é constatável que aquilo que antigamente era visto como um ato preparatório do crime de dano, hoje, mesmo que o ato não venha a produzir os seus efeitos, haverá consequências para o infrator[143].

---

[140] *Vide* art.º 3.º n.º 4 da Lei do Cibercrime, Lei n.º 109/2009, de 15 de setembro, disponível em http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1137&tabela=leis [Consultado em 29.04.2017].

[141] Nesta situação considerou-se crime de falsidade informativa a captura, em ATM, da informação existente na banda magnética de cartão de crédito. *Vd* Acórdão do Tribunal da Relação do Porto de 17-09-2014, disponível em http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/5fd1df126b7ffe9880257d6600370f95?OpenDocument [Consultado em 29.04.2017].

[142] Neste caso foram introduzidos no sistema informático do hospital falsos episódios de cirurgias realizadas em regime de ambulatório. Assim, uma vez que tais dados colocavam em causa o seu próprio valor probatório, bem como o da segurança e certeza jurídica, o Tribunal consignou que estes detinham os mesmos efeitos de um documento falsificado. *Vd* Acórdão do Tribunal da Relação do Porto de 26-05-2015, disponível em http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/aa9d0fb297dcca7880257e62003a86e4?OpenDocument [Consultado em 29.04.2017].

[143] Neste sentido, VERDELHO, Pedro, *"A nova Lei do Cibercrime...", op. cit.,* pp. 726 e 727.

4.4.3. Sabotagem Informática, art.º 5.º da LCiber

Mais uma vez, assiste-se a uma evolução da redação da Lei da Criminalidade Informática, tendo em conta que este conceito também se encontrava previsto no art.º 6.º da Lei n.º 109/91. Partilhando o destino dos artigos já mencionados, também o art.º 5.º da Lei n.º 109/2009 não apresenta alterações muito significativas, mantendo-se a principal estrutura do tipo legal de crime[144].

Porém, reproduzindo também os ideais quanto ao dano informático, este conceito acabou também por punir a difusão de programas maliciosos cuja finalidade vertesse na sabotagem informática. Anote-se também que se da atuação do agente resultarem consequências de grande dimensão, como por exemplo o ataque ao servidor de uma cadeia de supermercados, a moldura penal aplicável será a prevista no n.º 5 do art.º 5.º. O problema é que nem sempre é fácil quantificar as perdas monetárias fruto das sabotagens informáticas[145].

4.4.4. Acesso Ilegítimo, art.º 6.º da LCiber

A essência da norma surge do regime previsto no art.º 7.º da Lei da Criminalidade Informática, tutelando a "integridade do sistema informático lesado". No entanto, foram feitos alguns ajustamentos que, tal como aconteceu com outros ilícitos já mencionados, pune a mera tentativa. Na prática houve uma simplificação da redação, contudo é de relevar a incontestabilidade que, na atualidade e com o atual regime legislativo, independentemente do propósito lucrativo, ou não, do agente, haverá sempre lugar à consumação do crime. Deste modo, tal como resulta da letra da lei, apenas se exige o dolo genérico.

De acordo com o Tribunal da Relação do Porto este tipo de crime, na sua essencialidade, veio "(...) cobrir a área do que se vem denominando de "hacking informático"

[144] Neste sentido, VENÂNCIO, Pedro Dias, *Lei do Cibercrime...*, *op. cit.*, p. 53.

[145] VERDELHO, Pedro, *"A nova Lei do Cibercrime..."*, *op. cit.,* p. 728.

[146]", sendo de relevar a pretensão da lei em punir o chamado roubo de identidade, art.º 6.º n.º 2. Genericamente, passou a ser punida a atuação daqueles que, através de sistemas informáticos, obtêm informações confidenciais de terceiros (*PIN's*, *passwords*...) que lhes permitem aceder a plataformas não autorizadas, como por exemplo, contas de redes sociais, correio eletrónico, *homebanking*...

4.4.5. Interceção ilegítima, art.º 7.º da LCiber

O seu texto em pouco difere do art.º 8.º da Lei da Criminalidade Informática, tendo desaparecido algumas expressões tais como "rede informática". Seguindo o preceituado noutras disposições também neste artigo antecipou-se a tutela penal, fazendo com que a tentativa fosse punível.

Paralelamente a este crime identificamos o crime de violação de correspondência ou telecomunicações, p. e p. nos termos do art.º 194.º do CP. Face à redação do artigo em causa, não podem restar dúvidas que este visa principalmente a proteção da privacidade no ponto de vista da segurança e confiança jurídica[147].

4.4.6. Reprodução ilegítima de programa protegido, art.º 8.º da LCiber

Corresponde ao antigo art.º 9.º da Lei da Criminalidade Informática, divergindo apenas em algumas considerações com vista à uniformização da terminologia. No fundo esta norma visa a punição da violação dos direitos de autor sobre programas de computador, mesmo que tal duplicação não tenha fins comerciais.

---

[146] *Vd* Acórdão do Tribunal da Relação do Porto de 08-01-2014, disponível em http://www.dgsi.pt/jtrp.nsf/d1d5ce625d24df5380257583004ee7d7/b54faf2d4330b8d480257c6e004ff2df?OpenDocument [Consultado em 29.04.2017].

[147] VENÂNCIO, Pedro Dias, *Lei do Cibercrime...*, *op. cit.*, p. 68.

4.4.7. Responsabilidade penal das pessoas coletivas e entidades equiparadas, art.º 9.º da LCiber

Uma outra referência da LCiber tem a ver com a responsabilização criminal das pessoas coletivas ou entidades equiparadas, apesar de tal estatuição legal não ser uma absoluta novidade. De facto, já a revogada Lei da Criminalidade Informática regulava exacerbadamente a responsabilidade criminal das pessoas coletivas, tendo em conta que à data da sua publicação, na legislação penal geral, tal regime era inexistente.

Todavia, uma vez que à data da publicação da LCiber o CP já previa um regime geral de responsabilização das pessoas coletivas, o legislador português não sentiu a mesma necessidade que sentia à data da publicação da Lei da Criminalidade Informática. Por isto, bebendo do regime da Decisão-Quadro 2005/222/JAI e da Convenção de Budapeste, foi deixado claro na atual LCiber que as pessoas coletivas devem ser responsabilizadas nos mesmos termos e limites da responsabilização previstos no art.º 11.º do Código Penal[148].

4.4.8. Perda de bens, art.º 10.º da LCiber

Apesar da redação ligeiramente diferente, é constatável que o atual regime do art.º 10.º da LCiber, no qual é regulada a matéria quanto à perda a favor do Estado de objetos utilizados para a prática de crimes informáticos, é inspirado no art.º 12.º da Lei da Criminalidade Informática.

Ora, do agora preceituado no art.º 10.º parece que ficou à livre apreciação do julgador o decretamento da perda a favor do Estado dos objetos, materiais ou equipamentos apreendidos, sem qualquer critério decisivo. Assim, a pergunta que se impõe é se, na falta de critério, deverá o tribunal recorrer às regras gerais dos artigos 109.º a 111.º do CP, por força do art.º 28.º da

[148] Neste sentido, VERDELHO, Pedro, *"A nova Lei do Cibercrime...", op. cit.,* pp. 723 e 724.

LCiber[149]? Isto porque não pode a lei prever, em matéria penal, decisões arbitrárias, sem fornecimento de qualquer critério decisório.

Se assim for, não se vislumbra qualquer efeito útil do suposto regime "especial" do art.º 10.º, uma vez que se limita à remissão para o regime geral. Acresce ainda que, na versão prevista na Lei da Criminalidade Informática previa-se que a perda de bens "abrangia o lucro ilícito obtido com a prática da infração", contudo tal particularidade foi retirada com a LCiber, criando um regime mais favorável para o infrator[150].

De acordo com o Relatório Anual de Segurança Interna de 2016[151], em Portugal, assistiu-se a um aumento de alguns tipos de ilícitos praticados através de instrumentos informáticos, sendo o esquema *infra*, um leal espelho dessa realidade:

	Detidos		Prisão preventiva		Arguidos constituídos	
Tipo de crimes	Ano 2015	**Ano 2016**	Ano 2015	**Ano 2016**	Ano 2015	**Ano 2016**
Acesso ilegítimo ou indevido	0	**3**	0	**0**	54	**39**
Intercepção ilegítima	0	**0**	0	**0**	0	**0**
Burla informática e nas comunicações	18	**31**	6	**3**	322	**330**
Viciação/Dano relativo a dados ou programas informáticos	0	**0**	0	**0**	1	**0**
Devassa por meio informático	2	**1**	1	**0**	11	**8**
Falsidade informática	1	**0**	0	**0**	8	**16**
Reprodução ilegítima de programas protegidos	0	**0**	0	**0**	12	**5**
Sabotagem informática	0	**0**	0	**0**	6	**4**

Figura n.º 1: Análise dos inquéritos – detidos, prisão preventiva e arguidos constituídos referente aos anos de 2015 e 2016

[149] *Vide* o art.º 28.º da Lei n.º 109/2009, de 15 de setembro: *Em tudo o que não contrarie o disposto na presente lei, aplicam-se aos crimes, às medidas processuais e à cooperação internacional em matéria penal nela previstos, respetivamente, as disposições do Código Penal, do Código de Processo Penal e da Lei n.º 144/99, de 31 de Agosto.*

[150] Ainda nesta sentido, VERDELHO, Pedro, *"A nova Lei do Cibercrime...", op. cit.,* pp. 732 e 733.

[151] Cfr. Relatório Anual de Segurança Interna – Ano 2016, *op. cit.*, p. 32.

4.4.9. Disposições Processuais

Após este breve ensaio sobre as disposições penais materiais da LCiber, no que à matéria que trazemos em discussão concerne, cumpre agora fazer uma simples resenha quanto às estatuições processuais, uma vez que foi neste âmbito que se assistiu a uma verdadeira inovação, tendo-se criado novas normas com o objetivo de serem aplicadas em investigações cibercriminais, adaptando-as aos institutos de processo penal.

Deste modo, para além do art.º 11.º da LCiber definir o regime processual aplicável, no fundo, vai estendê-lo a dois segmentos de criminalidade, nomeadamente: os crimes cometidos por meio de um sistema informático e os crimes que se encontrem resguardados em suporte digital.

Dando cumprimento às obrigações resultantes nos artigos 16.º, 17.º e 18.º da Convenção sobre o Cibercrime, o legislador português veio criar novas figuras de preservação e revelação expedita de dados de tráfego, previstas nos arts.º 12.º e 13.º da LCiber, bem como de injunção para a apresentação ou concessão do acesso a dados, art.º 14.º da LCiber.

No art.º 12.º, em termos práticos, descreve-se a possibilidade de as autoridades judiciárias ordenarem a terceiros (primordialmente fornecedores de Internet) a preservação das transmissões de dados informáticos específicos, bem como os meramente armazenados num sistema informático. Deve atender-se que o artigo impõe simplesmente a obrigação de preservação desses dados por um certo período de tempo (medida cautelar não intrusiva), não oferecendo aos OPC a sua obtenção. No fundo, este artigo vem completar e reforçar o preceituado pela Lei n.º 32/2008.

Por outro lado, PEDRO VERDELHO[152] afirma que não é novidade para ninguém que uma comunicação criminosa ou mal-intencionada raramente utiliza sempre o mesmo serviço do mesmo fornecedor. Como tal, na maioria dos casos, a informação respeitante ao caminho efetuado pela comunicação, i.e, de onde ela veio e para onde ela foi, pode ficar registada de forma repartida por vários fornecedores de serviços, refletindo-se em demoras prejudiciais para a investigação criminal. Logo, foi face à imprescindibilidade de obtenção de forma expedita e eficaz

[152] Neste sentido, VERDELHO, Pedro, *"A nova Lei do Cibercrime..."*, *op. cit.*, p. 737.

do percurso informático de uma comunicação que a LCiber consagrou no seu art.º 13.º a revelação expedita de dados.

No que concerne à injunção para apresentação ou concessão do acesso a dados, a disposição inspirada no art.º 18.º da Convenção de Budapeste é verdadeiramente inovadora. É face à dificuldade sentida pelos investigadores, no que toca ao acesso à informação que se encontra armazenada nos modernos sistemas informáticos, que o legislador consagrou a colaboração obrigatória de quem tem a disponibilidade e domínio sobre esses mesmos sistemas informáticos, proibindo a recusa de cooperação da pessoa que tenha disponibilidade ou controlo sobre os dados informáticos.

Não obstante a proibição de recusa de cooperação, o âmbito deste regime não é absoluto, tendo em conta que nos termos dos n.ºs 5, 6 e 7 do art.º 14.º da LCiber a injunção não pode ser dirigida a suspeitos, arguidos, profissões sujeitas a sigilo profissional (e.g. advocacia ou atividades médicas) ou segredos de Estado, sendo aplicável com as necessárias adaptações o regime do segredo profissional do art.º 182.º do CPP.

A LCiber também procedeu à adaptação para o mundo virtual de novos meios de obtenção de prova que, através de um olhar mais atento, podemos concluir que não passam de uma adaptação à nova realidade digital dos clássicos meios de obtenção de prova previstos no CPP. Como tal, a LCiber passou a descrever a pesquisa de dados informáticos, art.º 15.º, a apreensão de dados informáticos, art.º 16.º, a apreensão de correio eletrónico e registos de comunicações de natureza semelhante, art.º 17.º e a interceção de comunicações, art.º 18.º.

Desde logo, no caso dos artigos 15.º e 16.º da LCiber, ou seja, no caso das pesquisas e apreensões de dados informáticos resulta da lei que a competência para ordenar cada uma das diligências depende das autoridades competentes em cada fase processual. No fundo, o art.º 15.º da LCiber mais não é do que uma busca no ambiente digital, sendo aplicável com as necessárias adaptações as regras de execução de buscas previstas no CPP. Nos termos do art.º 15.º n.º 5, mediante autorização ou ordem da autoridade competente, é permitida a extensão da pesquisa a outros sistemas informáticos. Isto consubstancia-se, por exemplo, naquelas situações em que é permitida a pesquisa de elementos num serviço de correio eletrónico quando o objeto

sujeito a pesquisa é um computador, havendo, por isso, dois objetos sujeitos a pesquisa, uma vez que, para além do visado, mais ninguém consegue aceder à conta de correio eletrónico[153].

Por outro lado, no âmbito das apreensões é constatável a salvaguarda quanto aos sistemas informáticos utilizados no âmbito de atividades sujeitas a sigilo profissional, art.º 16.º n.º 5, sendo ainda de ressalvar a preocupação da LCiber no que respeita à obrigatoriedade de intervenção do JIC, sob pena de nulidade, sempre que sejam apreendidos dados ou documentos informáticos cujo conteúdo seja suscetível de revelar dados pessoais ou íntimos que coloquem em causa a privacidade do seu titular, art.º 16.º n.º3[154]. É ainda de realçar, nos termos do art.º 16.º n.º 7, o tratamento específico dado às apreensões de dados informáticos, uma vez que este preceito consagra um tratamento menos lesivo como, por exemplo, a preservação da integridade dos dados, a apreensão por realização de cópia de dados, e o bloqueio do acesso aos mesmos[155].

Não procederemos, no entanto, a uma mais aprofundada análise, tanto do art.º 17.º como do art.º 18.º da LCiber, bem como das questões que se relacionam, por motivos de estruturação e economia de trabalho, tendo em conta que serão alvo de destaque no quarto e último capítulo da presente dissertação.

Por fim, com o art.º 19.º o legislador português tomou a liberdade de se distanciar do texto preceituado na Convenção sobre o Cibercrime, inserido na sua última disposição processual a admissibilidade do recurso às ações encobertas[156] aos crimes expressamente previstos na LCiber, mas também a todos aqueles "cometidos por meio de um sistema informático, quando lhes corresponda, em abstrato, pena de prisão de máximo superior a 5 anos ou, ainda que a pena seja inferior, e sendo dolosos, os crimes contra a liberdade e autodeterminação sexual nos casos em que os ofendidos sejam menores ou incapazes, a burla qualificada, a burla informática

---

[153] Neste sentido, VERDELHO, Pedro, *"A nova Lei do Cibercrime...", op. cit.*, p. 742.

[154] Atendendo à importância e fragilidade da prova cujo conteúdo é suscetível de revelar dados pessoais ou íntimos que possam colocar em causa a privacidade do seu titular ou de terceiros, sempre que subsistam dúvidas quanto à verificação de um crime, "(...) o chamado "corpo de delito", tem que ser especialmente flexível (...)" devendo ser apresentado, sob pena de nulidade, ao juiz que decidirá a sua junção tendo em conta os interesses do caso concreto. Acórdão do Tribunal da Relação do Porto de 13-04-2016, disponível em http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/ef54d51d3972157d80257fa4002e2d75?OpenDocument [Consultado em 14.05.2017].

[155] Em sentido idêntico, VERDELHO, Pedro, *"A nova Lei do Cibercrime..."*, *Idem, ibidem.*

[156] *Vide* o art.º 1.º n.º 2 da Lei n.º 101/2001, de 25 de agosto*: Consideram-se ações encobertas aquelas que sejam desenvolvidas por funcionários de investigação criminal ou por terceiro atuando sob o controlo da Polícia Judiciária para prevenção ou repressão dos crimes indicados nesta lei, com ocultação da sua qualidade e identidade.*

e nas comunicações, a discriminação racial, religiosa ou sexual, as infrações económico financeiras, bem como os crimes consagrados no título IV do Código do Direito de Autor e Direitos Conexos"[157].

Já relativamente à Cooperação Internacional a LCiber para além de incluir um capítulo sobre esta matéria também vai prever alguns institutos inovadores de cooperação internacional, como por exemplo a possibilidade de em Portugal se proceder à preservação e revelação expedita de dados informáticos no âmbito internacional, ou até mesmo o acesso a dados informáticos. Todavia, o maior destaque passa pela criação de um ponto de contacto permanente para a cooperação internacional, a funcionar durante 24 horas por dia, 7 dias por semana, no seio da PJ, assegurando toda a cooperação internacional urgente[158].

Por fim, importa ainda afirmar que também é estabelecida na LCiber a competência jurisdicional e territorial quanto aos cibercrimes. Assim, devido à inexistência de fronteiras e identidades na esfera digital, importa estabelecer qual o direito material aplicável e quais os tribunais competentes para os casos em concreto, uma vez que não podemos aplicar as regras gerais de localização espacial do ilícito. Assim, nos termos do art.º 27.º é determinada a aplicabilidade da LCiber quando estivermos perante factos praticados por portugueses cuja lei a aplicar não seja a de outro Estado; quando estamos perante factos cometidos em benefício de pessoas coletivas com sede em território português; quando estivermos perante factos praticados em Portugal, ainda que visem sistemas informáticos localizados fora desse território; e, finalmente, quando estivermos perante factos ilícitos, independentemente do lugar onde tenham ocorrido, desde que visem sistemas informáticos localizados em território português.

Se estivermos perante casos em que é simultaneamente competente Portugal ou outro país Estado membro da UE a lei vai permitir o recurso à intervenção de órgãos e mecanismos instituídos no seio europeu com vista à cooperação das autoridades e será através desta intervenção que se decidirá a concreta competência.

[157] *Vide* o art.º 19.º n.º2 da Lei n.º 109/2009, de 15 de setembro.

[158] VERDELHO, Pedro, *"A nova Lei do Cibercrime...", op. cit.*, p. 748.

5. Combate ao Cibercrime

Aqui chegados, e porque é gritante a constante evolução tecnológica e o consequente crescimento das práticas criminógenas, e em particular a cibercriminalidade, importa, pois, a contínua aposta contra esta flagelo, tendo em conta que a utilização do ciberespaço de forma livre, segura e confiável, na maioria das vezes, se traduz numa tarefa fatigante e de árdua consumação. Assim, perante esta nova área de difícil compreensão, que se reflete desde as burlas informáticas, ao *phishing*[159], *pharming*[160], furto de identidade, não esquecendo a falsificação de cartões bancários[161], resulta cristalina a necessidade de atualização e aprofundamento de novos entendimentos.

Na maioria dos casos, a investigação cibercriminal recorre a diligências de obtenção de prova em suporte digital que pressupõe a cooperação de entidade privadas, e.g., fornecedores de Internet, que por sua vez, são os únicos detentores de informação fulcral para a descoberta da verdade material[162]. Acresce ainda que, com base na utilização de redes telecomunicações, hoje, este tipo de investigações estão disseminadas pelos diversos OPC.

Para o efeito, a 7 de dezembro de 2011, foi criado por Despacho do Procurador-Geral da República o Gabinete Cibercrime[163], com sede na Procuradoria-Geral da República, coordenado pelo Procurador da República PEDRO VERDELHO. Destarte, este gabinete tem por objetivo a

---

[159] É uma fraude informática que se traduz na tentativa de obtenção de dados pessoais de diversos tipos (como passwords e dados financeiros) através da criação de uma identidade falsa por parte dos criminosos (como um banco ou uma instituição), que na maioria das vezes se reflete na criação de *e-mails* forjados, "pescando", desta forma, as suas vítimas. Neste sentido, GONÇALVES, Joana Margarida Andrade, *Pharming: Análise dogmático-penal, em especial enquanto forma de lesão do património*, Braga, Universidade do Minho – Escola de Direito, outubro 2015, pp. 19 e 20.

[160] "Conjunto de técnicas informáticas que manipulam a forma como os utilizadores localizam e se conectam aos domínios online de determinada organização, através da modificação do processo de resolução de nomes". No fundo, traduz-se na técnica informática através da qual o usuário da rede web ao digitar o nome de um website infetado é automaticamente redirecionado para um outro website. Cfr. GONÇALVES, Joana Margarida Andrade, *op. cit.*, p. 30.

[161] A este propósito, Relatório da Atividade setembro 2015 – dezembro 2016, Gabinete Cibercrime, p. 8, disponível em http://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/relatorio_anual_gabinete_cibercrime2015_02-03-2017.pdf [Consultado em 14.05.2017].

[162] *Vide* http://cibercrime.ministeriopublico.pt/pagina/o-que-fazemos-0 [Consultado em 14.05.2017].

[163] *Vide* http://cibercrime.ministeriopublico.pt/pagina/quem-somos [Consultado em 14.05.2017].

coordenação interna desta área criminal que se consubstancia na formação específica e sensibilização dos magistrados para esta celeuma, na interação com o setor privado através do estabelecimento de canais de comunicação com os fornecedores de serviço de acesso às telecomunicações, na interação com os OPC, bem como a padronização de procedimentos e promoção de boas práticas processuais com vista à cooperação na investigação criminal, em tempo útil e eficaz.

É neste âmbito que o Gabinete Cibercrime tem intervindo com o objetivo de tornar mais expedita a ação nesta área, tendo celebrado vários protocolos e bases de entendimento com diversos operadores de telecomunicações nacionais e internacionais[164], bem como a promoção de relacionamento com os OPC, no âmbito de diligências de inquérito, uma vez que os atuais fenómenos criminógenos exigem cada vez mais abordagens particulares. Ainda com vista ao combate do cibercrime, no âmbito interno, a ação do Gabinete Cibercrime prende-se também com os constantes planos de ação[165] que visam determinar minuciosamente as ações a estabelecer.

Não obstante todos os esforços de divulgação e sensibilização relacionados com a cibersegurança, bem como a criação de unidades nacionais competentes no combate ao cibercrime, como por exemplo, a Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica[166] da PJ, decorre de forma patente que a atual sociedade da informação ainda detém um longo caminho a percorrer no combate à criminalidade informática...

[164] *Vide* http://cibercrime.ministeriopublico.pt/sites/default/files/protocolo_comunicacoes.pdf [Consultado em 14.05.2017].

[165] *Vide* http://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/plano_acao_cibercrime_2015-2016.pdf [Consultado em 14.05.2017].

[166] Após alguns avanços e recuos com a criação da Unidade Nacional de Combate à Criminalidade Informática, em novembro de 2016, foi publicado em Diário da República uma moderna e adequada estrutura orgânica da PJ, i.e., a Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica. Com uma estrutura inspirada nos modelos adotados pela Europol, esta unidade foca-se não só no abuso sexual de crianças através da rede web, como os crimes de acesso ilegítimo, burlas informáticas, fraude com os cartões e outros meios de pagamento eletrónico e virtuais, entre outros... *Vide* https://www.rtp.pt/noticias/pais/unidade-de-combate-ao-cibercrime-e-criminalidade-tecnologica-da-pj-entra-em-funcionamento_n965660 e https://www.policiajudiciaria.pt/PortalWeb/page/%7BEC96A2D3-BA0F-4F51-9A3A-5BA3D222FE8B%7D [Consultado em 14.05.2017].

CAPÍTULO III

OS SERVIÇOS DE CORREIO ELETRÓNICO E DE MENSAGENS CURTAS

Após uma breve, mas não por isso menos importante, passagem pelo fenómeno do cibercrime, cumpre agora, e para que nos possamos aproximar da questão essencial decidenda do presente ensaio, fazer uma análise dos serviços de correio eletrónico e do serviço de mensagens curtas, vulgo, *SMS*.

Naturalmente que, tendo este objetivo, não fará sentido enveredarmos por uma abordagem extremamente rigorosa e excessivamente técnica destes serviços comunicacionais, todavia, tendo em vista o resultado final da presente dissertação e a diversidade estrutural e funcional no seio das telecomunicações, resulta cristalina a imprescindibilidade de análise, embora em traços necessariamente largos, das finalidades e problemáticas dos mesmos. É, por isso, nesses aspetos que nos iremos debruçar de seguida.

1. Dos "sinais de fumo" às telecomunicações, o que é que mudou?

O ato de comunicar, caracterizado como "(...) um fenómeno relacional de transmissão de informações (...)"[167], sempre foi uma necessidade e uma particularidade biológica básica do ser humano[168] que, tal como todas as características do mesmo, tem vindo a evoluir ao longo dos séculos. Se nos primórdios da humanidade a comunicação entre seres humanos não passava dos "grunhidos" semelhantes aos dos animais não racionais, o certo é que o ser humano foi evoluindo e ao longo dos anos assistimos à descoberta da comunicação oral, gestual, e até mesmo da escrita que, no fundo, pressupõe a emissão e exteriorização de uma mensagem,

[167] Cfr. OUBIÑA, Ana Mercedes da Silva Claro, "*As telecomunicações, a vida privada e o direito penal",* Direito Penal Hoje - Novos desafios e novas respostas, Organiz. MANUEL DA COSTA ANDRADE e RITA CASTANHEIRA NEVES, Coimbra, Coimbra Editora, 2009 p. 11.

[168] A este propósito, GONÇALVES, Pedro, *Direito das Telecomunicações*, Coimbra, Almedina, 1999, p. 9.

existindo, hoje, um número incontável de meios de comunicação que permitem o estabelecimento de relações comunicacionais entre interlocutores.

Se, por um lado, a fala é considerada a expressão superior de uma relação comunicacional, tendo em conta que este é o meio através do qual é possível a transmissão, num curto espaço de tempo, de uma quantidade de fluxo informacional, certa e precisa, que outras formas comunicacionais se mostram incapazes de realizar[169]; por outro lado, a palavra escrita (e consequente palavra virtual) veio permitir que este mesmo fluxo informacional permanecesse estável, em qualquer suporte físico (e/ou digital), sendo possível não só a sua cristalização, como ainda a distanciação com o seu próprio autor[170].

Não obstante, o certo é que o caminho trilhado desde os míticos "sinais de fumo" até às atuais *SMS* e correio eletrónico não foi uma tarefa fácil e célere, havendo séculos de história e de inovações que sempre tentaram colmatar aquele que é o busílis da questão no que concerne à comunicação, i.e., a necessidade e dependência da proximidade física, tanto em termos de espaço como de sincronismo temporal, entre o emissor e o recetor da comunicação. Se nos primórdios da nossa história a dependência da comunicação pessoal entre o emissor e o recetor era absolutamente incomportável, escusado será dizer que numa sociedade moderna, cada vez mais cosmopolita e global, mantém-se ainda acesa a chama dessa imprescindibilidade.

A premente necessidade de comunicação aliada ao desejo de obter meios ou sistemas que vençam a distância e a necessidade de disponibilidade síncrona (i.e., a necessidade de emissor e recetor estarem disponíveis para a comunicação no mesmo instante de tempo), bem como a urgência de obtenção de resposta em tempo quase real, conjugados com o sucesso das NTIC, conduziu ao inevitável incremento das comunicações, ou seja, à invenção das telecomunicações e à subsequente criação de redes ou sistemas de telecomunicações à distância, conhecidos como o novo motor comunicacional que afasta por completo todos os problemas relacionados com o distanciamento físico e temporal entre os interlocutores. No lapidar dizer de PEDRO GONÇALVES, a telecomunicação é "(...) um meio de transmissão ou de transporte de informações, representadas por sons, sinais escritos (dados) ou imagens (...)"[171]

---

[169] Neste mesmíssimo sentido, COSTA, José de Faria, *"As telecomunicações e a Privacidade: O olhar (in)discreto de um penalista",* As Telecomunicações e o Direito na Sociedade da Informação, Faculdade de Direito da Universidade de Coimbra, Instituto Jurídico da Comunicação, 1999, pp. 52 e 53.

[170] Sobre esta temática, COSTA, José de Faria, *"As telecomunicações e a Privacidade...", op. cit.,* pp. 54 – 56.

[171] Cfr. GONÇALVES, Pedro, *Idem*, *ibidem*.

que visa a satisfação básica de uma necessidade do ser humano do séc. XXI, fazendo uso dos meios ou sistemas técnicos, caracteriza-se por ser o elo de ligação pelo qual corre o fluxo informacional permitindo o próprio ato de comunicação[172].

Ora, é através do apoio em meios técnicos, redes ou sistemas telecomunicacionais físicos e/ou incorpóreos (desde os fios, cabos, sistemas óticos, rádios ou satélites) que as telecomunicações asseguram a comunicação entre as pessoas. É através destes meios que o obstáculo do distanciamento físico, no que se refere ao espaço e tempo, entre os interlocutores deixa de ser uma perturbação à troca de informações e consequente impedimento para as relações interpessoais dotadas de características como a individualidade, privacidade, reciprocidade e celeridade.

Ora, é com base na necessidade de privacidade das comunicações eletrónicas que a Comissão Europeia[173] tomou a liberdade de propor medidas com vista à criação de novas possibilidades de processamento de dados de comunicação e reforço na confiança e segurança no mercado único digital, apresentando regras para as comunicações eletrónicas com os novos padrões de classe mundial do Regulamento Geral de Proteção de Dados da UE. No fundo, a Comissão Europeia veio propor novas regras de privacidade aquando do processamento de dados pessoais por parte das instituições e órgãos da UE, bem como definir uma abordagem estratégica para as questões relativas às transferências internacionais de dados pessoais.

[172] Neste mesmíssimo sentido, GONÇALVES, Pedro, *op. cit.,* p. 133.

[173] Com as propostas apresentadas, que vão desde a aplicação do novo Regulamento Geral de Proteção de Dados aos fornecedores de serviços de comunicações eletrónicas, como *WhatsApp* ou *Facebook Messenger*, à aplicação de regras de confidencialidade, entre outros, a Comissão Europeia pretende proporcionar aos cidadãos e às empresas um completo quadro legal relativo à privacidade e proteção de dados na Europa. Mais informações podem ser encontradas aqui: *European Commission – Press release – Commission proposes high level of privacy rules for all electronic communications and updates data protection rules for EU institutions*, January 2017, disponível em http://europa.eu/rapid/press-release_IP-17-16_en.htm [Consultado em 10.01.2017].

2. O Serviço de Correio Eletrónico

Não obstante todos os evidentes esforços, escusado será dizer que o direito e a informática apresentam sempre uma enorme dificuldade em se sintonizarem. Se, por um lado, o direito quer-se "(...) estável, rigoroso e ponderado (...)"[174], por outro lado, a informática, caracteriza-se essencialmente pelo seu rigor e lógica, mas também pela sua constante mudança e evolução. Nesta sequência, a Internet, desde os seus primórdios, enquanto espaço de comunicação, veio a reclamar a liberdade e firmar-se como um espaço antijurídico pulverizado por um sistema capaz de se autoreformular, em alguns milissegundos, firmada no constante progresso científico, no qual, desde sempre, se impôs a necessidade de encontrar a estabilidade entre a liberdade e regulação por parte das diversas áreas do direito[175].

Ora, é através da Internet que um dos principais meios de comunicação da sociedade atual, i.e., o *e-mail*[176], também conhecido como serviço de correio eletrónico, é sobejamente utilizado. De acordo com a definição dada pelo legislador europeu, nos termos do art.º 2.º al. h) da Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, o "correio eletrónico é qualquer mensagem textual, vocal, sonora ou gráfica enviada através de uma rede pública de comunicações que pode ser armazenada na rede ou no equipamento terminal do destinatário até o destinatário a recolher"[177]. Contudo, para cabal compreensão, antes de delinearmos pormenorizadamente este serviço de comunicação, importa fazer uma breve resenha história.

Como bem sabemos, na sequência do desenvolvimento da comunicação escrita surgiram os pombos correio, os mensageiros e, numa realidade mais próxima, os serviços de correio postal que, desde a sua criação, se caracterizou pela sua constante evolução aleada aos seus postos de receção de correspondência, meios diversificados de distribuição e outros serviços. Sucede que, nos finais dos anos 60 do século passado, surgiram os computadores e desde logo a comunicação à distância, mais rápida, segura e sofisticada passou a ser uma real aposta e também objeto de investigação pelos principais programadores informáticos. *À*

---

[174] Cfr. MARTINS, António Gomes Lourenço / MARQUES, J. A. Garcia / DIAS, Pedro Simões, *op. cit.*, p. 91.

[175] Veja-se, LEITÃO, Adelaide Menezes, *"Metatags e Correio Electrónico entre os Novos Problemas do Direito da Internet",* Direito da Sociedade da Informação – Volume IV, APDI – Associação Portuguesa de Direito Intelectual, Coimbra, Coimbra Editora, 2003, pp. 405 e 406.

[176] Embora a origem da palavra *e-mail* esteja associado a "*eletronic mail*", em português correio eletrónico, desconhece-se a origem concreta desse termo. Contudo, dúvidas não subsistem que deriva do verbo "*to mai"l*, que significa enviar.

[177] Disponível para consulta em https://www.anacom.pt/render.jsp?contentId=964154 [Consultado em 29.06.2017].

posteriori, mais concretamente no ano de 1971, foi pelas mãos de RAY TOMLINSON e através da ARPANET[178] que foi enviado o primeiro *e-mail* da história da humanidade, antes sequer da criação da Internet como hoje a conhecemos.

Poucos anos depois, a partir das várias experiências informáticas, foi aprimorado o modo de envio das mensagens, nomeadamente através da criação de um conjunto de procedimentos a respeitar na emissão/receção de mensagens, sendo possível a transmissão de mensagens eletrónicas[179]. O certo é que o advento das novas tecnologias tem sido tão abismal que hoje o acesso ao *e-mail* já não é unicamente feito através de um computador, uma vez que os *smartphones*, *tablets* e outros dispositivos móveis já detêm este tipo de configurações. Portanto, podemos afirmar que o correio eletrónico veio revolucionar as formas de comunicar, traduzindo-se numa maior aceleração do envio de mensagens (a par de uma diminuição dos custos inerentes às mesmas), sendo importante afirmar que com esta desmedida evolução tecnológica tudo o que poderia não passar de um sonho e/ou imaginação faz hoje parte de uma realidade bem concreta. Ao contrário do correio postal, o correio eletrónico é rápido, barato, autónomo e fácil de distribuir, não dependendo da ação direta de outros agentes e dos seus horários laborais, uma vez que pode ser distribuído 24 sobre 24 horas.

Aqui chegados e antes de pormenorizarmos este serviço informático, denominado de correio eletrónico, importa fazer um breve reparo. Se atentarmos à letra da legislação nacional não somos capazes de designar exatamente o serviço de correio eletrónico. Ora, tal apenas se poderá dever ao facto de o legislador nacional, conhecedor da mutabilidade informática (que nunca é passível de concordância técnica), não se querer comprometer com uma definição que, num curto espaço de tempo, poderá desvanecer.

Assim, atendendo à necessidade de caracterizar de uma melhor forma este serviço, muitos foram aos autores que, dando largas aos seus conhecimentos, se aventuraram na axiologia informática. Deste modo, CASABONA[180] veio definir o correio eletrónico como uma modalidade de comunicação pessoal composta por ficheiros de texto, voz ou imagem,

---

[178] Acrónimo de *Advanced Research Projects Agency Network*, surgiu no Departamento de Defesa dos EUA na década de 60, ficou conhecida como a "mãe da Internet de hoje" tendo em conta que foi a primeira rede operacional de computadores que tinha como principal objetivo a comunicação de dados em alta velocidade para fins militares. Mais informações sobre esta rede operacional poderão ser obtidas no *website* http://www.history.com/topics/inventions/invention-of-the-internet [Consultado em 02.07.2017].

[179] Neste sentido, RAMOS, Armando Dias, *op. cit.*, p. 23.

[180] Neste exato sentido, CASABONA, Carlos María Romeo, *"La protección penal de los mensajes de correo electrónico y de otras comunicaciones de carácter personal a través de Internet",* Derecho y Conocimiento, Vol. 2, 2002, p. 129.

usufruindo das redes telemáticas como a tecnologia de transmissão e receção dos sistemas informáticos. Por outra banda, PEDRO VERDELHO[181] descreve o correio eletrónico como uma comunicação em rede entre dois aparelhos informáticos, um emissor e um recetor, sendo que quando a mensagem chega ao dispositivo deste último pode ficar ali guardada sob forma de ficheiro informático. Já ARMANDO DIAS RAMOS apresenta o serviço *e-mail* como "(...) um programa informático que permite a comunicação instantânea, de modo diferido, entre quem a envia e quem a recebe, através das redes de informação e comunicação, independentemente do local onde se encontrem, sem a necessidade deste se encontrar instalado no computador"[182].

Independentemente de todas as designações apresentadas pelos diversos autores, podemos afirmar com clareza que, para que o serviço de correio eletrónico seja considerado um verdadeiro serviço comunicacional digital, é necessário que detenha as seguintes especificidades[183]:

I) eletrónico – uma vez que utiliza meios eletrónicos de gestão e de transporte;

II) assíncrono – tendo em conta que não é simultânea e não existe qualquer necessidade de sincronia entre e emissão e receção de mensagens, ou seja, cujos utilizadores enviam e recebem mensagens apenas quando lhes convier, sem agendamento prévio;

III) ubiquidade – atendendo ao facto que é permitido o seu acesso em qualquer local;

IV) digital – sendo apenas empregue informação digitalizada;

V) informática – relaciona-se com as tecnologias de informação.

[181] A este propósito, VERDELHO, Pedro, *"Técnica no Novo C.P.P...", op. cit.*, p. 164.

[182] Cfr. RAMOS, Armando Dias, *op. cit.,* p. 25.

[183] RAMOS, Armando Dias, *Idem, ibidem.*

2.1. A arquitetura e entidades intervenientes no serviço de Correio Eletrónico

Para uma melhor compreensão do nosso estudo, importante parece-nos agora caracterizar o conteúdo e os componentes do serviço de correio eletrónico. Tal como já foi previamente mencionado, não é novidade nenhuma que um *e-mail* pode conter uma mensagem de texto em vários formatos, imagens, sons e até *hiperlinks*[184]. Por outro lado, o "coração" do *e-mail* é composto por três grandes componentes, nomeadamente:

- *User agents* (agente de utilizador);
- *Mail servers* (servidores de *e-mail*); e
- *SMTP – Simple Mail Transfer Protocol* (Protocolo de transferência de correio simples)[185].

Para uma melhor descrição das funções de cada componente, nada melhor do que imaginarmos a situação em que o "A" (remetente) envia um *e-mail* para o "B" (destinatário). Nesta banal situação, os agentes de utilizador permitem que o emissor/recetor leia e responda aos *e-mails* recebidos e guarde os *e-mails* escritos, sendo exemplos dos agentes de utilizador o *Microsoft Outlook* ou o *Mozilla Thunderbird*.

Quando o "A" termina a composição da sua mensagem o seu agente de utilizador envia a mensagem para o seu servidor de saída de *e-mail*, onde a mensagem fica guardada na caixa de mensagens de saída do servidor de correio eletrónico do remetente[186]. Posteriormente, quando o "B" quiser ler a mensagem que o remetente lhe enviou, o seu próprio agente de utilizador vai recuperar a tal mensagem na caixa de entrada do seu próprio servidor de *e-mail*. Os servidores de correio constituem, portanto, o núcleo da infraestrutura de *e-mail*.

Cada destinatário de *e-mail* tem uma caixa de correio eletrónico localizada num servidor de *e-mail* e, regra geral, é na caixa de correio que se vão gerir e se irão manter (até serem

[184] É uma ligação/atalho dentro de um documento que redireciona o utilizador para outro documento. Mais informações poderão ser obtidas no *website* https://www.computerhope.com/jargon/h/hyperlin.htm [Consultado em 02.07.2017].

[185] Nesta senda, KUROSE, James F., ROSS, Keith W., *Computer networking: a top-down approach*, 6th ed., Pearson Education, Inc., 2013, pp. 119 e 120.

[186] Este servidor de correio eletrónico procurará encaminhar a mensagem para o servidor de correio eletrónico do destinatário, desta forma, a mensagem poderá passar por servidores intermédios até ser depositada e armazenada no servidor de *e-mail* destinatário, na sua caixa de correio.

eliminadas) as mensagens enviadas e recebidas. O certo é que uma mensagem inicia a sua jornada no agente do utilizador do remetente, viaja para o servidor de *e-mail* do remetente, segue caminho para o servidor de *e-mail* do destinatário e, por fim, é depositado na caixa de correio desse mesmo destinatário. Não obstante o trajeto previamente mencionado, devemos atender ao facto que podem existir falhas técnicas tanto por parte do servidor de *e-mail* do remetente, como por parte de algum servidor intermédio ou ainda através do servidor de *e-mail* do destinatário. Se no exemplo *supra* exposto o servidor do "A" não conseguir entregar a mensagem ao servidor do "B" (ou a algum servidor intermédio), então o servidor do remetente (ou algum servidor intermédio) manterá a mensagem numa "fila de espera", tentando transferi-la mais tarde. Regra geral, tenta fazê-lo numa frequência de aproximadamente trinta minutos e se todas as tentativas forem mal sucedidas durante um período de tempo (regra geral 72 horas), então o servidor de *e-mail* notificará o remetente desse mesmo erro[187].

Importante parece-nos ainda referir que no percurso de uma mensagem de correio eletrónico, entre o servidor do remetente e o servidor do destinatário, os dados são transferidos de forma fragmentada, sendo unicamente unificados quando chegam ao destino, tornando-se assim acessíveis ao recetor[188].

Por outra banda, o *SMTP* caracteriza-se por ser o protocolo *standard* utilizado na entrega e receção de mensagens de correio eletrónico que tem por objetivo o envio de *e-mails* do agente de utilizador para o servidor de *e-mail* e, posteriormente, do servidor do remetente para o servidor do destinatário[189]. Num percurso normal de um *e-mail*, o agente de utilizador do remetente não "dialoga" diretamente com o servidor de *e-mail* do destinatário, tendo em conta que essa tarefa se encontra incumbida ao *SMTP*.

Tal como acontece com a maioria dos protocolos de camada de aplicação, o *SMTP* tem dois lados: um "lado do cliente" que é executado no servidor de *e-mail* do remetente, e um "lado do servidor" que é executado no servidor de *e-mail* do destinatário, sendo através do *SMTP* que será feita a "ponte comunicacional"[190]. Mesmo quando os dois servidores de correio estão localizados em extremidades opostas do mundo, o *SMTP* não utilizará servidores de correio intermediários para o envio de mensagens.

---

[187] KUROSE, James F., ROSS, Keith W., *op. cit.,* p. 121.

[188] Neste mesmíssimo sentido, RAMOS, Armando Dias, *op. cit.*, pp. 27 – 29.

[189] Para mais informações: https://www.hmailserver.com/documentation/v4.3/?page=whatis_pop3imapsmtp [Consultado em 08.07.2017].

[190] A este propósito, KUROSE, James F., ROSS, Keith W., *Idem, ibidem.*

Por fim, importa ainda acrescentar que o protocolo *SMTP* pode ser completado com mais um (ou dois) protocolos, nomeadamente o *POP3*[191] e o *IMAP*[192], que são os protocolos usados pelos agentes de utilizador para obter ou fazer o acesso às mensagens de correio eletrónico.

2.2. Fraudes informáticas e crimes praticados através do serviço de Correio Eletrónico

Tendo por referência as principais características deste meio de comunicação, como a sua celeridade e/ou baixo custo, escusado seria dizer que o *e-mail* é considerado um ótimo meio para a produção de ataques informáticos ou, até mesmo, um alvo perfeito para ilícitos. Atendendo à banalização do serviço de *e-mail* e face à quantidade de mensagens de cariz duvidoso que circulam hoje na rede *web*, infelizmente, todos os utilizadores são obrigados a lidar diariamente com diversos contratempos que vão desde o *SPAM*[193] ao perigoso *malware* e que, num curto espaço de tempo, são capazes de infetar milhões de utilizadores e até mesmo paralisar nações.

Logicamente que quando um computador está infetado, os criminosos poderão ser capazes de aceder, remotamente, a tudo ou a quase tudo o que ali se encontre, podendo

---

[191] O *POP3* (*Post Office Protocol*) é aquele protocolo específico que tem como objetivo o download das mensagens de correio eletrónico, exatamente como são, sem quaisquer modificações, através do servidor de *e-mail*. Assim, através deste protocolo será possível a consulta de *e-mails* em modo *offline*. *Vide* https://www.webhs.pt/dicas/smtp-imap-pop3-explicacao/ [Consultado em 08.07.2017].

[192] O *IMAP* (*Internet Message Access Protocol*) é aquele protocolo que permite o acesso e consequente manipulação de *e-mails* num servidor. Detentor de mais recursos do que o POP 3, o IMAP foi criado para permitir que os usuários mantenham e armazenem as suas mensagens de correio eletrónico no servidor. *Vide* https://pplware.sapo.pt/internet/pop-ou-imap-qual-o-melhor/ [Consultado em 08.07.2017].

[193] O *SPAM* (também denominado de *Sending and Posting Advertisement in Mass*) é aquele tipo de mensagens enviadas em massa, de forma automática, e que, por vezes, transportam material que pode infetar irremediavelmente os terminais de destino, i.e., *PC*, telemóveis, *tablets*, entre outros, através da utilização de servidores denominados de *botnets*. Para saber mais sobre este assunto: https://www.anacom.pt/render.jsp?categoryId=346972 [Consultado em 08.07.2017]. Na perspetiva do utilizador o *SPAM* pode tornar a utilização do correio eletrónico insuportável, atendendo ao tempo perdido ao fazer a triagem do correio eletrónico que é suposto ser lido, do que não é, sem falar na possibilidade de propagação de *malware*. O problema é que uma legislação que viesse proibir o *SPAM*, pura e simplesmente seria um atentado às liberdades de expressão e de informação, art.º 37.º CRP e às liberdades de criação cultural, art.º 42.º, entre outros. Para mais desenvolvimentos sugere-se a leitura de LEITÃO, Luís Menezes, *"A Distribuição de Mensagens de Correio Eletrónico Indesejadas (SPAM)"*, Direito da Sociedade da Informação – Volume IV, APDI – Associação Portuguesa de Direito Intelectual, Coimbra, Coimbra Editora, 2003, pp. 195 – 212.

"espiar" todas as utilizações do computador e ainda praticar ilícitos, em nome do utilizador, sem que este último se aperceba da intrusão. Na sequência destas fragilidades e com vista a não corrermos riscos absolutamente evitáveis, é normal que hoje um bom agente de utilizador consiga remeter automaticamente para outras pastas, que não a "caixa de entrada" correio eletrónico, as mensagens "filtradas" como "perigosas", alertando o utilizador para a possibilidade de apagar este tipo de mensagens sem sequer as abrir[194].

Apesar de em Portugal não ser comum este tipo de insólitos, recorrentes no universo dos filmes e séries televisivas, a verdade é que já se encontram disponíveis várias decisões de tribunais superiores reveladoras dos ilícitos que podem ser cometidos com recurso ao serviço de *e-mail*. A título de exemplo, em 2016, o Tribunal da Relação de Coimbra, no Acórdão n.º 902/13.4TBCNT.C1[195], refletiu sobre o perigo originado através da atuação ilícita denominada de *phishing* efetuado através do envio de mensagens de correio eletrónico (*spamming* de *e-mails*) com vista à obtenção de palavras-passe de serviços bancários, *PINS* ou outras informações privadas dos destinatários. Já numa perspetiva menos futurista e nada surpreendente, em 2014, foi constatado pelo Tribunal da Relação do Porto[196] a facilidade com que uma pessoa consegue introduzir-se na conta de correio eletrónico de um terceiro com vista à divulgação e consequente devassa de dados e informações pessoais ou privadas ou vedadas do proprietário dessa conta de *e-mail*.

---

[194] RAMOS, Armando Dias, *op. cit.*, pp. 57 – 59.

[195] Acórdão do Tribunal da Relação de Coimbra de 02-02-2016, com o seguinte sumário: "*Não se tendo provado que o cliente forneceu a terceiros (ao aceder a página ilícita) as chaves de acesso ao serviço de home banking nem que, ao navegar na inter-net, permitiu que outrem tenha capturado as credenciais de acesso e validação, recai sobre o banco a responsabilidade pela movimentação fraudulenta da sua conta bancária, através da internet (Serviços Homebanking).*". Disponível em http://www.dgsi.pt/jtrc.nsf/c3fb530030ea1c61802568d9005cd5bb/aba8f7cea02531c180257f4f003e6e54?OpenDocument [Consultado em 25.07.2017].

[196] Acórdão do Tribunal da Relação do Porto de 08-01-2014, já previamente mencionado, com o seguinte sumário: "*A alínea d) do n.º 2 do art.º 120º do CPP abrange a omissão de atos ou diligências processuais na fase de julgamento e de recurso, que se reputem essenciais à descoberta da verdade. O juízo sobre a essencialidade ou indispensabilidade da diligência de prova cabe ao tribunal e deve basear-se em critérios objetivos, independentes das convicções pessoais dos intervenientes processuais. A sentença é nula quando a fundamentação da convicção for insuficiente para efetuar uma reconstituição do iter que conduziu a considerar cada facto provado ou não provado. O crime de acesso ilegítimo, previsto no art.º 6º da Lei n.º 109/2009, de 15/9, (Lei do Cibercrime), estruturalmente acolhe o crime anterior, previsto no art.º 7º da Lei 109/91, de 17/8, com alterações decorrentes dos compromissos internacionais que Portugal assumiu e, em particular, da Convenção sobre Cibercrime do Conselho da Europa. A factualidade incriminada é exatamente a mesma que era antes, não se exigindo, agora, qualquer intenção específica, por exemplo, a de causar prejuízo ou a de obter qualquer benefício ilegítimo pois que apenas se exige o dolo genérico. O bem jurídico protegido é a segurança do sistema informático. O crime de acesso ilegítimo é praticado por quem actue de forma não autorizada, concretizando-se por qualquer modo normalmente idóneo de aceder a um sistema ou rede informáticos. O crime de devassa por meio de informática, previsto no art.º 193º do C. Penal, decorre do art.º 35º, n.º 3, da CRP, e visa proteger a reserva da vida privada contra possíveis atos de discriminação, que a utilização de meios informáticos torna exponencialmente perigosos*".

Por isto, convém manter a convicção que as máquinas e consequentemente o correio eletrónico são falíveis e podem ser uma porta aberta para a prática de inúmeros ilícitos. Basta pensarmos que com a possibilidade de envio de anexos, com as respetivas mensagens, o correio eletrónico torna-se no motor ideal para a prática de vários crimes, que vão desde a sabotagem informática, danos relativos a programas ou outros danos informáticos, divulgação de pornografia de menores, não esquecendo as banais injúrias ou difamações.

Com efeito, existem já hoje soluções tecnológicas como, por exemplo, as Infraestruturas de Chaves Públicas (PKI), que permitem uma maior segurança quer na determinação da autenticação do emissor/destinatário da mensagem de correio eletrónico, quer na verificação da integridade, e mesmo inviolabilidade, do respetivo conteúdo. Não obstante, o certo é que estas soluções mais robustas em termos de segurança são ainda pouco utilizadas, atendendo à sua complexidade, à (ainda) baixa usabilidade e ainda aos custos associados. No entanto, urge que a solução passe pela concertação de esforços entre todas as partes envolvidas (utilizadores, operadores de rede, fornecedores de serviços e legislador), sob pena de constantes violações e ameaças de segurança.

3. O Serviço de Mensagens Curtas

Fruto da evolução tecnológica e do consequente desenvolvimento do mercado das novas tecnologias, nasceu aquele que é considerado um dos principais meios de comunicação da sociedade da informação, i.e., as mensagens curtas, também denominadas de *SMS* (*Short Message Service*). Desenvolvido na década de oitenta e atendendo à facilidade, rapidez e preço deste tipo de serviço, dúvidas não podem subsistir quanto à sua verdadeira necessidade, especulando-se o envio diário de centenas de milhares de mensagens curtas[197].

[197] Em 2013, a União Internacional de Telecomunicações estimou que cerca de 85% da população mundial tivesse acesso a este serviço, sendo hoje o serviço móvel mais popular, medido por um grande volume de transmissão e participações de mercado. Veja-se, ACKER, Amelia, *"The Short Message Service: Standards, infrastructure and innovation",* Telematics and Informatics, Volume 31, Issue 4, Pittsburgh, University of Pittsburgh, January 2014, p. 559.

O serviço de mensagens curtas, para além de poder ser utilizado a qualquer hora e em qualquer lugar (dependendo essencialmente da cobertura de rede celular), é também usado no âmbito pessoal e profissional do seu utilizador, sendo inclusivamente utilizado por todo o tipo de indústrias (governamentais, retalho, publicitárias, redes sociais, companhias aéreas...), bem como por serviços alimentados por *SMS* que possibilitam o alcance e/ou autenticação dos seus clientes por via de mensagens, como por exemplo, os serviços de alertas, notícias, *homebanking*[198], entre tantos outros.

Recuando um pouco na história, é sabido que as *SMS* poderão encontrar a sua origem na radiotelegrafia de estação para estação do século XIX, uma vez que foi esta a primeira evolução do modo de transmissão de mensagens de texto marcando assim o início da comunicação verdadeiramente "móvel". A ideia da transmissão celular móvel foi criada nos EUA, na década de 40 do século passado, contudo foi só nos anos 60 que a ideia passou do papel para a prática[199]. Anos mais tarde, mais concretamente em 1970, a tecnologia de enviar e receber mensagens móveis tornou-se tecnicamente viável, no entanto, o certo é que as primeiras redes móveis ainda eram vistas como extensões de redes fixas, ou linhas fixas, em nada se assemelhando à atual arquitetura móvel.

O ano de 1982 ficou marcado pela conferência europeia de correio e telecomunicações, onde foi criado um grupo de trabalho, apelidado de "*Groupe Spécial Mobile*", responsável pelo futuro das comunicações móveis digitais, conhecido mais tarde por "*Global System for Mobile Communication – GSM*". Na senda do legado do "*Groupe Spécial Mobile*", o GSM ficou encarregue de desenvolver os sistemas digitais móveis, criando desta forma, um novo tipo de processo de padronização onde, pela primeira vez, os fabricantes de equipamentos privados e pesquisadores da indústria puderam moldar e influenciar o desenvolvimento de padrões de comunicação móvel, criando um novo modelo de parcerias público-privadas[200]. Já na década de 90 podemos assistir ao nascimento das tecnologias móveis de 2.ª geração[201], na primeira década

[198] TU, Guan-Hua, *et al., "New Security Threats Caused by IMS-based SMS Service in 4G LTE Networks"*, Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2016. p. 1118.

[199] Nesta senda, ACKER, Amelia, *op.cit*, p. 561.

[200] ACKER, Amelia, *op.cit*, p. 562.

[201] *Vide* https://pt.slideshare.net/brunoms18/apresentao-novas-tecnologias-e-a-internet [Consultado em 08.07.2017].

de 2000 assistimos ao surgimento das tecnologias de 3.ª e 4.ª geração[202] e o certo é que, na atualidade, já vamos caminhando a passos largos para a 5.ª geração[203].

Aquando do estabelecimento das primeiras redes móveis, uma grande parcela da indústria de telecomunicações na Europa e nos EUA previu que os serviços de dados com comutação de circuitos, como as chamadas de voz, seriam os aplicativos móveis mais importantes para os utilizadores, renegando para segundo plano as *SMS* que, inicialmente, eram vistas como um simples complemento sem grande potencial comercial, ficando atrás dos serviços *fax* que pareciam ser muito mais promissores.

Contudo, bem sabemos que a realidade vivida hoje é bem diferente da então especulada e, o certo é que, após muita evolução, os atuais serviços de comunicação em rede passaram a utilizar uma arquitetura móvel composta por torres e estações de base que permitem a transferência de informações que não dependem de um ponto pré-fixado para transmitir dados ou chamadas de voz, criando assim uma nova forma de comunicação e transmissão de dados sem fio[204], possibilitando, dessa forma, o constante envio e receção de *SMS*.

O serviço de mensagens curtas, como o próprio nome indica, é um dos principais serviços em redes móveis que se traduz na troca de mensagens curtas alfanuméricas (160 caracteres, o que equivale a aproximadamente 160 bytes) entre os seus utilizadores. Suportado por quase todo o tipo de comunicações móveis, este serviço é possibilitado por um conjunto de padrões, protocolos, *standards*, *design* e infraestruturas próprias de transmissão que, em grosso modo, têm vindo a desenvolver-se graças à sua constante procura. No âmbito das *SMS*, novos serviços têm vindo a ser introduzidos, como as mensagens de multimédia (*MMS – multimedia messaging service*[205]), com imagens ou outros conteúdos multimédia, o que tem vindo a estimular a inovação dos serviços prestados[206]. Contudo, não obstante a variedade de serviços que se encontram ao dispor do utilizador, o serviço de mensagens curtas continua a manter-se

---

[202] JEYA, R. e AMUTHA, Dr. B., *"Wireless Generations - a Survey"*, International Journal of Pure and Applied Mathematics, Volume 115, No. 6, Sofia: Academic Publications, 2017, p. 427.

[203] *Vide* http://www.3gpp.org/news-events/3gpp-news/1614-sa_5g [Consultado em 12.10.2017].

[204] Neste mesmíssimo sentido, ACKER, Amelia, *op.cit*, pp. 560 e 561.

[205] Também conhecido por serviço de mensagens multimédia, é o serviço de mensagens que possibilita a receção e envio de mensagens de texto com imagens, vídeo e/ou áudio. *Vide* https://www.infopedia.pt/dicionarios/siglas-abreviaturas/MMS [Consultado em 08.07.2017].

[206] A este propósito, Electronic Communications Committee Report 52, *Short Message Service (SMS) in fixed and mobile networks*, Gothenburg, July 2004, disponível em http://www.erodocdb.dk/Docs/doc98/official/pdf/ECCRep052.pdf [Consultado em 08.07.2017].

como um dos principais meios de comunicação atual e, segundo vários autores[207], todo sucesso das *SMS* decorre de dois principais fatores, nomeadamente:

1) não obstante os problemas que possam haver com a entrega de mensagens curtas, é sabido que, regra geral, toda e a qualquer *SMS* é entregue confidencial e integralmente ao seu destinatário[208];
2) o caráter da imprescindibilidade advém, principalmente, pelo facto de o serviço de *SMS* ser o meio mais conveniente para que os fornecedores de serviços atinjam bilhões de utilizadores móveis.

Em contraste com os modelos iniciais de mensagens armazenadas, como os *pagers*[209], o serviço de mensagens curtas revelou-se absolutamente capaz de não só receber, como armazenar e enviar mensagens para outros dispositivos móveis pessoais. O serviço de mensagens curtas abriu caminho para o real sucesso do mercado das telecomunicações móveis que, atualmente, encontra-se na 4ª geração, também denominada de *Long Term Evolution – LTE*, baseada numa arquitetura de rede plana *"all IP"*, com todos os serviços baseados na versão 6 do *Internet Protocol*, *IPv6*.

3.1. A arquitetura do serviço de mensagens curtas

O *LTE* foi introduzido na sequência das telecomunicações de terceira geração (globalmente conhecidas por 3G) e, hoje, é tido como o mais recente avanço tecnológico na área das telecomunicações[210], tendo sido idealizado para suportar apenas serviços com comutação de

[207] Neste mesmo sentido, TU, Guan-Hua, *et al, op. cit.*

[208] Note-se, no entanto, que não é um serviço absolutamente garantido, uma vez que a *SMS* poderá ser descartada se o terminal de destino estiver sem serviço (desligado ou fora do alcance) de rede durante um longo período de tempo.

[209] É um pequeno aparelho eletrónico e portátil, bastante aclamado nos anos 80 e 90 que, através de sinais sonoros ou luminosos, informa que alguém quer comunicar com o seu portador. Apesar de também existirem "*two-way pagers*" (são aqueles *pagers* que permitem a receção e envio de mensagens), os vulgarmente conhecidos são os "*one-way pagers*" (aqueles que só permitem a receção de mensagens). Para mais informações: http://searchmobilecomputing.techtarget.com/definition/pager [Consultado em 15.07.2017].

[210] Neste sentido, David Pernes, *et. al., Análise de Cobertura e Capacidade em Redes Móveis LTE de Quarta Geração (4G)*, Área Departamental de Engenharia de Eletrónica Telecomunicações e de Computadores (ADEETC), ISEL, Lisboa, Portugal, disponível em https://www.anacom.pt/streaming/DavidPernes_CongressoURSI2012.pdf?contentId=1148345&field=ATTACHED_FILE [Consultado em 16.07.2017].

pacotes, compatível com as redes *GSM* (*Global System for Mobile Communications*) e *HSPA (High Speed Packet Data Access)*. Ao contrário dos anteriores padrões de redes móveis, a tecnologia de rede utilizada no *LTE* caracteriza-se por ser mais simples e segura, traduzindo-se em respostas mais céleres e eficientes por parte dos destinatários das *SMS*, tendo em conta que possibilita a transmissão e receção de mensagens ao mesmo tempo. Ora, podemos considerar que esta nova geração de comunicações móveis, para além de oferecer um bom desempenho, segurança, diminuição do custo por *bit* transportado e uma grande velocidade de conexão, também trouxe consigo uma arquitetura bastante mais simples do que aquelas que estávamos habituados.

Assim, muito resumidamente, podemos afirmar que arquitetura de rede e elementos do *LTE* é composta por três partes interligadas[211]. Na sequência dos anteriores padrões de redes móveis, a primeira parte é o equipamento do utilizador que, por sua vez, contém dois elementos:

1) o primeiro componente é o aparelho móvel ou estação móvel (*Mobile station – MS*) do utilizador, ou seja, é aquilo a que todos nós apelidamos de telemóvel. Ora, como bem sabemos, o telemóvel é o equipamento através do qual podemos fazer e receber chamadas, mensagens/notificações, entre outros, cuja identidade é relevada através do cartão *SIM* que, por sua vez, vai permitir a troca de chamadas/mensagens através de uma rede móvel.
2) para além do cartão *SIM*, cada telemóvel será detentor de um *IMEI*[212] que é exclusivo para cada aparelho móvel.

Deste modo, quando os utilizadores enviam uma mensagem de texto dos seus dispositivos móveis, o aparelho vai transmitir a mensagem para a segunda parte da arquitetura de rede, i.e., a rede de acesso, também conhecido por *E-UTRAN* (*Evolved Terrestrial Radio Access*). A *E-UTRAN* é composta por *eNodeB* (*Evolved Node B*), que corresponde às estações de base dos anteriores padrões de redes móveis. Essencialmente, o *eNodeB* tem como principais funções a receção e envio de transmissões de rádio através do processamento de sinal digital da interface *LTE* e o controlo de operações de baixo nível de todos os telemóveis. Por sua vez, vai ser o *eNodeB* quem vai transmitir a mensagem curta para a terceira e última parte da arquitetura de rede do *LTE*, ou seja, o *EPC* (*Evolved Packet Core*).

---

[211] *Vide* https://www.tutorialspoint.com/lte/lte_network_architecture.htm [Consultado em 15.07.2017].

[212] *International Mobile Equipment Identity*, em português, "Identificação Internacional de Equipamento Móvel". *Vd* http://whatis.techtarget.com/definition/IMEI-International-Mobile-Equipment-Identity [Consultado em 15.07.2017].

A arquitetura de rede *EPC*, baseada no protocolo *IP*, vai permitir a integração com outras redes de comunicação como as redes *GSM* e *HSPA*, permitindo a conectividade com outras formas de acesso. Esta terceira parte da arquitetura de rede também é responsável pela gestão e processamento de pacotes de informações, evitando a perda de dados ou o sobre carregamento da rede[213].

De seguida, a mensagem curta irá percorrer o *Evolved Node B* do destinatário da mensagem curta chegando, finalmente, ao subsistema de estação móvel, ou seja, o telemóvel do recetor da mensagem.

3.2. Fraudes informáticas e crimes praticados através do serviço de mensagens curtas

Não obstante todas as evoluções no âmbito das telecomunicações, não nos podemos esquecer que as mensagens curtas são transferidas através de protocolos e canais legíveis para qualquer agente e que vivemos num período informativo de fácil acesso, não sendo necessário, graças à tecnologia de ponta existente, grandes conhecimentos tecnológicos para que haja lugar à prática de crimes informáticos. Crimes esses, tantas vezes promovidos através de uma simples *SMS*. Muito se tem trabalhado nesta área e muitos desenvolvimentos se têm feito, contudo o nó górdio vai sempre prender-se com as constantes inovações informáticas e permanentes ataques que, ainda que em menor escala, se têm verificado[214]. No fundo, salvo douto entendimento, isto é reflexo da falta de evolução dos mecanismos de segurança relacionados com as *SMS*, enquanto as evoluções tecnológicas acabam por ser uma constante.

A titulo de exemplo[215], podemos identificar casos em que o proprietário do telemóvel é vítima de *malware* que explora "silenciosamente" todo o conteúdo constante no telemóvel, situações em que é esgotado o saldo do aparelho, casos em que até são utilizadas

[213] *Vide* https://www.gta.ufrj.br/grad/09_1/versao-final/umts/lte.html [Consultado em 15.07.2017].

[214] A título de exemplo, podemos referir a prática de *Phishing*, i.e., o ato de enviar uma mensagem curta e/ou *e-mail*, alegando ser uma entidade (como uma instituição bancária), com o objetivo de fazer com que a vítima indefesa entregue voluntariamente as informações pretendidas, como por exemplo, o *username* e *password* ao criminoso. *Vide* https://pplware.sapo.pt/informacao/ataque-de-phishing-chega-via-sms-em-nome-do-seu-banco/ [Consultado em 18.07.2017].

[215] Neste mesmo sentido, TU, Guan-Hua, *et al, op. cit.*

funcionalidades do dispositivo móvel sem o consentimento do seu utilizador ou, até mesmo, casos de fraudes promovidas através do serviço de mensagens curtas[216].

É sabido que as *SMS* são uma parte fundamental nas comunicações móveis pessoais e profissionais e, tendo por base esta premente necessidade, acabam por se tornar o canal perfeito para a promoção de fraudes informáticas. Apesar de em 2014 a consultora *P1 Security* ter concluído que o nosso país era dos que apresentava um "risco médio" relativamente à proteção dos seus consumidores quanto às falhas de privacidade causadas por ataques informáticos[217], a verdade é que também existem decisões dos tribunais superiores que se debruçam sobre esta temática não sendo, de todo, aconselhável fechar os olhos a esta realidade.

Assim, em 2014, o Tribunal da Relação de Évora[218] pronunciou-se quanto às fraudes informáticas exercidas no âmbito das autorizações/autenticações promovidas através dos serviços de *SMS* e, nesta senda, veio concluir que sendo o *homebanking* uma plataforma prestada pelo banco ao cliente, compete à identidade bancária a segurança desse mesmo serviço da maneira a que o cliente não fique privado dos valores previamente depositados, competindo a este último observar todas as regras de segurança que lhe tenham sido recomendáveis e que são expectáveis, segundo o padrão de normalidade. Desta forma, o tribunal decidiu que todos os riscos e/ou falhas do sistema informático, bem como os ciber ataques que o sistema bancário pode ser alvo só podem correr por conta da entidade bancária. Ainda na perspetiva da autenticação/autorização promovida através do serviço de mensagens curtas, em 2013, o Tribunal da Relação de Guimarães[219] também se pronunciou quanto à

---

[216] Recentemente, foi notícia a fraude através da qual foram enviadas várias *SMS* para alguns utentes do Hospital Pedro Hispano e todos os centros de saúde de Matosinhos com vista à cobrança de taxas moderadoras. Para mais informações *vd* http://observador.pt/2016/01/22/burla-taxas-moderadores-atraves-sms/ [Consultado em 18.07.2017].

[217] Para mais informações *vide* http://www.dn.pt/sociedade/interior/ss7-a-porta-dos-hackers-para-controlar-a-nossa-vida-no-telemovel-5136137.html [Consultado em 18.07.2017].

[218] Acórdão do Tribunal da Relação de Évora de 22-05-2014, com o seguinte sumário: "*O homebanking sendo um serviço prestado ao cliente, compete à entidade bancária diligenciar pela segurança desse serviço, de modo a que o seu utilizador não fique privado dos valores depositados pelo abusivo acesso a terceiros, sem a sua autorização ou consentimento, competindo ao cliente observar as regras de segurança que lhe tenham sido comunicadas e aquelas que, segundo um padrão de normalidade, o comum utilizador sabe que devem ser observadas, designadamente a não divulgação de chaves de acesso e números de telemóveis associados à utilização por SMS. Os riscos da falha do sistema informático utilizado, bem como dos ataques cibernautas ao mesmo, têm de correr por conta da entidade bancária, por a tal conduzir o disposto no artigo 796º, nº1 do C. Civil, não se podendo imputar a culpa ao cliente/utilizado".* Disponível em http://www.dgsi.pt/jtre.nsf/-/2FF1D3B3BC6D929080257DF100383C04 [Consultado em 18.07.2017].

[219] Acórdão do Tribunal da Relação de Guimarães de 30-05-2013, com o seguinte sumário: *O contrato de "homebanking" estabelecido entre o banco e o cliente consiste numa simplificação de processos e operações disponibilizados, a este último, possibilitando-lhe um acesso mais*

responsabilidade das entidades bancárias nos casos de ataques informáticos às plataformas *homebanking*.

Já noutra perspetiva, é sabido que o serviço de mensagens curtas também acaba por ser um meio bastante convidativo para a prática de outro tipo de ilícitos como por exemplo os crimes de difamação, injúrias, ou até mesmo ameaças. Exemplos disso mesmo podemos verificar no acórdão do Tribunal da Relação de Lisboa[220] no qual foram enviadas mensagens curtas – injuriosas e ameaçadoras – do telemóvel do arguido para o telemóvel da vítima. Ainda nesta sequência, em 2014, o Tribunal da Relação de Coimbra[221] veio inclusive fazer uma

---

continuado e rápido e, permitindo-lhe a realização de outras operações, bem como a obtenção de vários serviços, de forma em princípio mais cómoda e, simultaneamente, com enormes poupanças de escala, por parte do banco, nomeadamente, na possível diminuição do número de funcionários em atendimento, o que explica a razão dos mesmos em promoverem estes serviços, insistentemente, junto dos seus clientes. Assim, não é legítimo ao banco invocar a sua irresponsabilidade numa situação de fraude informática, designada "phishing" de dados de autenticação do cliente, como o argumento que tal ocorreu no computador deste e não em qualquer sistema informático seu ou por si dominado, sabido que, é pressuposto deste tipo de serviço a utilização de computadores pessoais e não do próprio banco. É justa e equilibrada a indemnização no montante de € 20.000,00 a pagar pelo banco (guardião do depósito), a título de compensação pelos danos morais sofridos pela A. (cliente do banco), devido aos transtornos que lhe advieram por, da sua conta aberta naquele, sem sua autorização ter sido feita uma transferência no valor de € 13.000,00 (eventualmente, devido a burla informática) e, por isso vê devolvido um cheque apresentado a pagamento depois de concretizada aquela transferência. E, é assim, porque o cliente/ A. tinha avisado o banco do sucedido e da emissão do cheque e solicitado ao banco/R. que travasse aquela transferência, não logrando este demonstrar ter desenvolvido as diligências necessárias no sentido de o evitar, o que causou, não só, a sua devolução, com a "indicação de falta de provisão", (apesar do banco reconhecer, antes do cheque ser apresentado a pagamento, da existência de uma página Web falsa, imitando a sua página de abertura) como a A., em virtude de comunicação efetuada pelo seu próprio banco ao Banco de Portugal, vê o seu nome incluído na listagem de utilizadores de risco e sofre, por via disso, diversos danos, incluindo perda de clientes". Disponível em http://www.dgsi.pt/jtrg.nsf/86c25a698e4e7cb7802579ec004d3832/1964cc05baf5047c80257b900037c92a [Consultado em 18.07.2017].

[220] Acórdão do Tribunal da Relação de Lisboa de 15-07-2008, com seguinte sumário: *As mensagens que, depois de recebidas, ficam gravadas no recetor deixam de ter a natureza de comunicação em transmissão, nesta perspetiva, são comunicações recebidas, pelo que deverão ter o mesmo tratamento da correspondência escrita já recebida e guardada pelo destinatário tal como acontece na correspondência efetuada pelo correio tradicional, diferenciar-se-á a mensagem já recebida mas ainda não aberta da mensagem já recebida e aberta. Na apreensão daquela rege o art.º 179.º do CPP, mas a apreensão da já recebida e aberta não terá mais proteção do que as cartas recebidas, abertas e guardadas pelo seu destinatário. As mensagens escritas - SMS - que o arguido remeteu ao queixoso via telemóvel, cujo conteúdo foi copiado pela PJ e junto aos autos, constituem um meio de prova lícito e não configuram, de forma alguma, um caso de intromissão na vida privada do mesmo.* Disponível em http://www.dgsi.pt/jtrl.nsf/0/9182245992c7c5d18025749000503b8c?OpenDocument [Consultado em 18.07.2017].

[221] Acórdão do Tribunal da Relação de Coimbra de 18-06-2014, com o seguinte sumário: *Com introdução do n.º 2 do art.190.º do Código Penal, através da Reforma de 1995 - « Na mesma pena incorre quem, com intenção de perturbar a vida privada, a paz e o sossego de outra pessoa, telefonar para a sua habitação.» - e, posteriormente, com acrescentamento ao mesmo da expressão « ou para o seu telemóvel» através da Reforma de 2007, o legislador quis abranger todas as formas possíveis de comunicação tecnicamente permitidas através de telefone, sejam fixos ou móveis, incluindo a palavra escrita para os telefones móveis, que com a sua receção emitem um som de aviso. Uma vez que "telefonar" significa comunicar pelo telefone e que resulta dos factos dados como provados que o arguido, a partir do seu telemóvel enviou para o telemóvel do ofendido, as mensagens cujo teor consta da mesma factualidade, e que ao assim atuar quis e conseguiu perturbar a vida privada, a paz e o sossego do ofendido, conhecendo e querendo a realização daqueles factos antijurídicos e agindo com consciência da ilicitude, preencheu com a sua conduta todos os elementos constitutivos dos crimes de perturbação da vida.* Disponível em http://www.dgsi.pt/jtrc.nsf/c3fb530030ea1c61802568d9005cd5bb/84f1229d9b11c97680257d00003591fb?OpenDocument [Consultado em 18.07.2017].

interpretação extensiva à letra da lei, concretamente, ao art.º 190.º n.º 2 do CP, que pune a violação de domicílio ou perturbação da vida privada. Assim, o tribunal entendeu que não obstante o n.º 2 do artigo *supra* citado prever a punição da perturbação da vida privada relativamente a quem "*(...)com intenção de perturbar a vida privada, a paz e o sossego de outra pessoa, telefonar para a sua habitação ou para o seu telemóvel.*", não contemplar o envio de mensagens curtas, a verdade é que a utilização deste serviço, bem como o envio de mensagens por carta, bilhetes, ou através de outros suportes físicos e/ou virtuais, também acabam por ser um meio idóneo para a perturbação de outra pessoa. No fundo, o tribunal entendeu que as mensagens curtas enviadas pelo arguido lograram a perturbação do bem-estar da vítima, com a mesma eficácia que um mero telefonema teria, e que, por isso, o arguido preencheu todos os elementos constitutivos do crime de perturbação da vida privada.

Perante este cenário, parece-nos claro que não é aconselhável a confiança cega que por vezes é depositada no serviço de mensagens curtas. É necessário que a sociedade tenha consciência que os serviços de *SMS* podem ser facilmente um meio para a prática de um ilícito, ou, até mesmo, o componente integrador do tipo legal criminalmente punido. Segundo alguns autores[222], uma Infraestrutura de Chaves Públicas (*PKI*) providencia um grande nível de segurança no envio e receção de mensagens curtas, resolvendo maioria dos problemas relacionados com a segurança das *SMS*, contudo tais infraestruturas são suscetíveis de diminuírem a *performance* dos dispositivos. Assim, urge que a solução passe pela concertação de esforços entre todas as partes envolvidas (utilizadores, operadoras e OPC), sob pena da propagação de danos e ameaças de segurança.

[222] Neste sentido, MEDANI, *et al, "Review of mobile short message service security issues and techniques towards the solution"*, Scientific Research and Essays Vol. 6(6), March 2011, p. 1164.

CAPÍTULO IV

A APREENSÃO E INTERCEÇÃO DOS SERVIÇOS DE CORREIO ELETRÓNICO E DE MENSAGENS CURTAS

Aqui chegados, e porque é gritante que o sistema tal como se encontra desenhado levanta inúmeros paradigmas, cumpre, a título final, concentrarmo-nos na apreensão e interceção dos serviços de correio eletrónico e de mensagens curtas, uma vez que num país como Portugal o apuramento da verdade e a preparação de elementos de prova que possam ser reproduzidos em fase de julgamento carece sempre de aprovação constitucional. A recolha e obtenção de prova eletrónica é uma categoria que exige operações árduas de adaptação, atendendo ao terreno instável e periclitante que suscita inúmeros desafios, que vão muito para além da prova.

Como é comummente sabido, a recolha de prova na investigação criminal é dirigida com vista à descoberta da verdade material, significando isto que esta é a fase do processo na qual são reunidos a maior parte de indícios que permitem concluir a prática (ou não) de um crime, contudo terá a "encruzilhada legislativa processual penal portuguesa" respostas previamente estabelecidas para os problemas levantados pela reforma digital? Não será necessário um olhar renovado sobre um novo mundo no qual a desmaterialização é a palavra de ordem?

Ora, não desvirtuando a imprescindibilidade do tema e, não obstante a consciência que o tratamento da matéria que nos propusemos a desenvolver seria merecedor de um estudo muito mais aprofundado, e respeitando a extensão do conteúdo da presente dissertação, parece-nos ser este o momento oportuno para nos debruçarmos sobre a apreensão/interceção do correio eletrónico e das mensagens curtas, que continuam a dar azo a interessantes e controversas discussões na doutrina e jurisprudência portuguesa.

1. Encruzilhada legislativa

Comecemos então, sem individualismos e sem tentações, porque despidos de preconceitos estaremos melhor preparados para o estudo que procuramos elaborar, desbravar aquele que é um dos principais dilemas com a inauguração da era tecnológica e com o incremento das NTIC, i.e., a complexa "teia legislativa" na matéria da obtenção de prova digital, tal é a quantidade de fontes e normas que regulam parcelarmente esta matéria, nomeadamente: o CPP, a Lei n.º 32/2008 e a Lei n.º 109/2009.

Como seria expectável, esta trilogia legislativa apenas suscita a descodificação da centralidade normativa do CPP, a falta de articulação entre os vários preceitos legais, como contribui irremediavelmente para a indesejável incongruência axiológica que apenas poderá ser superada através de uma longa reflexão doutrinal e consequente adequada intervenção legislativa. Nas palavras eruditas de JOÃO CONDE CORREIA, "As peças do *puzzle* não se encaixam facilmente. Em vez de seguir o velho conselho iluminista e de optar por poucas leis, simples e claras, o legislador escolheu a via incerta da pluralidade e da complexidade, gerando um sistema anárquico, onde, muitas vezes, nem a sua letra, nem o seu espírito, nem, tão pouco, a sua história fornecem a bússola necessária para encontrar o caminho mais seguro" [223].

Ora, a título de exemplo, já a versão originária do CPP de 1987 consagrava na Parte I, Livro III, Título III, quatro meios de obtenção da prova que se mantiveram até hoje, nomeadamente: os exames, revistas e buscas, apreensões e escutas telefónicas. No Capítulo IV do Título III, mais propriamente no art.º 190.º[224], que corresponde parcialmente ao atual art.º 189.º, era consagrado o regime de extensão das escutas telefónicas a todos os meios técnicos que fossem "diferentes" do telefone, sendo uma norma contaminada de diversas dúvidas interpretativas.

[223] Cfr. CORREIA, João Conde, "*Prova Digital: as leis que temos e a lei que devíamos ter",* Revista do Ministério Público, Ano 35.º, nº 139", Julho-Setembro, 2014, pp. 30 e 31.

[224] De acordo o CPP de 1987, "*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.*"

De facto, desde cedo, JOSÉ DE FARIA COSTA[225] levantou a questão da querela da excecionalidade do regime de extensão previsto no atual art.º 189.º do CPP. O autor não consegue depreender, razoavelmente, o porquê de o legislador estender este tipo de regime excecional e que, por isso, não se pode alargar, sob pena de surgirem contradições indesejáveis e insanáveis.

Desta feita, não obstante as sucessivas alterações operadas minuciosamente no âmbito do regime de extensão das escutas telefónicas, o segundo nó górdio vai ainda prender-se com tal opção legislativa e, principalmente, com as diversas realidades técnicas previstas na atual redação do art.º 189.º do CPP. Neste artigo, o legislador não só vem estender a outro tipo de comunicações ou conversações tidas por qualquer outro meio diferente do telefone o regime das interceções telefónicas, proporcionando uma tutela mais protetora[226] como, no seu n.º 2, vem ainda regular a obtenção e junção aos autos de dados sobre a localização celular ou de registos de realização de conversações ou comunicações, já guardados "em suporte digital", esquecendo-se de outros suportes[227]. No fundo, o legislador optou por descaracterizar o instituto das escutas telefónicas, já que estendeu a diversas realidades as mesmas necessidades práticas, prejudicando desmesuradamente a investigação criminal[228].

Posteriormente, PEDRO VERDELHO[229] alerta para a desconsideração do real interesse da investigação criminal por parte do legislador, uma vez que a interceção de comunicações eletrónicas, como por exemplo o *e-mail*, em processo de inquérito, está totalmente proibida quando estejam em causa crimes de ameaça, difamação, injúria e devassa por meio de informática. Deste modo, interpretando restritivamente a cláusula de extensão prevista no art.º 189.º CPP, este tipo de crimes fica sujeito ao catálogo de admissibilidade das interceções telefónicas[230], como tal, não obstante a al. e) do n.º 1 do art.º 187.º do CPP autorizar a

---

[225] A este propósito, COSTA, José de Faria, "*As Telecomunicações e a Privacidade...*", *op. cit.*, pp. 76 e 77.

[226] A título de exemplo, a interceção de comunicações necessita de autorização por despacho fundamentado do JIC, mediante requerimento do MP, durante a fase de inquérito do processo.

[227] Nomeadamente o suporte em papel.

[228] Neste sentido, ANDRADE, Manuel da Costa, *op. cit.*, pp. 185 e 186. Neste mesmo sentido, MESQUITA, Paulo Dá, *Processo Penal, Prova e Sistema Judiciário*, Coimbra, Coimbra Editora, 2010, p. 89.

[229] A este propósito, VERDELHO, Pedro, *"Técnica no Novo C.P.P..."*, *op. cit.*, pp. 165 e 166. Neste mesmíssimo sentido, CORREIA, João Conde, *"Prova Digital..."*, *op. cit.*, p. 32.

[230] O artº 187.º n.º 1 do CPP prevê que "*(...) a interceção e a gravação de conversações ou comunicações telefónicas só podem ser autorizadas durante o inquérito, 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, por despacho fundamentado do juiz de instrução e mediante requerimento do Ministério Público, quanto a crimes:*

interceção deste tipo de crimes quando são cometidos através do telefone, o certo é que, por exemplo, não é permitida a apreensão de mensagens de correio eletrónico injuriosas, difamatórias ou ameaçadoras perpetradas através de um computador ou um *tablet,* porque não só detêm uma moldura penal inferior àquela que se encontra consagrada na al. a) do n.º 1 do art.º 187.º, como o dispositivo tecnológico utilizado nem sequer se encontra consagrado na lei processual penal[231].

Como tal, para além da falta de fundamentação, imprecisão técnica e de gerar indesejáveis confusões, a remissão prevista no CPP não satisfaz as exigências, nem apresenta respostas inteligíveis, aos problemas das comunicações realizadas através de sistemas informáticos.

Já noutra senda, JOÃO CONDE CORREIA[232] critica a duplicação de regimes consagrados no art.º 187.º do CPP e no art.º 9.º da Lei n.º 32/2008. De acordo com o autor, a transmissão de dados de tráfego só é concebível num restrito catálogo de crimes, através de despacho fundamentado do JIC, se houver razões para crer na indispensabilidade para a descoberta da verdade ou na impossibilidade da prova de outra forma, só sendo admitida a transmissão de dados relativos ao restrito grupo do n.º 3. Ora, não teria sido mais útil a consagração de normas gerais no CPP e de normas especiais e sobretudo questões técnicas na Lei n.º 32/2008? A esta "casa dos horrores hermenêuticos" não podemos esquecer que, inclusive, o art.º 187.º do CPP consagra um catálogo de crimes que excede, em larga escala, os crimes graves previstos no art.º 2.º da Lei n.º 32/2008.

Na sequência do *supra* mencionado, podemos ainda reforçar mais um pequeno pormenor ao mais desatento leitor. Assim, tal como já foi afirmado, o legislador português optou por proceder à extensão do regime da interceção de *e-mail* ao regime das interceções telefónicas, de acordo com o art.º 189.º do CPP. Por outro lado, ARMANDO DIAS RAMOS[233] alerta para o facto de se estivermos perante um caso de apreensão de *e-mail*, a LCiber ordena a aplicação do regime de apreensão de correspondência, *vd* art.º 179.º CPP, *ex vi* art.º 17.º

---

a) Puníveis com pena de prisão superior, no seu máximo, a 3 anos;

e) De injúria, de ameaça, de coação, de devassa da vida privada e perturbação da paz e do sossego, quando cometidos através de telefone;"

[231] Apesar do escasso desenvolvimento no que às comunicações eletrónicas diz respeito, por parte do legislador processual penal português, é sabido que, no entanto, o art.º 18.º da LCiber consagra, de facto, a interceção de comunicações eletrónicas cometidas através de um sistema informático. Assim, não se compreende a razão de o legislador português não ter consagrado este preceito no CPP...

[232] Neste sentido, CORREIA, João Conde, *"Prova Digital...", op. cit.*, p. 33.

[233] A este propósito, RAMOS, Armando Dias, *op. cit.,* p. 45.

LCiber. Ainda que muitos autores refutem esta dualidade de tratamento, não teria sido mais simples a criação de um artigo que compreendesse as duas realidades, evitando enigmas desnecessários e quiçá decisões mal fundadas?

Além disso, BENJAMIM SILVA RODRIGUES[234] vem condenar a inércia e desinteresse por parte do legislador português na forma como veio reger a matéria da obtenção de comunicações eletrónicas. De facto, vem o art.º 189.º n.º 1 do CPP referir que o disposto nos art.º 187.º e 188.º é correspondentemente aplicável às conversações ou comunicações tidas por qualquer meio diferente do telefone, como por exemplo o correio eletrónico ou o serviço de mensagens curtas. Mas, por outro lado, olhando para o preceituado no art.º 17.º da LCiber[235], questionamo-nos como é que podemos compreender que um juiz possa configurar a apreensão de comunicações eletrónicas, que se considerem de grande interesse para a descoberta da verdade, se não é ele quem preside essas mesmas investigações? É ainda ininteligível o regime geral para o qual o art.º 17.º da LCiber remete, ou seja, o art.º 179.º n.º 3 do CPP, regime este que se caracteriza pela sua especificidade no que toca ao facto de o juiz ser o primeiro a tomar conhecimento do conteúdo da própria correspondência, tendo o poder de fazê-la juntar ao processo[236]. Sem sombra de dúvidas, que só podemos constatar o infeliz esquecimento, por parte do legislador, da complexa regulamentação do art.º 179.º n.º 3 do CPP, bem como a do art.º 189.º do CPP.

Por último, desengane-se aquele que julgue que a Lei n.º 109/2009 tem unicamente uma importância acessória no sistema processual de prova digital. De facto, as suas disposições processuais penais, previstas nos art.º 11.º a 21.º, aplicam-se à cibercriminalidade em sentido amplo e em sentido restrito, como se um autêntico regime geral de prova digital se tratasse, "(...) assumindo uma inquestionável vocação transversal a todo o sistema processual penal (...)"[237]. Mais uma vez, não teria sido um ótimo entrave na dissipação e na luta contra o

---

[234] A este propósito, RODRIGUES, Benjamim Silva, *Da Prova Penal, Tomo IV...*, *op. cit.,* p. 36.

[235] Artigo 17.º - Apreensão de correio eletrónico e registos de comunicações de natureza semelhante

Quando, no decurso de uma pesquisa informática ou outro acesso legítimo a um sistema informático, forem encontrados, armazenados nesse sistema informático ou noutro a que seja permitido o acesso legítimo a partir do primeiro, mensagens de correio eletrónico ou registos de comunicações de natureza semelhante, o juiz pode autorizar ou ordenar, por despacho, a apreensão daqueles que se afigurem ser de grande interesse para a descoberta da verdade ou para a prova, aplicando-se correspondentemente o regime da apreensão de correspondência previsto no Código de Processo Penal.

[236] Ainda neste sentido, RODRIGUES, Benjamim Silva, *Da Prova Penal, Tomo IV...*, *op. cit.,* p. 531.

[237] Cfr. CORREIA, João Conde, *"Prova Digital...", op. cit.*, p. 34.

cibercrime se, em vez de termos legislações extravagantes, tivéssemos um regime geral de obtenção de prova eletrónica no próprio CPP, com um capítulo autónomo?

PAULO DÁ MESQUITA[238] menciona três frágeis razões de ordem para o enquadramento legal apresentado:

1) é tradição portuguesa, especificamente na área penal, existirem outros diplomas estruturantes relativos a matérias específicas, por exemplo, a Lei n.º 15/2001, de 05 de junho (Regime Geral das Infrações Tributárias), ou o DL n.º 15/93, de 22 de janeiro (Legislação de Combate à Droga);
2) inconveniência de ver em diplomas do ordenamento penal regras especiais;
3) interesse prático, para *quem de direito*, em se encontrarem sistematizadas as normas relativas a um setor específico de criminalidade.

Ora, quanto ao primeiro argumento, tal como o autor *supra* mencionado refere, e bem, muita tradição é apenas uma sucessão de maus hábitos. No que às legislações mencionadas diz respeito, no primeiro argumento, é sabido que estas apenas se reportam a regras especiais relativas aos crimes consagrados nesses diplomas e não são aplicáveis genericamente como acontece com a LCiber. Deste modo, também o segundo argumento acaba por ser destronado tendo em conta que, por exemplo, as regras processuais previstas na LCiber são aplicáveis a um elenco de crimes bem mais amplo do que o previsto no âmbito das escutas telefónicas. Por fim, nem o terceiro argumento chega a "bom porto", uma vez que as normas processuais previstas na LCiber não se reportam unicamente a um setor específico de criminalidade.

Tal como já foi mencionado anteriormente[239], o CPP renuncia temas carecidos de atenção, não revela grandes soluções para a quantidade de problemas suscitados pela prova eletrónica ou sequer uma sistematização fiel, técnica e rigorosa quanto à interceção de telecomunicações e recolha da prova digital. Nas proverbiais palavras de RITA CASTANHEIRA NEVES "(...) o Direito tem que cuidar de tratar correctamente a evolução que passa diante de si,

[238] MESQUITA, Paulo Dá, *op. cit.* pp. 98 e 99.

[239] *Vide supra* o 1.º capítulo da presente dissertação de mestrado, onde, subtilmente, são colocados alguns dos problemas suscitados pela prova digital.

tratar igualmente o que é igual e diferentemente o que é diferente, sendo esta a única maneira de se constituir como realização de um Estado de Direito que se quer justo e actual" [240].

Com efeito, são diversos os aspetos relacionados com o mundo cibernético que carecem de uma acuidade especial por se tratarem de questões que estão em constante evolução e que, por isso mesmo, não se podem coadunar com as normas existentes. Como se depreende, encontramo-nos perante uma crescente incerteza e insegurança jurídicas dificultando as instâncias de controlo o que, consequentemente, só pode conduzir à impossibilidade de sucesso da investigação criminal. Com toda esta encruzilhada parece-nos que as comunicações eletrónicas continuarão a fazer o seu constrangedor percurso na doutrina e jurisprudência portuguesa...

2. O que distingue a apreensão da interceção de comunicações eletrónicas?

Embora o objetivo da presente dissertação passe pela análise da problemática dos meios de obtenção de prova digital, mais concretamente, os dilemas enfrentados com as mensagens curtas e com o correio eletrónico, na sequência da *supra* distinção operada entre apreensões e interceções e porque seria contraproducente ignorá-la, o certo é que para que possamos inteligir a sua verdadeira função, cumpre-nos desbravar, num plano epistemológico, a diferença entre estas duas realidades que, hoje, se refletem na esfera das comunicações eletrónicas.

Sem mais demoras, chamamos a atenção para a própria definição dada pelo Dicionário da Língua Portuguesa quanto aos dois substantivos em causa. Deste modo, por um lado, a apreensão[241] define-se como o ato de alguém se apoderar do que outrem não deve ter, deixando

[240] Cfr. 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, Coimbra Editora, 2011, p. 144.

[241] Definição de apreensão, em Dicionário Priberam da Língua Portuguesa, disponível em https://www.priberam.pt/dlpo/apreens%C3%A3o [Consultado em 21.08.2017].

para o art.º 178.º do CPP[242] os objetos que são suscetíveis de apreensão e pressupostos da mesma.

Já noutra senda, o Dicionário da Língua Portuguesa vem definir a interceção[243] como o ato de intercetar, ou seja, é o deter ou interromper o curso de algo, como por exemplo uma mensagem, fazendo com que esta não chegue ao destino previamente pretendido.

Contudo, no lapidar dizer de CARLOS CASABONA[244], o vocábulo interceção tem caráter polissémico, ou seja, tem vários sentidos. Assim, em primeiro lugar, a interceção pode entender-se como o ato de alguém se apoderar de algo antes que essa coisa chegue ao lugar ou à pessoa a que se destina. Da mesma forma, pode caracterizar-se como o ato de obstrução de uma via de comunicação. Em último lugar, o autor defende que a interceção pode ser o ato de aceder a uma comunicação de terceiros sem interromper essa mesma comunicação.

---

[242] Artigo 178.º - Objeto e pressupostos da apreensão

1 - São apreendidos os instrumentos, produtos ou vantagens relacionados com a prática de um facto ilícito típico, e bem assim todos os objetos que tiverem sido deixados pelo agente no local do crime ou quaisquer outros suscetíveis de servir a prova.

2 - Os instrumentos, produtos ou vantagens e demais objetos apreendidos nos termos do número anterior são juntos ao processo, quando possível, e, quando não, confiados à guarda do funcionário de justiça adstrito ao processo ou de um depositário, de tudo se fazendo menção no auto.

3 - As apreensões são autorizadas, ordenadas ou validadas por despacho da autoridade judiciária.

4 - Os órgãos de polícia criminal podem efetuar apreensões no decurso de revistas ou de buscas ou quando haja urgência ou perigo na demora, nos termos previstos na alínea c) do n.º 2 do artigo 249.º

5 - Os órgãos de polícia criminal podem ainda efetuar apreensões quando haja fundado receio de desaparecimento, destruição, danificação, inutilização, ocultação ou transferência de instrumentos, produtos ou vantagens ou outros objetos provenientes da prática de um facto ilícito típico suscetíveis de serem declarados perdidos a favor do Estado.

6 - As apreensões efetuadas por órgão de polícia criminal são sujeitas a validação pela autoridade judiciária, no prazo máximo de setenta e duas horas.

7 - Os titulares de instrumentos, produtos ou vantagens ou outros objetos apreendidos podem requerer ao juiz a modificação ou a revogação da medida.

8 - O requerimento a que se refere o número anterior é autuado por apenso, notificando-se o Ministério Público para, em 10 dias, deduzir oposição.

9 - Se os instrumentos, produtos ou vantagens ou outros objetos apreendidos forem suscetíveis de ser declarados perdidos a favor do Estado e não pertencerem ao arguido, a autoridade judiciária ordena a presença do interessado e ouve-o.

10 - A autoridade judiciária prescinde da presença do interessado quando esta não for possível.

11 - Realizada a apreensão, é promovido o respetivo registo nos casos e nos termos previstos na legislação registal aplicável.

12 - Nos casos a que se refere o número anterior, havendo sobre o bem registo de aquisição ou de reconhecimento do direito de propriedade ou da mera posse a favor de pessoa diversa da que no processo for considerada titular do mesmo, antes de promover o registo da apreensão a autoridade judiciária notifica o titular inscrito para que, querendo, se pronuncie no prazo de 10 dias.

[243] Definição de interceção, em Dicionário Priberam da Língua Portuguesa, disponível em https://www.priberam.pt/dlpo/interce%C3%A7%C3%A3o [Consultado em 21.08.2017].

[244] Não obstante o caracter polissémico inicialmente invocado, o autor rapidamente conclui que a interceção só poderá ser conducente com o ato de aceder à comunicação de um terceiro, desde que não interrompa o destino da mesma. Neste sentido, CASABONA, Carlos María Romeo, *op. cit.,* p. 137.

Por outro lado, DÁ MESQUITA[245] afirma, em várias passagens da sua obra, que a interceção é o ato que se destina a recolher informações armazenadas num sistema informático em tempo real, através de vários dispositivos próprios para o efeito, caracterizando-se por ser um outro meio de acesso legítimo a sistema informático, para além da própria busca informática.

Independentemente dos pequenos pormenores apontados pelos autores *supra* mencionados, existe um aspeto na qual existe uma total concordância, i.e., que a interceção de comunicações eletrónicas compreende sempre o ato de recolha de informações durante o trajeto da própria mensagem, ou seja, durante o trajeto do *e-mail* ou da *SMS* que saiu do computador ou telemóvel do emissor, para o equipamento eletrónico do recetor, através das redes de servidor.

Sublinhe-se que, não obstante as traições epistemológicas que a língua portuguesa, por vezes, sugere, e ainda a confusão da natureza e semelhança entre os regimes específicos da interceção e da apreensão, o certo é que o legislador não permitiu o estabelecimento de hipóteses concretas no que à obtenção de comunicações eletrónicas diz respeito, convidando a uma pluralidade de soluções.

2.1. Requisitos legais para a apreensão e interceção de comunicações

Aqui chegados, importa ainda fazer um pequeno parenteses. É nossa convicção que face às novas realidades digitais e ao nascimento do Direito Penal substantivo e adjetivo neoliberal que têm vindo a surgir novos tipos de ilícitos, obrigando a uma constante atualização dos OPC. Contudo, existe sempre, no seio da investigação criminal, uma linha que não pode ser ultrapassada pelas entidades competentes, i.e., a própria lei.

Deste modo, e tal como já foi sugerido no Capítulo I, a lei é clara no que toca ao tipo de prova que considera proibida, principalmente no que às comunicações diz respeito,

[245] A este propósito, MESQUITA, Paulo Dá, *op. cit.* p. 120.

nomeadamente no art.º 126.º n.º 3 do CPP[246], art.º 32.º n.º 8 CRP[247] e ainda no art.º 34.º n.º 4 da CRP[248], estipulando a nulidade e, consequentemente, a sua não utilização para aquele tipo de prova que foi obtida à revelia do estipulado legalmente.

Através destes artigos é possível constatar que a proteção conferida à vida privada é equiparada à correspondência dos demais meios de comunicação, nos quais se incluem, claro, os novos meios de comunicação eletrónica. A consagração destes ideais pretende estipular, sem margem para dúvidas, que o investigador não pode recorrer aos mesmos métodos de quem é investigado, que existem outros direitos que devem igualmente ser protegidos por lei, havendo requisitos formais que obrigatoriamente têm de ser cumpridos, principalmente devido à preocupante intromissão na vida privada no ambiente digital.

Ora, cumpre agora tipificar quais os requisitos legais para haver lugar a uma correta apreensão e interceção de comunicações eletrónicas. Assim, no que à apreensão de comunicações diz respeito, e de acordo com o art.º 179.º do CPP, formalmente, é necessário que:

1) o JIC autorize ou ordene, por despacho, a apreensão de comunicações expedidas pelo arguido, ou que lhe seja dirigida, mesmo sob nome diverso ou através de outra pessoa, sendo o próprio JIC a primeira pessoa a tomar conhecimento do conteúdo da correspondência apreendida;
2) esteja em causa um crime punível com pena de prisão superior, no seu máximo, a 3 anos;
3) a diligência se revele de grande interesse para a descoberta da verdade ou para a prova.

Por outra banda, de acordo com o art.º 187.º e ss do CPP, estaremos perante uma correta interceção de comunicações, desde que:

1) o processo se encontre em fase de inquérito;

---

[246] *Vide* o art.º 126.º n.º 3 do Código de Processo Penal: *Ressalvados os casos previstos na lei, são igualmente nulas, não podendo ser utilizadas, as provas obtidas mediante intromissão na vida privada, no domicílio, na correspondência ou nas telecomunicações sem o consentimento do respetivo titular.*

[247] *Vide* o art.º 32.º n.º 8 da Constituição da República Portuguesa: *São nulas todas as provas obtidas mediante tortura, coação, ofensa da integridade física ou moral da pessoa, abusiva intromissão na vida privada, no domicílio, na correspondência ou nas telecomunicações.*

[248] *Vide* o art.º 34.º n.º 4 da Constituição da República Portuguesa: *É proibida toda a ingerência das autoridades públicas na correspondência, nas telecomunicações e nos demais meios de comunicação, salvos os casos previstos na lei em matéria de processo criminal.*

2) tem de haver razões para crer que a diligência seja indispensável para a descoberta da verdade material, ou que a prova seria, de outro modo, difícil ou impossível de obter;
3) seja operada pelos OPC, mediante despacho fundamentado do JIC;
4) mediante requerimento do MP;
5) no âmbito dos crimes previstos no art.º 187.º n.º1 e 2;
6) nos casos previstos no n.º 2, a autorização é levada, no prazo máximo de 72 horas, ao conhecimento do juiz do processo, para tramitação subsequente;
7) a interceção só pode ser autorizada no que toca ao grupo restrito de pessoas previsto no n.º 4;
8) no que à durabilidade da interceção diz respeito, esta só é autorizada pelo prazo máximo de 3 meses, renovável por períodos sujeitos ao mesmo limite, desde que se verifiquem os respetivos requisitos;
9) com base na elaboração do auto e respetivo relatório, com indicação das partes relevantes para a prova, os OPC levam a interceção ao conhecimento do MP, que por sua vez, transmite ao juiz competente no prazo máximo de quarenta e oito horas.

Como tal, embora a legislação seja clara, no que aos métodos proibidos de prova diga respeito, o certo é que no art.º 34.º n.º 4 da CRP está consagrado o pilar que permite a apreensão e interceção de comunicações eletrónicas, nomeadamente nos casos previstos na lei em matéria de processo criminal (existindo ainda a exceção do consentimento do próprio visado[249]), sendo com base nesta exceção que o processo penal consagrou os atuais meios de obtenção de prova. Ademais, também é sabido que, de acordo com os preceitos legais *supra* enumerados, se os agentes não procederem de acordo com os respetivos requisitos de admissibilidade, a apreensão[250] ou interceção[251] de comunicações eletrónicas é considerada nula[252], não podendo ser posteriormente utilizada[253].

[249] Neste sentido, VERDELHO, Pedro, *"A obtenção de prova...", op. cit.,* p. 120.

[250] *Vide* a primeira parte do art.º 179.º n.º1 do Código de Processo Penal: *Sob pena de nulidade, o juiz pode autorizar ou ordenar (...).*

[251] *Vide* o art.º 190.º do Código de Processo Penal: *Os requisitos e condições referidos nos artigos 187.º, 188.º e 189.º são estabelecidos sob pena de nulidade.*

[252] A este propósito, BRAVO, Rogério, *"Da não equiparação do correio-electrónico ao conceito tradicional de correspondência por carta",* Polícia e Justiça, Revista do Instituto Superior de Polícia Judiciária e de Ciências Criminais, III Série, n.º 7, Coimbra, Coimbra Editora, janeiro – junho 2006, p. 3.

2.2. Qual a consequência para a violação dos requisitos legais para a apreensão e interceção de comunicações?

Ora, se assim for, ou seja, se os requisitos de admissibilidade não forem cumpridos e se as comunicações eletrónicas forem consideradas nulas, poderá haver lugar à constituição de crime? Podem estes métodos de obtenção de prova ser utilizados com o fim exclusivo de proceder contra os OPC que procederam à investigação?

Apesar de não procederemos, no entanto, a uma mais aprofundada análise, tanto do direito em si, como das questões que se relacionam, por motivos de estruturação e economia de trabalho, cumpre-nos referir, ainda que a título meramente indicativo que, de facto, atentos à letra da lei, nomeadamente o n.º 4 do art.º 126.º do CPP[254], parece-nos haver única e simplesmente uma resposta afirmativa à questão *supra* mencionada, contudo, a mesma pode não ser tão nítida como aparenta.

Assim, atentos às doutas palavras de PEDRO VERDELHO[255], importa atender que não obstante o art.º 194.º do CP[256] punir aquele que, sem consentimento, violar a correspondência

---

[253] Acórdão do Tribunal da Relação do Porto de 13-05-2015, com o seguinte sumário: *Só podem valer como prova em julgamento as comunicações [no caso, uma SMS] que o Ministério Público mandar transcrever (ao órgão de polícia criminal que tiver efetuado a interceção e gravação) e indicar como meio de prova na acusação. O art. 190.º, do CPP, trata de forma não diferenciada a inobservância de requisitos e condições de admissibilidade e o mero incumprimento de certas formalidades de procedimento da interceção e gravação de conversações ou comunicações telefónicas. A inobservância das regras do art. 188.º, do CPP, constitui nulidade que impede toda e qualquer utilização do material probatório assim obtido. Trata-se, portanto, não de uma nulidade da sentença, mas de uma invalidade que atinge apenas essas concretas conversações ou comunicações telefónicas, impedindo a sua utilização em juízo como meio que contribua para a formação da convicção dos juízes do julgamento. Arredado esse elemento probatório, impõe-se determinar se existem outros que permitam concluir pela responsabilidade criminal do arguido.* Disponível em http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/e3e21d9e62cdb86f80257e520037f3a0?OpenDocument [Consultado em 25.08.2017].

[254] *Vide* o art.º 190.º n.º 4 do Código de Processo Penal: *Se o uso dos métodos de obtenção de provas previstos neste artigo constituir crime, podem aquelas ser utilizadas com o fim exclusivo de proceder contra os agentes do mesmo.*

[255] A este propósito, VERDELHO, Pedro, *"Apreensão de Correio Electrónico em Processo Penal"*, Revista do Ministério Público, Ano 25.º, nº 100, outubro-dezembro, 2004, pp. 161 – 164.

[256] 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 1 ano ou com pena de multa até 240 dias.

ou telecomunicação de um terceiro, nem tudo é tão claro quanto pode parecer. Nesta perspetiva, o autor defende que às comunicações eletrónicas, como os *e-mails* e *SMS* aplicaríamos o regime das telecomunicações, e que só podemos considerar comunicações eletrónicas (e também telecomunicações) a comunicação que, de facto, existiu. Assim, sugere que um *e-mail* ou uma *SMS* só são consideradas comunicações a partir do momento que chegaram ao seu destino e terminaram, resultando num ficheiro informático guardado num *PC* ou num telemóvel.

Operando estas considerações, somos levados a crer que após a receção de um *e-mail* ou *SMS* jamais em tempo algum poderia haver lugar violação de comunicação eletrónica, nos termos do art.º 194.º do CP, porque não é possível a intromissão numa coisa que já cessou e que já não existe. PEDRO VERDELHO conclui, portanto, que na legislação portuguesa se verifica um *real vazio legislativo* e consequente desproteção penal das comunicações eletrónicas. Assim, o autor defende que havendo lugar a "violação" de telecomunicações ela unicamente poderá ser punida se, e só se, o destinatário ainda não rececionou a comunicação em causa. Em contrapartida, se a interceção ou apreensão de uma comunicação (que já chegou ao seu destino) não for operada de acordo com os seus critérios de admissibilidade então, o seu infrator, não poderá ser punido nos termos do artigo em causa.

Porém, a doutrina diverge, havendo quem defenda que não obstante a comunicação ter terminado, o seu conteúdo perdura e, como tal, aquele que violar as comunicações eletrónicas como um *e-mail* ou *SMS*, será punido nos termos do n.º 2 do art.º 194.º do CP[257].

Deste modo, mais uma vez, são constatáveis as prementes incongruências do processo penal português no que às comunicações eletrónicas diz respeito, parecendo ser uma realidade a evitar a todo custo. Com o surgimento das NTIC não só não houve uma plena e harmoniosa atualização do processo penal português como também constatamos que o direito penal ficou um pouco à margem do que seria esperado, uma vez que não houve uma aceitação de que, na atualidade, podem ser operadas novas lesões através de variadíssimas novas vias.

Certo é que nem toda a história do processo penal no que a este assunto diz respeito foi um pesadelo. E, em 1987, por exemplo, foi dada a conhecer a possibilidade de intercetar

---

2 - Na mesma pena incorre quem, sem consentimento, se intrometer no conteúdo de telecomunicação ou dele tomar conhecimento.

[257] Neste sentido, RODRIGUES, Benjamim Silva, que defende a condenação daqueles que venham a aceder, sem qualquer consentimento, ou autorização por quem de direito, a comunicações eletrónicas, *Das Escutas Telefónicas...*, *op. cit.,* pp. 438 – 450.

comunicações telefónicas[258] e em 2009 até surgiu a LCiber... No entanto, urge que a lei processual penal portuguesa esteja, de facto, relacionada com as demais comunicações eletrónicas, estabelecendo regimes concretos, claros e esclarecidos, para a troca de informações mais expeditas e mais económicas, como é o caso das novas formas de comunicação. Afigura-se necessário que o legislador português abra os olhos para a sociedade de hoje, para as realidades vividas no séc. XXI, que resolva todas as dúvidas de interpretação que têm vindo a ser suscitadas e que proceda à real atualização legislativa em congruência com as leis já se encontram em vigor.

3. Análise dos regimes de recolha de comunicações eletrónicas – a real batalha doutrinal

Terminada a análise da distinção entre a apreensão e interceção de comunicações eletrónicas chegamos àquele que é, provavelmente, o ponto fulcral da presente dissertação, sendo esta a principal razão que nos levou a optar pela escolha do tema objeto de estudo.

Consideramos que o ponto de partida para o presente subcapítulo prende-se basicamente com o seguinte dilema: quando um agente envia uma *SMS* ou um *e-mail*[259] para um segundo agente, o certo é que a recolha deste tipo de prova digital pode ser levada a cabo em distintas fases. Se, por um lado, a jurisprudência[260] uniformizou-se quanto à desnecessidade de intervenção judicial na obtenção de comunicações eletrónicas quando o destinatário (em regra, o lesado) fornece a autorização para junção aos autos dessas comunicações, é sabido que o

[258] A este propósito, NEVES, Rita Castanheira, *op. cit.* p. 24.

[259] Relembramos que o regime aplicável ao *e-mail* será na íntegra aplicado ao serviço de mensagens curtas, de um qualquer telemóvel, tendo em conta o elemento comum, i.e., a transmissão de uma mensagem digital em texto. Neste sentido, VERDELHO, Pedro, *"A obtenção de prova...", op. cit.*, p. 124; ANDRADE, Manuel da Costa, *op. cit.*, pp. 145 – 159; RODRIGUES, Benjamim Silva, *Das Escutas Telefónicas...*, *op. cit.*, p. 435, BRAVO, Rogério, *op. cit.* p. 2 e ainda NEVES, Rita Castanheira, *op. cit.,* p. 171.

[260] A título de exemplo, veja-se o Acórdão do Tribunal da Relação do Porto de 03-04-2013, com o seguinte sumário: *As SMS recebidas no equipamento de comunicação (telemóvel) da ofendida e por ela disponibilizadas estão a coberto de qualquer procedimento de validação judicial. Trata-se de um meio de prova fornecido de forma espontânea pelo recetor e seu legítimo detentor. O seu uso em processo não constitui meio de prova proibido.* Disponível em http://www.dgsi.pt/jtrp.nsf/d1d5ce625d24df5380257583004ee7d7/d21c6752627b971780257b4f003caa5d?OpenDocument [Consultado em 23.08.2017].

mesmo já não sucede quando as mensagens estão guardadas em terminais de quem não autoriza a obtenção das comunicações.

Ora, não é novidade para ninguém que podemos recolher aquela comunicação eletrónica enquanto o destinatário ainda não a recebeu; quando o destinatário já a recebeu, mas ainda não a leu; ou podemos ainda reunir comunicações eletrónicas após o receção e consequente leitura da mesma, que simplesmente se encontra armazenada no seu respetivo dispositivo. Perante distintas ocasiões, haverá lugar para distintas análises e conclusões?

Por sabermos que o risco de nos deixarmos contaminar pelos textos opinativos é real, selecionaremos, desde logo, aquelas que são as doutrinas maioritárias que, em todo caso, são seguidas pelas doutrinas minoritárias, no que à interceção/apreensão de comunicações eletrónicas diz respeito.

Assim, atendendo ao facto que os conceitos básicos já foram previamente delimitados, que a recolha do conteúdo de um *e-mail* e de uma *SMS* pode ser efetuado em diversas fases cumpre-nos, finalmente, desenhar a essência que a doutrina e jurisprudência têm estabelecido em sede de obtenção de prova digital na investigação criminal, o caso particular do regime jurídico dos serviços de correio eletrónico e de mensagens curtas, afirmando desde já que este é talvez o ponto mais discutível do novo regime legal de obtenção de prova digital.

3.1. Teoria defendida por PEDRO VERDELHO

Ora, como já tivemos oportunidade de constatar, o regime jurídico do art.º 189.º do CPP vem sugerir que o regime das interceções telefónicas seja correspondentemente aplicável às comunicações transmitidas através de qualquer meio técnico diferente do telefone, como é o caso do correio eletrónico ou outras formas de transmissão de dados por via telemática.

De acordo com este preceito, PEDRO VERDELHO reforça, e bem, em várias passagens das suas obras, que uma comunicação eletrónica pode ser utilizada como prova de um crime depois de já ter sido recebida e lida pelo destinatário, momento este em que já se encontra armazenada no equipamento terminal a que se destinava, ou até pode ainda ser intercetada em

tempo real, no decurso de uma determinada investigação. Basicamente, este autor vem defender que uma comunicação não pode estar guardada, sendo quando muito guardado unicamente o seu registo, como tal sugere a aplicação de um regime tripartido[261] no que à obtenção de prova digital diz respeito, distinguindo-se da seguinte forma:

1) se estivermos perante um caso de interceção em tempo real de uma comunicação eletrónica devemos aplicar o regime das interceções telefónicas, nos termos do art.º 189.º CPP;
2) se a comunicação eletrónica chegou ao seu destino, mas ainda não foi lida, então a comunicação cessou e encontra-se no dispositivo tecnológico do destinatário à espera de ser lida, como tal será um ficheiro em formato digital e deverá ser aplicado o regime da apreensão de correspondência, previsto no art.º 179.º do CPP;
3) se a comunicação eletrónica já foi recebida, aberta e lida, então o meio de obtenção de prova que deverá ser aplicado será o das normais apreensões, previsto no art.º 178.º do CPP.

Portanto, o autor sugere que se estamos perante três momentos completamente distintos, então teremos obrigatoriamente de ter três regimes completamente distintos. É defendido, portanto, que perante uma comunicação eletrónica que ainda não tenha chegado ao seu terminal de destino deverá ser aplicado o regime das interceções telefónicas, detentor de um regime restritivo de acesso.

Por outro lado, se uma comunicação eletrónica já foi rececionada, mas ainda não foi lida pelo destinatário, então deveríamos aplicar o regime da apreensão de correspondência, estando sujeita às formalidades previstas no art.º 179.º do CPP. Daqui podemos admitir que a possibilidade de apreensão de comunicações eletrónicas no dispositivo eletrónico do destinatário, ou no servidor onde essa comunicação se encontra conservada[262].

Por fim, se a comunicação eletrónica já tiver sido recebida e consequentemente lida, a mensagem em si já deixou de ter a essência de uma comunicação em transmissão, para passar a ser um registo de comunicação recebida e lida tendo, porventura, a mesma essência da

[261] Relembramos que à data de duas primeiras referências bibliográficas *infra* mencionadas ainda não tinha sido operada a reforma de 2007 do CPP, e relembramos que todas as referências são mais antigas do que a LCiber. Neste sentido, VERDELHO, Pedro, *"A obtenção de prova...", op. cit.*, pp. 121 – 124; *"Apreensão de Correio Electrónico...", op. cit.,* pp. 153 – 164; e ainda *"Técnica no Novo C.P.P...", op. cit.,* pp. 163 – 168 que vem dar uma lufada de ar fresco após a reforma de 2007 do CPP.

[262] VENÂNCIO, Pedro Dias, *"Breve Introdução...", op. cit.,* pp. 23 e 24.

correspondência em papel. Perante esta afirmação, e à semelhança do que acontece com o correio dito tradicional, no âmbito da obtenção de prova em processo penal, uma comunicação eletrónica que já tenha sido aberta e porventura lida não deverá ter mais proteção que a correspondência em papel, devendo, por isso mesmo, ter exatamente o mesmo nível de proteção.

Sem qualquer reserva, o autor defende que as comunicações eletrónicas que já foram recebidas e lidas serão consideradas meros documentos escritos que, por exemplo, podem ser apreendidos no decurso de uma busca, sem qualquer problema, não usufruindo da aplicação do regime de proteção da reserva de correspondência e de telecomunicações[263], nem sequer serão abrangidas pela proteção constitucional do sigilo da correspondência. No fundo, é defendido que as comunicações eletrónicas que foram recebidas e lidas (permanecendo, por exemplo, no servidor de *e-mail*, no computador, ou no telemóvel do destinatário) são equiparáveis às cartas em papel que foram lidas e, posteriormente, guardadas numa gaveta.

Foi através da divisão operada pelo autor *supra* mencionado que o Tribunal da Relação de Lisboa, em 15 de julho de 2008[264], conclui que uma comunicação eletrónica, tal como qualquer comunicação, ocorre durante um período temporal, como tal só podendo ser intercetada durante o período que se compreende entre o dispositivo do recetor e do destinatário. Posteriormente, é acolhida a tese que a comunicação fica guardada no equipamento eletrónico do recetor e, como tal, o meio de obtenção de prova ideal a ser utilizado já será o regime das correspondências, sendo que temos de fazer uma distinção se a mensagem já foi aberta e lida, ou se somente foi rececionada, mas ainda não foi aberta e lida[265].

Num olhar atento e perspicaz, cumpre-nos agora realçar algumas das principais contribuições do Procurador da República no âmbito da obtenção de prova digital e no que toca aos principais cuidados que devemos ter com a interpretação das leis que temos em vigor. Assim, primeiramente, é realçada a *nuance* perturbadora que os regimes de tratamento de comunicações eletrónicas estão sujeitos. De facto, nem sempre é tecnicamente seguro acolher a perspetiva que determinada mensagem foi rececionada e lida, uma vez que, hoje, o mais leigo

[263] Neste sentido, VERDELHO, Pedro, *"Apreensão de Correio Electrónico..."*, *op. cit.*, pp. 153 e 154.

[264] *Vd* Acórdão do Tribunal da Relação de Lisboa de 15-07-2008, já previamente mencionado.

[265] O autor releva ainda que no que aos anexos que, por exemplo, um *e-mail* possa ter, parece ser de defender que tendo em conta que o anexo (como uma imagem ou uma música) faz parte da própria mensagem, então esse anexo só poderá compreender o mesmo regime da comunicação eletrónica. VERDELHO, Pedro, *"Técnica no Novo C.P.P..."*, *op. cit.*, p. 168.

dos agentes pode muito bem marcar certa e determinada mensagem como "*não lida*" e, posteriormente, esse tipo de comunicação ser alvo de diferente tratamento[266].

Já noutra perspetiva, o autor alerta ainda para a falta de sentido prático e técnico do regime de apreensão de comunicações eletrónicas[267]. Assim, se por exemplo, no decurso de uma busca for encontrado um grande conjunto de telemóveis ou computadores, com *SMS* ou *e-mails*, que se julgue ter relevo probatório (ainda que nem sequer se saiba se as comunicações já foram abertas e lidas), então, de acordo com o regime de apreensão de correspondência, o mais acertado seria o JIC competente emitir uma ordem de apreensão prévia dessas eventuais comunicações, não devendo, por meio de atuação dos OPC, aceder ao conteúdo das comunicações em causa. Todavia, salvo distinto entendimento, não se torna sequer funcional exigir de apenas um JIC a complexa e rigorosa análise de, imaginemos, 50 telemóveis e 50 computadores.

Contudo, não obstante todas as contribuições do Procurador, tendo principal destaque a divisão tripartida no que toca à obtenção de comunicações eletrónicas, o certo é que nem todas as suas opiniões acolheram uma total concordância pela doutrina e jurisprudência portuguesa, sendo talvez a própria divisão tripartida umas das mais debatidas, advogando-se, por um lado, um regime dual de apreensão de comunicações e, por outro, a não aplicação de um regime de comunicações às comunicação eletrónicas abertas e lidas. A título de exemplo, já RITA CASTANHEIRA NEVES referia que "(...) sempre se diga considerar-se desprovida de qualquer lógica aplicar o regime da correspondência a correio eletrónico já aberto e lido, quando nem sequer as próprias cartas gozam desta exacerbada protecção: estas, depois de abertas e lidas, passam automaticamente a ser consideradas normais escritos e não mais correspondência/comunicação"[268].

Pondo de lado as críticas à visão tripartida defendida pelo autor, o certo é que tem sido esta a teoria maioritariamente seguida pela jurisprudência portuguesa[269].

---

[266] Ainda a este propósito, VERDELHO, Pedro, *"Apreensão de Correio Electrónico...", op. cit.*, pp. 159 e 160.

[267] A este propósito, VERDELHO, Pedro, *"Técnica no Novo C.P.P..."*, *op. cit.*, p. 165 e nesse mesmo sentido, *"A obtenção de prova...", op. cit.*, pp. 123 e 124.

[268] Cfr. NEVES, Rita Castanheira, *op. cit.*, p. 152.

[269] A título de exemplo, *vd.* o Acórdão do Tribunal da Relação do Porto de 22-05-2013, com o seguinte sumário: *As mensagens, depois de recebidas, deixam de ter a essência de uma comunicação em transmissão para passarem a ser uma comunicação já recebida, que terá porventura a mesma essência da correspondência, em nada se distinguindo de uma carta remetida por correio físico. Tendo sido já recebidas, se já foram abertas e porventura lidas e mantidas no computador ou no telemóvel, não deverão ter mais protecção que as cartas em papel que são*

3.2. Teoria defendida por BENJAMIM SILVA RODRIGUES

Com uma visão tripartida semelhante, BENJAMIM SILVA RODRIGUES[270] refere que o legislador português não pode apenas ter em atenção que a ingerência nas comunicações eletrónicas implica a lesão da inviolabilidade do sigilo ou segredo das comunicações privadas, art.º 34.º n.º 1 e 4 da CRP, como também pode acarretar a violação do direito à autodeterminação informacional e comunicacional, até chegar à questão que a final se quer ver resolvida, i.e., qual o regime a ser aplicado, enquanto meio de obtenção de prova, às intromissões nas comunicações eletrónicas?

Na verdade, o autor opta por defender que o regime das escutas não se restringe às formas de comunicação oral tendo a sua razão de ser na captação de áudio, mencionando, para o efeito, uma posição atualizada e consequente aplicação do regime das escutas à monitorização de comunicações eletrónicas. Não obstante legitimar a posição tripartida de PEDRO VERDELHO, o autor não sugere a generalização do regime das escutas telefónicas a todo tipo de obtenção de comunicações eletrónicas.

Ora, tal como defende o Procurador da República, o autor também defende a opinião que relativamente à monitorização de comunicações eletrónicas em tempo real se deve aplicar o regime das interceções telefónicas, nos termos do art.º 189.º do CPP.

---

recebidas, abertas ou porventura guardadas numa gaveta, numa pasta ou num arquivo, visto o disposto no art. 194º, n.º 1 do C. Penal. A junção voluntária aos autos feita pela pessoa que recebeu a mensagem, dispensa a intervenção de qualquer autoridade judiciária, designadamente do JIC. Disponível em http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/abf6a7fedb6f7ba580257b88004ed413 [Consultado em 22.10.2017]. E ainda o Acórdão do Tribunal da Relação de Lisboa de 24-09-2013, com o seguinte sumário: *As mensagens electrónicas (sms) deixam de ter a essência de uma comunicação em transmissão para passarem a ser antes uma comunicação já recebida, que terá porventura a mesma essência da correspondência», em nada se distinguindo de uma «carta remetida por correio físico». E tendo sido já recebidas, «se já foram abertas e porventura lidas e mantidas no computador (ou no telemóvel, acrescenta-se) 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», visto o disposto no art.194, nº1, do CP. É o destinatário da correspondência que sobre a mesma tem toda a disponibilidade e não o seu remetente, tendo toda a legitimidade para divulgar o seu conteúdo, nomeadamente autorizar que deste tomassem conhecimento as autoridades policiais.* Disponível em http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/c60dfe830c97cf8980257c0000368afa?OpenDocument [Consultado em 22.10.2017].

[270] A este propósito, RODRIGUES, Benjamim Silva, *Das Escutas Telefónicas...*, *op. cit.*, pp. 434 – 450 e ainda, NEVES, Rita Castanheira, *op. cit.*, p. 154 – 159.

Porém, quanto à segunda hipótese, i.e., às comunicações que já se encontram nos equipamentos dos destinatários, mas que ainda não foram abertas e lidas, BENJAMIM SILVA RODRIGUES defende que se trata de uma comunicação em trânsito, tendo em conta que está dependente de recolha, como tal, também aqui a obtenção de prova digital deve ser regida de acordo com o regime das escutas telefónicas. O autor advoga que tanto no primeiro caso, como no segundo, estamos perante a ingerência nas comunicações privadas dos interlocutores, estando em causa o sigilo das mesmas.

Não obstante, o autor vem defender que se estivermos perante um caso em que a comunicação eletrónica foi, de facto, rececionada, aberta e lida, então não estamos perante um caso de documentos eletrónicos, mas perante um documento detentor de dados pessoais, estando em causa o direito à autodeterminação informacional e comunicacional que requer uma proteção legal adicional, nos termos da Lei n.º 41/2004, de 18 de agosto (Proteção de Dados Pessoais e Privacidade nas Telecomunicações) e da Lei n.º 67/98, de 26 de outubro (Lei da Proteção de Dados Pessoais).

Ora, apesar de o autor fazer esta distinta divisão, em bom rigor, apenas reconduz à obtenção de prova digital dois regimes diversos, tendo por base a abertura da comunicação, no entanto, o mesmo vem sempre defender a autonomização do regime de obtenção de comunicações eletrónicas em processo penal, distante de complexas e incongruentes remissões[271].

3.3. Teoria defendida por MANUEL DA COSTA ANDRADE

Partindo destas noções e considerações, COSTA ANDRADE, após desenhar a importância relativa ao sigilo da correspondência e à confiança da tutela de privacidade à distância e antes de se debruçar na temática de recolha de comunicações eletrónicas, refere um pequeno pormenor que, provavelmente, passou despercebido ao mais atento dos leitores. Assim, o autor refere que o sigilo das comunicações eletrónicas está vinculado apenas ao

[271] Neste sentido, Rita Castanheira, *op. cit.*, p. 159.

processamento de comunicação, dominado pela empresa de telecomunicações, compreendendo o seu conteúdo e circunstâncias processuais. Acresce que, tal como PEDRO VERDELHO explicitou, defende que a comunicação apenas existe no processo de transmissão, ou seja, até ao momento em que a mensagem entra no domínio do recetor[272], como tal julga incompreensível a redação dada pelo legislador português ao art.º 189.º do CPP[273].

Assim, ao contrário da teoria tripartida defendida pelo Procurador da República, este autor vem sugerir que a proteção dada às comunicações eletrónicas só existe até ao momento em que a mensagem é lida e rececionada, sendo que, na mesma ótica de RITA CASTANHEIRA NEVES, defende que após esse momento, o processo de comunicação à distância findou, refutando, de todo, o regime das correspondências previsto no art.º 178.º e ss do CPP. Como tal, podemos afirmar que este autor defende que após um *e-mail*, *SMS*, ou outro tipo de comunicação eletrónica, ter sido rececionado, lido e guardado no dispositivo a que se destina, a comunicação passa a valer como um normal escrito, sujeito ao regime de, por exemplo, uma nota, um documento, ou qualquer ficheiro produzido e arquivado pelo utilizador. Mais uma vez, aqui podemos encontrar outro aspeto divergente entre as duas posições, para já, manifestadas.

De acordo com COSTA ANDRADE, uma vez que vamos encarar as comunicações eletrónicas já abertas e lidas como um documento normal escrito e atendendo ao seu *hiato de perigo*, então tal documento é objeto idóneo de busca (que pode ser operado através de apreensão de computador ou do telemóvel), em sentido tradicional. Segundo ele, isto acontece porque a partir do momento que o destinatário abre e lê a comunicação eletrónica "(...) passa a dispor de meios de autotutela, desde a instalação de sistemas de segurança, programas anti-vírus, codificação críptica, *firewalls* (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"[274].

[272] A este propósito, ANDRADE, Manuel da Costa, *op. cit.*, pp. 158 – 159.

[273] O autor defende e eliminação do art.º 189.º do CPP, tendo em conta que o mesmo sugere a extensão do regime das interceções telefónicas a várias formas de comunicação, afirmando que deveria deixar-se para o âmbito da inviolabilidade das comunicações eletrónicas aquilo que fosse, de facto, inviolável. Neste mesmo sentido NEVES, Rita Castanheira, *op. cit.*, pp. 148 – 150.

[274] Cfr. ANDRADE, Manuel da Costa, *op. cit.*, p. 160.

3.4. Teoria defendida por ROGÉRIO BRAVO

Por seu turno, já numa perspetiva totalmente oposta, ROGÉRIO BRAVO inicia a sua posição[275] com um dilema. Assim, questiona-se se o correio eletrónico guardado num sistema informático de um fornecedor de serviços, ainda não aberto e lido pelo destinatário, deve ser equiparado a correspondência fechada, nos termos do art.º 179.º do CPP, e, como tal, ter de ser o JIC o primeiro a tomar conhecimento do conteúdo de tal comunicação.

Consciente que alguma doutrina é a favor desta equiparação, desde logo, o autor vem enumerar um conjunto de razões que o levam a optar pela não equiparação do correio eletrónico, guardado num sistema informático, à correspondência fechada[276] [277], afirmando que o primeiro não passa de meros dados informáticos armazenados num equipamento eletrónico[278].

Primus, o autor vem defender que na busca do conceito de correspondência em legislações internacionais não é possível de depreender qualquer aplicação do regime de correspondência ao regime das comunicações eletrónicas. Sugere também que a redação do art.º 194.º do CP não parece querer referir-se às comunicações eletrónicas digitais, uma vez que expressões como "encomenda", "carta" e "escrito fechado" são uma constante, sugerindo, unicamente, a correspondência corpórea dita tradicional. Ao contrário da natureza de uma carta, um *e-mail*, por exemplo, nunca está fechado, a não ser que esteja cifrado, a sua eliminação, por

[275] Neste sentido, BRAVO, Rogério, *Idem, ibidem.*

[276] RITA CASTANHEIRA NEVES também vem defender a teoria levada a cabo por este autor, recorrendo um conjunto de razões de ordem técnica e prática que a levam a optar por esta posição, nomeadamente: as comunicações eletrónicas não utilizam redes postais públicas para a sua transmissão, o art.º 179.º do CPP foi desenhado para a apreensão de um objeto físico e palpável (como por exemplo as cartas e encomendas), em termos práticos seria impraticável que o JIC tivesse de ser a primeira pessoa a tomar conhecimento de todas as comunicações eletrónicas, entre outros... Ademais, esta autora vem ainda referir que se às comunicações eletrónicas que ainda não foram abertas e lidas pelo destinatário poderiam existir dúvidas quanto à aplicação do regime de correspondência, no qua toca à correspondência aberta e consequentemente lida, jamais poderíamos reger a obtenção de comunicações eletrónicas através desse regime. Neste mesmo sentido, NEVES, Rita Castanheira, *op. cit.*, pp. 183 – 190.

[277] ARMANDO DIAS RAMOS, através de uma perspetiva obtida "*in locus*" também vem defender a não equiparação do regime das comunicações eletrónicas ao regime do correio tradicional. A título de exemplo, por um lado, o autor vem apontar a banalização do envio automático de *e-mails* e *SMS*, em formato *SPAM*, que se tornaram numa porta para a difusão de *malware* no equipamento eletrónico do destinatário. Neste sentido, RAMOS, Armando Dias, *op. cit.,* pp. 65 e 66.

[278] A este propósito, BRAVO, Rogério, *op. cit.*, p. 3.

exemplo, pode não constituir uma destruição total[279], não circula em ambiente seguro, sendo, na sua essência, uma comunicação imaterial[280].

Secundus, o autor defende que jamais em tempo algum os DLG devem ficar eternamente dependentes da tecnologia. Afirma que, por vezes, o utilizador peca por partir da conjugação de perceções visuais, como por exemplo o facto de o *e-mail* quando se encontra na caixa de entrada exibir uma imagem de uma carta selada que quando é lida deixa de aparecer, caindo na tentação igualar a correspondência dita tradicional ao correio eletrónico. Contudo, como bem sabemos, "(...) maior parte dos programas deixa ao alcance do utilizador a possibilidade de remarcar sem limite de vezes as mensagens já lidas, como estando ainda *"por ler"*"[281].

Nesta sequência, o autor reivindica apenas uma visão bipartida do regime de obtenção de comunicações eletrónicas sendo que o que vem atribuir decisivamente o regime a aplicar é o momento em que a comunicação chega ao local de destino. Deste modo, é defendido que ao primeiro momento, o da comunicação, deve ser aplicado o regime das escutas telefónicas. Por outra banda, no segundo momento, a comunicação eletrónica deve ser equiparada a um normal escrito, não necessitando de proteção acrescida[282]. Independentemente, da teoria defendida, o certo é que também este autor reivindica ao legislador o princípio da legalidade e da tipicidade, solicitando a simplificação definitiva do tema em causa, bem como o indesejável arrastamento deste debate.

3.5. Teoria defendida por RITA CASTANHEIRA NEVES

Ora, tendo por referência a longa arquitetura de um *e-mail* e de uma *SMS*, desde a "caixa de saída" do remetente até à "caixa de entrada" do destinatário, RITA CASTANHEIRA NEVES, por sua vez, vem também defender que este tipo de comunicações pode facilmente ser

[279] Neste mesmíssimo sentido, BRAVO, Rogério, *op. cit.,* pp. 5 e 6 e ainda RODRIGUES, Benjamim Silva, *Das Escutas Telefónicas...*, *op. cit.,* pp. 439 – 441.

[280] BRAVO, Rogério, *op. cit.,* p. 7.

[281] Cfr. BRAVO, Rogério, *Idem, ibidem.*

[282] Neste mesmo sentido, NEVES, Rita Castanheira, *op. cit.*, p. 165.

intercetadas por inúmeros leitores, contudo com algumas ressalvas. Com efeito, a autora também vem sugerir uma visão bipartida do regime de obtenção de comunicações eletrónicas[283], sendo que o primeiro momento se caracteriza por ser o da interceção da comunicação, no entanto, não é uma defensora do alargamento desenfreado do regime das escutas telefónicas, tal como se encontra previsto nos termos do art.º 189.º do CPP...

Desde logo, a autora destaca que o alargamento do regime das interceções telefónicas a outro tipo de comunicações não pode, de todo, ser uma solução, apresentando um conjunto de razões que a levam a optar por um trilho diferente. Deste modo, em primeiro lugar, é defendido que, relativamente à violação dos direitos pessoais, a diferentes tipos de comunicações devem corresponder diferentes graus de intensidade, não sendo o facto de se tratar de um telemóvel, telefone, ou Internet que permite o estabelecimento de regimes distintos. Como tal, a distinção entre regimes não deve surgir pelos instrumentos técnicos que são utilizados, mas antes pela própria comunicação, ou seja, na distinção que é conferida à palavra falada e à palavra escrita. Enquanto a primeira extingue-se no momento em que é proferida, não sendo suposto haver qualquer perpetuação, a segunda já terá um carater imortalizado. Sendo assim, ao regime das interceções telefónicas deve única e simplesmente corresponder a comunicação oral[284]. Ademais, a autora preconiza que uma vez que ao regime das escutas telefónicas corresponde um catálogo de crimes específico, então também deveria existir um catálogo de crimes específico que guiasse a interceção e registo das restantes comunicações eletrónicas[285].

Num primeiro instante, que se estabelece entre o momento em que é enviado o *e-mail* ou *SMS* até à sua abertura e consequente leitura, a autora vem, portanto, defender a aplicação de um regime autónomo de interceções de comunicações eletrónicas e não uma extensão do regime das interceções telefónicas, com vista a captar o próprio conteúdo da mensagem[286]. Ademais, a autora vem ainda acrescentar que, à semelhança do regime das escutas, este regime autónomo também será suscetível de:

1) despacho judicial de autorização;

[283] Neste sentido, NEVES, Rita Castanheira, *op. cit.*, pp. 172 – 183.

[284] Uma outra razão, apontada pela autora, que leva a que palavra falada se distinga da escrita deve-se ao facto de a primeira ter uma maior capacidade em perturbar a vida privada de um indivíduo, apesar de não sermos da mesma opinião. Veja-se, NEVES, Rita Castanheira, *op. cit.*, p. 176.

[285] NEVES, Rita Castanheira, *op. cit.*, p. 174.

[286] Refira-se que, em alguns casos, nem sempre o conteúdo da comunicação se revela o ponto mais significativo da investigação, mas antes os dados relativos às mesmas que possam ajudar a captar a "movimentação" do arguido.

2) controlo judicial;
3) catálogo de crimes específicos;
4) limitação máxima de duração;
5) lógica de subsidiariedade e proporcionalidade com a causa.

Por outro lado, a autora advoga que caso a comunicação já tenha sido aberta e lida deve ser tratada como um simples ficheiro em formato digital que pode ser buscado/gravado, e/ou apreendido para posterior análise em laboratórios especializados. "De comunicação passa a ser ficheiro. De interceptável passa a ser buscada (...)"[287]. Como tal, aquilo que distingue o regime a aplicar será unicamente a abertura e leitura da mensagem em causa. Não obstante, é preconizado que não devemos fazer uma análise semelhante a todo o tipo de comunicações eletrónicas que tenham sido abertas e lidas, uma vez que podemos estar perante comunicações que por especiais razões de proteção jurídica se imponha uma eventual tutela acrescida de confidencialidade[288].

3.6. Teoria defendida por ARMANDO DIAS RAMOS

Tendo por referência as doutrinas *supra* referenciadas e ainda o conhecimento e experiência profissional adquirida no terreno em mais de 15 anos, este autor vem, de facto, dar um contributo muito mais prático no que à obtenção de comunicações eletrónicas diz respeito. Assim, em primeiro lugar, desde logo, é afirmado por este autor que à falta de um regime específico que venha regular aquele tipo de comunicação que se inicia "(...) quando o destinatário faz "send" (enviar) e termina o seu trajeto quando chega ao servidor de correio eletrónico ou ao terminal do destinatário"[289], a melhor opção passa mesmo pela extensão do regime da interceção e gravação das escutas telefónicas, caso contrário ficaríamos com um vazio legislativo.

[287] Cfr. NEVES, Rita Castanheira, *op. cit.*, p. 183.

[288] A este propósito, NEVES, Rita Castanheira, *op. cit.*, p. 171.

[289] Cfr. RAMOS, Armando Dias, *op. cit.,* p. 59.

Contudo, por outra banda, e tal como já podemos referenciar, ainda que em nota de rodapé, o autor vem defender que o legislador com a LCiber veio, infelizmente, aplicar a duas realidades distintas a mesma realidade[290]. Constata-se, portanto, que o autor é absolutamente contra a reflexão da imagem das comunicações eletrónicas no regime do correio tradicional muito também por causa da dificuldade de asseverar com rigor quando é que uma comunicação eletrónica foi, de facto, lida e o diferente tratamento concedido à correspondência aberta e lida, da não aberta e não lida. Como já tivemos oportunidade de referir, com a nova realidade informática, nada é claro, nada é 100% certo, podendo o mais leigo dos agentes marcar certa mensagem como "não lida", mesmo após ter sido lida e, por isso, alterar todo o regime de obtenção de prova.

Ora, após uma longa reflexão e constantes paralelismos entre diferentes ordenamentos jurídicos, o autor vem perseverantemente defender a posição levada a cabo pelo ordenamento jurídico alemão, ou seja, vem refletir a teoria que o segredo das comunicações eletrónicas apenas terá guarida aquando do seu trânsito, sendo que, por outro lado, i.e., quando a mensagem já se encontrar no poder do destinatário, a apreensão processar-se-á como se tratasse de um mero documento em formato digital, não havendo qualquer distinção entre comunicações "lidas" ou "não lidas"[291].

4. Será que a LCiber veio revogar o regime processual relativo à obtenção de prova digital constante no CPP?

Tal como DÁ MESQUITA alerta, no âmbito do direito probatório, são realçados os problemas suscitados pela desmaterialização eletrónica, bem como a necessidade de articulação das perspetivas político-criminais com a nova realidade informática, considerando, como já tivemos oportunidade de mencionar, a reforma de 2007 e posterior revisão de 2009 do CPP como oportunidades perdidas para se satisfazer as exigências estimuladas pelos novos sistemas informáticos. A título de exemplo, nas palavras do autor, as referências previstas no art.º 189.º

[290] Neste sentido, RAMOS, Armando Dias, *op. cit.,* p. 56.

[291] A este propósito, RAMOS, Armando Dias, *op. cit.,* pp. 81 – 89.

do CPP vieram unicamente criar indesejáveis e desnecessárias querelas, já que misturam realidades opostas que não se reportam aos universos plasmados e que, por isso, com a adaptação da Convenção do Cibercrime ao direito português deveriam ter sido revistas e alteradas.

Assim, e tal como mencionamos previamente no segundo capítulo, cumpre agora fazer uma breve análise dos artigos 17.º e 18.º da LCiber, atendendo à sua utilidade na apreensão e interceção de comunicações eletrónicas. Deste modo, retomando o nosso trajeto no art.º 17.º, é constatável que o legislador pretendeu transpor para o ambiente digital o regime de apreensão de correspondência previsto no CPP, contudo fê-lo de modo a levantar inúmeros dilemas e incertezas. Desde logo, a título de exemplo, PEDRO VERDELHO[292] levanta a eterna questão da necessidade da exigência prévia de despacho judicial ordenando a apreensão de comunicações eletrónicas, na sequência do art.º 179.º do CPP. Por seu turno, atento às necessidades da vida prática[293], o Procurador defende que a única imposição legal para a apreensão de comunicações eletrónicas prende-se unicamente com a existência de uma forma legítima de acesso ao meio informático em que as mensagens estavam guardadas, contudo ressalva que esta apreensão terá unicamente caráter provisório, uma vez que caso o juiz pretenda a apreensão das mensagens em causa, deverá autorizá-las previamente, devendo, em caso contrário, ser devolvidas ou destruídas. Por outra banda, VERDELHO também chega a pronunciar-se sobre a necessidade de o JIC ser o primeiro a tomar conhecimento das comunicações eletrónicas aproveitando, desde logo, para defender a extensão conferida ao art.º 252.º n.º 2 e 3 do CPP[294], defendendo, por isso, a apreensão provisória de comunicações sem autorização judicial prévia. A título de nota final, PEDRO VERDELHO sugere que o art.º 17.º da LCiber deverá aplicar-se, com

[292] Neste sentido, VERDELHO, Pedro, *"A nova Lei do Cibercrime...", op. cit.*, p. 743.

[293] O autor defende que antes de, por exemplo, uma busca não sabemos se vamos encontrar um computador ou telemóvel e se esses equipamentos estarão munidos de comunicações eletrónicas relevantes para a investigação criminal. Portanto, torna-se impraticável que na vida real seja necessária a obtenção de autorização para a possibilidade de encontrarmos estes terminais com estas características, em qualquer tipo de busca. Neste mesmíssimo sentido, VERDELHO, Pedro, *"A nova Lei do Cibercrime...", op. cit.*, p. 744.

[294] Artigo 252.º - Apreensão de correspondência

2 - Tratando-se de encomendas ou valores fechados suscetíveis de serem apreendidos, sempre que tiverem fundadas razões para crer que eles podem conter informações úteis à investigação de um crime ou conduzir à sua descoberta, e que podem perder-se em caso de demora, os órgãos de polícia criminal informam do facto, pelo meio mais rápido, o juiz, o qual pode autorizar a sua abertura imediata.

3 - Verificadas as razões referidas no número anterior, os órgãos de polícia criminal podem ordenar a suspensão da remessa de qualquer correspondência nas estações de correios e de telecomunicações. Se, no prazo de quarenta e oito horas, a ordem não for convalidada por despacho fundamentado do juiz, a correspondência é remetida ao destinatário.

as adaptações necessárias, ao regime de apreensão do art.º 179.º do CPP, tal como é regido pelo próprio preceito legal[295].

Por seu turno, no art.º 18.º da LCiber é consagrada a possibilidade de interceção de comunicações, mecanismo este que há muito se encontra consagrado no CPP, mais concretamente no art.º 189.º, onde podemos constatar a extensão do regime das comunicações telefónicas a outro tipo de comunicações. Porém, a extensão prevista no art.º 189.º já desde há algum tempo que não tem grande viabilidade prática quanto aos crimes informáticos, tendo em conta que estes últimos nem sequer se encontram incluídos no catálogo de crimes em relação aos quais é permitido proceder à interceção telefónica. No fundo, o art.º 18.º veio consagrar um regime especial permitindo, desta forma, o enquadramento legal da realização de interceções de comunicações aquando da investigação de crimes informáticos, em tempo real[296].

Ora, cumpre finalmente a título de despedida do presente capítulo desvendar se, no nosso ponto de vista, somos a favor ou contra a revogação da extensão conferida aos artigos referentes à obtenção de prova digital constantes no CPP. Assim, antes de darmos aquele que será o nosso último contributo, cumpre fazer um pequeno apontamento das mais elementares aulas do curso de Direito. Como bem sabemos, perante um conflito de normas e como explicita o art.º 7.º do CC[297], as estatuições especiais prevalecerão sobre as gerais, *lex specialis derogat legi generali*. Nesta sequência, desde já podemos afirmar que tratando-se de uma matéria controversa, a doutrina não se revela uníssona, como tal a resposta não é simples, nem sequer se esperaria que assim fosse.

Deste modo, em primeiro lugar, é constatável que em momento algum é possível afirmar com clareza que a LCiber veio revogar os meios de obtenção de prova digital previstos

---

[295] A este propósito, VERDELHO, Pedro, *"A nova Lei do Cibercrime..."*, *op. cit.*, p. 745 e ainda, por exemplo, o facto de não se pretender que a correspondência abranja unicamente os crimes puníveis com pena de prisão superior a três anos, NEVES, Rita Castanheira, *op. cit.*, pp. 274 e 275.

[296] Ainda neste sentido, VERDELHO, Pedro, *"A nova Lei do Cibercrime..."*, *op. cit.*, p. 746 e *a contrario*, VENÂNCIO, Pedro Dias, *Lei do Cibercrime...*, *op. cit.,* pp. 119 e 120.

[297] Artigo 7.º- Cessação da vigência da lei

1 - Quando se não destine a ter vigência temporária, a lei só deixa de vigorar se for revogada por outra lei.

2 - A revogação pode resultar de declaração expressa, da incompatibilidade entre as novas disposições e as regras precedentes ou da circunstância de a nova lei regular toda a matéria da lei anterior.

3 - A lei geral não revoga a lei especial, excepto se outra for a intenção inequívoca do legislador.

4 - A revogação da lei revogatória não importa o renascimento da lei que esta revogara.

no CPP uma vez que, a lei, somente é clara no que toca à revogação expressa da Lei da Criminalidade Informática.

Contudo, sem quaisquer demoras, PAULO DÁ MESQUITA vem apontar o art.º 17.º da LCiber como o ponto de partida da revogação de algumas implicações do regime previsto no CPP, tendo em conta que a apreensão de correio eletrónico e registos de comunicações de natureza semelhante passou a ser diretamente regulada por este preceito. Por seu turno, CASTANHEIRA NEVES[298] vem indicar a possibilidade obtenção de comunicações eletrónicas cujo crime em causa esteja p. e p. na LCiber. Contudo, salvo douto entendimento, não obstante a norma prevista na LCiber regular a apreensão de comunicações eletrónicas, a doutrina não tem vindo a considerar a revogação do art.º 179.º do CPP, tendo em conta que, a nosso ver, este preceito não tem como sua génese um regime puramente extensivo da apreensão de correspondência. Todavia, a mesma realidade já não se reflete no âmbito do regime de extensão previsto no art.º 189.º do CPP que, por sua vez, tendo vindo a dar lugar a extensos e longos debates doutrinais.

Assim, por um lado, PEDRO VERDELHO vem defender a não revogação do regime que resulta do art.º 189.º do CPP afirmando, para sua defesa, que a LCiber apenas procedeu "(...) à instituição de um regime especial, destinado a ser aplicado em casos específicos, como resulta do respetivo art.º 11.º(...)"[299]. Sucede que, não nos parece que este deverá ser o caminho trilhado, tendo em conta a máxima *supra* mencionada, no que ao conflito de normas diz respeito. Ainda no mesmo sentido, PAULO PINTO DE ALBUQUERQUE[300], por sua vez, vem defender a não revogação do art.º 189.º do CPP, por força do art.º 18.º da LCiber, muito porque este último artigo prevê unicamente a interceção de comunicações para prova de crimes previstos na lei especial, ou para a prova de crimes previstos no art.º 187.º do CPP. Assim, o autor alerta que mesmo com a LCiber o juiz não pode ordenar a interceção de comunicações eletrónicas para a prova de crimes de injúrias, difamações, ou ameaças porque não se encontram plasmados nem no art.º 11.º da LCiber, nem sequer no art.º 187.º do CPP.

Por outra banda, PAULO DÁ MESQUITA vem, desde logo, defender uma revogação parcial do art.º 189.º do CPP, tendo em conta que este preceito legal deverá unicamente ser

---

[298] NEVES, Rita Castanheira, *op. cit.*, p. 274.

[299] Cfr. VERDELHO, Pedro, *"A nova Lei do Cibercrime..."*, *Idem, ibidem*.

[300] Com razão, ALBUQUERQUE, Paulo Pinto de, *Comentário do Código de Processo Penal: à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem*, 4ª edição, Lisboa, Universidade Católica Editora, abril 2011, p. 549.

aplicado "(...) à interceptação das comunicações entre presentes e outros meios à distância que não constituem comunicações electrónicas ou transmissão de dados informáticos"[301], uma vez que a LCiber é detentora de disposições processuais específicas para a apreensão e interceção de comunicações eletrónicas. Dúvidas não podem subsistir aquando do teor do art.º 18.º da LCiber[302], mais concretamente o seu n.º 4, no qual é sublinhado que os regimes dos artigos 187.º, 188.º e 190.º do CPP são aplicados em tudo que não for contrariado pelo art.º 18.º. Acresce ainda que, RITA CASTANHEIRA NEVES vem sugerir o vazio do âmbito de aplicação do art.º 189.º do CPP, tendo em atenção à complexa regulação do art.º 18.º da LCiber[303].

Ora, pese embora a natureza esquizofrénica da LCiber[304] e apesar de não ser do entendimento geral da doutrina a revogação do artigo 189.º n.º 1 do CPP, no que às telecomunicações, recolha de prova eletrónica e crimes informáticos diga respeito, como tivemos oportunidade de referir, de facto o mesmo deixa de ter aplicabilidade prática com a exaustiva regulação do art.º 18.º da LCiber, sendo este o principal preceito de referência para os OPC em matéria de recolha de prova digital. E neste ponto assenta a jurisprudência[305] e, portanto, somos

---

[301] Cfr. MESQUITA, Paulo Dá, *op. cit.* p. 103.

[302] Artigo 18.º - Interceção de comunicações

1 - É admissível o recurso à interceção de comunicações em processos relativos a 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 eletrónico, quando tais crimes se encontrem previstos no artigo 187.º do Código de Processo Penal.

2 - A interceção e o registo de transmissões de dados informáticos só podem ser autorizados durante o inquérito, 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, por despacho fundamentado do juiz de instrução e mediante requerimento do Ministério Público.

3 - A interceção pode destinar-se ao registo de dados relativos ao conteúdo das comunicações ou visar apenas a recolha e registo de dados de tráfego, devendo o despacho referido no número anterior especificar o respetivo âmbito, de acordo com as necessidades concretas da investigação.

4 - Em tudo o que não for contrariado pelo presente artigo, à interceção e registo de transmissões de dados informáticos é aplicável o regime da interceção e gravação de conversações ou comunicações telefónicas constante dos artigos 187.º, 188.º e 190.º do Código de Processo Penal.

[303] A este propósito, NEVES, Rita Castanheira, *op. cit.*, p. 280.

[304] Neste sentido, MESQUITA, Paulo Dá, *op. cit.* p. 97.

[305] Acórdão do Tribunal da Relação de Évora de 06-01-2015, com o seguinte sumário: *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 eletrónicas", "crimes informáticos" e "recolha de prova eletrónica". A pretensão do legislador (quer o nacional quer o da Convenção de Budapeste sobre o Cibercrime) é o de alargar o âmbito da aplicação da lei até onde haja necessidade de fazer prova com o conteúdo existente em qualquer "sistema informático". Do artigo 11º da Lei n. 109/2009 resulta evidente que as normas contidas nos artigos 12º a 17º da supramencionada Lei contêm um completo regime processual penal para os crimes que, nos termos das alíneas do n. 1 do artigo 11º, estão previstos na lei nº 109/2009, são ou foram cometidos por meio de um sistema informático ou em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico. Mas coexistem dois regimes processuais na Lei n. 109/2009: o regime dos artigos 11º a 17º da dita Lei; o regime dos artigos 18º e 19º do mesmo diploma. Podemos, portanto, caracterizar o regime processual especial dos artigos 11º a 17º como o regime processual "geral" do cibercrime e da prova eletrónica. Isto porquanto existe um segundo catálogo na Lei n. 109/2009, o do*

do entendimento que, pelo menos, atendendo ao pequeno campo de aplicação que o art.º 189.º do CPP ficou confinado, no que toca à obtenção de prova digital, deve considerar-se o artigo 189.º n.º 1 do CPP parcialmente revogado.

artigo 18º, n. 1 do mesmo diploma a que corresponde um segundo regime processual de autorização e regulação probatória. O artigo 18º, n. 1 da Lei 19/2009, exclui daquele novo sistema "geral" de autorização e acesso probatório relativamente aos crimes (a) nela previstos ou (b) cometidos por meio de um sistema informático ou em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico, quando tais crimes se encontrem previstos no artigo 187.º do Código de Processo Penal, desde que (em ambos os casos) esteja em causa a interceção de comunicações. Nestes casos aplica-se, por remissão do n. 4 do artigo 18º da Lei 109/2009, o regime previsto nos artigos 187º, 188º e 190º do Código de Processo Penal, no que constitui uma remissão expressa que substitui o regime de extensão previsto no artigo 189º do Código de Processo Penal. O elemento distintivo entre os regimes processuais contidos nos artigos 11º a 17º da Lei n. 109/2009 e o regime previsto no artigo 18º da mesma é, portanto, o conceito de "interceção em tempo real de comunicações", sendo que esta interceção pode abranger os dados de tráfego e de conteúdo. (...) O catálogo de crimes mais restritivo do artigo 187º do Código de Processo Penal apenas é aplicável havendo "interceção de comunicações" e apenas nos casos dos crimes previstos na al. b) do artigo 18º. O artigo 189º do Código de Processo Penal nunca é aplicável a crimes informáticos, seja qual for o catálogo aplicável. Disponível em http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/847dae6b85353cb880257de10056ff4c?OpenDocument [Consultado em 25.08.2017]. Ainda neste sentido, Acórdão do Tribunal da Relação de Évora de 20-01-2015, disponível em http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/2fbdd21285478f5f80257de10056ff7a?OpenDocument [Consultado em 25.08.2017].

CONCLUSÃO

Chegado o momento de conclusão da presente dissertação, começamos por sublinhar o óbvio, i.e., que o estudo sobre os meios de obtenção de prova digital, nomeadamente, o regime jurídico dos serviços de correio eletrónico e de mensagens curtas não se encontrar, de facto, vertido sem levantar quaisquer dúvidas interpretativas na legislação portuguesa. As dificuldades sentidas pelos juristas em compreenderem matérias completamente diferentes da ciência do Direito, aliadas aos "espaços deixados em branco" pelo legislador e atual "complexa teia legislativa" sobre os meios de obtenção de prova, em particular o regime jurídico dos *e-mails* e das *SMS*, simplesmente reflete a necessidade de readaptação do Direito a uma realidade muito mais rica, obscura e complexa, como a odisseia digital.

Neste contexto, iniciamos a exposição crítica da temática que nos dispusemos a dissecar com as mais elementares averiguações que refletiram as diferenças entre a prova, os meios de prova e os meios de obtenção de prova. Metaforicamente, podemos exemplificar a prova como sendo o objetivo que se pretende alcançar, o meio de prova como "o caminho" que as entidades competentes têm de percorrer para alcançar a real prova, e o meio de obtenção de prova como o instrumento utilizado pelas autoridades judiciárias na investigação e recolha da prova. Por outro lado, ainda averiguamos as dificuldades sentidas na obtenção de um tipo de prova imaterial, sendo este o seu principal traço distintivo que justifica uma especial adaptação, manuseamento e novidade em sede da sua obtenção, uma vez que a realidade informático-criminal representa hoje uma razoável parcela dos crimes investigados em território nacional. Não obstante o suporte no qual a prova digital se encontra armazenada, bem como todas as suas especificidades, o certo é que a reforma do CPP de 2007 simplesmente referenciou a esta realidade o regime de interceção de comunicações, não conseguindo empurrar o legislador para novos e inovadores meios de obtenção de prova.

Grande relevo foi dado ao Cibercrime, à sua definição e à sua consagração legislativa refletida no Código Penal, no Código de Processo Penal, na Convenção do Conselho da Europa sobre a Cibercriminalidade, na Lei do Cibercrime e, ainda, em menor dimensão e com diferente

natureza, na Lei da Conservação de Dados Gerados ou Tratados no Contexto Oferta de Serviços de Comunicações Eletrónicas. Foi despidos de preconceitos que tentamos precisar realidades que apesar de próximas, refletem noções totalmente opostas, não fosse então necessário fazer um breve esclarecimento entre, por exemplo, *vírus* e *malware*, ou até mesmo diferenciar um *hacker* de um *cracker*.

A nível informático, do que vimos, tantos os *e-mails* como as mensagens curtas são detentores de uma complexa e eficiente arquitetura de serviços, podendo não só ser meios que auxiliam a prática de um crime, como também podem ser vistos como uma realidade ofendida. Constatamos que apesar da tecnologia de ponta existente aparentar a receção automática de um *e-mail* ou uma *SMS* pelo destinatário, de facto, a comunicação eletrónica ainda tem um pequeno percurso a percorrer na arquitetura dos seus serviços, não sendo, por isso, tão instantânea quanto aparenta. Não obstante a *ciberignorância* de alguns, não podemos deixar de afirmar que hoje já podemos observar algumas decisões dos tribunais superiores acerca deste tipo de matérias.

Concluímos esta viagem com um problema que qualquer interpretador do Direito se depara assim que pretenda estudar a presente temática, ou seja, a complexa rede de legislação em volta do cibercrime que convida apenas a inúteis querelas interpretativas, sem qualquer critério de coordenação, contribuindo para uma ineficaz investigação e consequente injustiça[306]. Concordamos, sem dúvida, com o lapidar dizer de JOÃO CONDE CORREIA[307] quando menciona que as leis do cibercrime são "(...) más leis e são insuficientes, estando na hora de ser alteradas. A experiência e o conhecimento adquiridos já permitem superar as suas deficiências e criar um sistema que, sem esquecer o nível ideal de proteção dos direitos fundamentais, contribua para a eficácia da justiça penal." Distinguimos ainda o regime de apreensão e interceção de comunicações, não deixando de referir quais os seus requisitos legais e consequências para a violação dos mesmos.

Foi face a esta encruzilhada legislativa que provavelmente nasceu uma das maiores batalhas doutrinais, em sede de investigação cibercriminal, mais concretamente no âmbito das comunicações eletrónicas. Deste modo, no que à apreensão e interceção deste tipo de comunicações diz respeito, ousamos expor a nossa convicção no sentido de que o segredo das

[306] Para melhor desenvolvimento, CORREIA, João Conde, *"Prova Digital...", op. cit.*, p. 59.

[307] Cfr. CORREIA, João Conde, *"Prova Digital...", Idem, ibidem*.

comunicações eletrónicas não deve acolher três momentos de "vida", mas apenas deverá refletir-se em dois momentos. Assim, uma comunicação apenas deverá ter guarida aquando do seu trânsito, sendo que, por outro lado, ou seja, quando a mensagem se encontrar no poder do seu destinatário, a apreensão dessa comunicação será processada como se tratasse de um mero documento em formato digital. Seguindo, desta forma, as palavras de ARMANDO DIAS RAMOS onde deixamos de lado todos os problemas que podem surgir com o advento informático, como por exemplo, o marcar uma mensagem como "não lida", quando, de facto, já a lemos, ou até mesmo o facto de podermos guardar mensagens num disco externo, quando ainda nem sequer foram abertas. Cremos que, com a posição adotada, não mais se assistiria a constrangimentos em sede de investigação, ultrapassando, desta forma, todas as fobias que, em regra, os juristas padecem aquando do envolvimento com esta área, optando por um tratamento igual, daquilo que é igual, e um tratamento diferente, daquilo que é diferente, na medida da sua diferença, não havendo lugar a "analogias cegas" entre os regimes de comunicações eletrónicas, da correspondência tradicional e das escutas telefónicas. Por fim, ainda asseveramos que face a um regime tão esquizofrénico como aquele sobre o qual nos dispusemos a estudar, somos do entendimento que a LCiber não veio revogar todas as consagrações relativas aos meios de obtenção de prova previstos no CPP, contudo, atendendo ao pequeno campo de aplicação que o art.º 189.º do CPP ficou confinado, no que toca à obtenção de prova digital, o mesmo deverá considerar-se parcialmente revogado.

Aproveitando para fazer uma pequena analogia a outros ordenamentos jurídico-processuais[308], salvo douto entendimento por posição diversa, somos da opinião que o legislador português deveria acrescentar um Capítulo V aos meios de obtenção de prova que já se encontram previstos no atual CPP, contendo um regime muito mais amplo e descritivo face às novas realidades digitais, em vez de conter um regime de extensão (ou de legislação avulsa) que em nada auxilia a investigação e aqueles que têm como função decidir uma causa[309].

[308] A título meramente exemplificativo, o Código de Processo Penal Espanhol, também conhecido por "Ley de Enjuiciamiento Criminal", voltado para as realidades práticas existentes e consciente da atenção solicitada em sede de comunicações eletrónicas, recentemente, optou por consagrar um regime livre de tensões desnecessárias e rico em modalidades de investigação tecnológica, aquando da obtenção de prova. Para mais desenvolvimentos aconselhamos vivamente a leitura de LAINZ, José Luis Rodríguez, *El Secreto de las Telecomunicaciones y su Interceptación Legal: Adaptado a la Ley Orgánica 13/2015, de reforma de la Ley de Enjuiciamiento Criminal,* Madrid, Sepin, 2016, pp. 73 – 77.

[309] PAULO DÁ MESQUITA chega mesmo a sugerir que o capítulo III da LCiber deve ser interpretado como um envergonhado ou escondido novo capítulo V do CPP. Veja-se MESQUITA, Paulo Dá, *op. cit.* p. 101.

É com a sensação que muito mais havia para se dizer que, finalmente, só poderíamos concluir que o ficar preso às amarras do passado simplesmente se traduz como um dos principais erros do processo penal português. Urge que não só o Direito, mas também os órgãos de polícia criminal, o Ministério Público, os Magistrados e os advogados em geral se saibam adaptar à cibercriminalidade e à nova odisseia digital, até porque só assim é que poderemos punir os cibercriminosos e restabelecer a confiança que os agentes reclamam em sede das NTIC. Certo é que almejávamos muito mais e que esta viagem se revelou bem mais árdua do que o expectado, mas a exiguidade da presente dissertação obriga-nos a deixar tal estudo para *quiçá* um momento posterior.

BIBLIOGRAFIA

ACKER, Amelia, "*The Short Message Service: Standards, infrastructure and innovation*", Telematics and Informatics, Volume 31, Issue 4, Pittsburgh, University of Pittsburgh, January 2014, pp. 559 – 568.

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 Figueiredo Dias, por ocasião dos 20 anos do Código de Processo Penal Português, Coord. MÁRIO FERREIRA MONTE, Trad. INÊS FERNANDES GODINHO, Coimbra, Coimbra Editora, 2009, pp. 725-743, ISBN 978-972-32-1657-8.

ALBUQUERQUE, Paulo Pinto de, *Comentário do Código de Processo Penal: à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem*, 4ª edição, Lisboa, Universidade Católica Editora, abril 2011, ISBN 978-972-54-0295-5.

ANDRADE, Manuel da Costa, *"Bruscamente no Verão Passado", a Reforma do Código de Processo Penal: Observações Críticas sobre uma Lei que podia e devia ter sido diferente*, Coimbra, Coimbra Editora, julho 2009, ISBN 978-972-32-1726-1.

ANTUNES, Maria João, *Direito Processual Penal*, Coimbra, Almedina, abril 2016, ISBN 978-972-40-6558-8.

AMARAL, Maria Lúcia, *A Forma da República – Uma Introdução ao Estudo do Direito Constitucional*, Reimpressão, Coimbra, Coimbra Editora, outubro 2012, ISBN 978-972-32-2103-9.

ASCENSÃO, José Oliveira, *"Criminalidade Informática"*, Direito da Sociedade da Informação – Volume II, FDUL – Faculdade de Direito da Universidade de Lisboa / APDI – Associação Portuguesa de Direito Intelectual, Coimbra, Coimbra Editora, 2001, pp. 203 – 228, ISBN 972-32-0994-2.

_____*Estudos sobre Direito da Internet e da Sociedade de Informação*, Coimbra, Almedina, 2001, ISBN 978-972-40-1501-9;

BRAVO, Rogério, *"Da não equiparação do correio-electrónico ao conceito tradicional de correspondência por carta"*, Polícia e Justiça, Revista do Instituto Superior de Polícia Judiciária e de Ciências Criminais, III Série, n.º 7, Coimbra, Coimbra Editora, janeiro – junho 2006, pp. 1 – 8.

CANOTILHO, J. J. Gomes e MOREIRA, Vital, *Fundamentos da Constituição*, Coimbra, Coimbra Editora, novembro 1991, ISBN 972-32-0474-6.

CASABONA, Carlos María Romeo, *"La protección penal de los mensajes de correo electrónico y de otras comunicaciones de carácter personal a través de Internet"*, Derecho y Conocimiento, Vol. 2, 2002, pp. 123 – 149.

CORREIA, João Conde, *"Qual o significado de Abusiva Intromissão na Vida Privada, no Domicílio, na Correspondência e nas Telecomunicações (art. 32.º, n.º 8, 2ª parte da C.R.P.)?"*, Revista do Ministério Público, Ano 20.º, n.º 79, julho-setembro, 1999, pp. 45 – 67.

_____ *"Prova Digital: as leis que temos e a lei que devíamos ter"*, Revista do Ministério Público, Ano 35.º, nº 139, Julho-Setembro, 2014, pp. 29 – 59.

COSTA, José de Faria, *"As Telecomunicações e a Privacidade: O Olhar (In)Discreto de um Penalista"*, As telecomunicações e o Direito na Sociedade da Informação, Faculdade de Direito da Universidade de Coimbra, Instituto Jurídico da Comunicação, 1999, p. 49 – 78, ISBN 972-98462-0-0.

_____ *"Sobre o objecto de protecção do direito penal: o lugar do bem jurídico na doutrina de um direito penal não iliberal"*, Revista de Legislação e de Jurisprudência, ano 142.º, n.º 3978, janeiro-fevereiro 2013, Coimbra, Coimbra Editora, pp. 158 – 173.

_____*Noções Fundamentais De Direito Penal: (Fragmenta Iuris Poenalis): Introdução – A Doutrina Geral Da Infração [A Ordenação Fundamental Da Conduta (Facto) Punível; A Conduta Típica (O Tipo); A Conduta Ilícita (O Ilícito); A Conduta Culposa (A Culpa)]*, 4ª Edição, Coimbra, Coimbra Editora, setembro 2015, ISBN 978-972-32-2328-6.

DIAS, Jorge de Figueiredo, *Clássicos Jurídicos – Direito Processual Penal* (Reimpressão da 1ª Edição de 1974), Coimbra, Coimbra Editora, junho 2004, ISBN 972-32-1250-1.

_____*Direito Penal - Parte Geral – Tomo I – Questões Fundamentais; A Doutrina Geral do Crime*, 2.ª Edição - 2.ª Reimpressão, Coimbra, Coimbra Editora, outubro 2012, ISBN 978-972-32-2108-4.

FREITAS, Pedro Miguel Fernandes, *Determinação da medida da pena privativa de liberdade: um olhar crítico a partir do direito anglo-saxónico*, Braga, Universidade do Minho – Escola de Direito, setembro 2015.

GONÇALVES, Joana Margarida Andrade, *Pharming: Análise dogmático-penal, em especial enquanto forma de lesão do património*, Braga, Universidade do Minho – Escola de Direito, outubro 2015.

GONÇALVES, Pedro, *Direito das Telecomunicações*, Coimbra, Almedina, 1999, ISBN 972-40-1186-0.

JEYA, R. e AMUTHA, Dr. B., "*Wireless Generations – a Survey*", International Journal of Pure and Applied Mathematics, Volume 115, No. 6, Sofia: Academic Publications, 2017, pp. 427 – 435.

JESUS, Francisco Marcolino, *Os Meios De Obtenção Da Prova Em Processo Penal*, 2ª edição rev., at. e amp, Coimbra, Almedina, março 2015, ISBN 978-972-40-5874-0.

LAINZ, José Luis Rodríguez, *El Secreto de las Telecomunicaciones y su Interceptación Legal: Adaptado a la Ley Orgánica 13/2015, de reforma de la Ley de Enjuiciamiento Criminal*, Madrid, Sepin, 2016, ISBN 978-84-16521-45-6.

LEITÃO, Adelaide Menezes, *"Metatags e Correio Electrónico entre os Novos Problemas do Direito da Internet"*, Direito da Sociedade da Informação – Volume IV, APDI – Associação Portuguesa de Direito Intelectual, Coimbra, Coimbra Editora, 2003, pp. 405 – 431, ISBN 972-32-1169-6.

LEITÃO, Luís Menezes, *"A Distribuição de Mensagens de Correio Eletrónico Indesejadas (SPAM)"*, Direito da Sociedade da Informação – Volume IV, APDI – Associação Portuguesa de Direito Intelectual, Coimbra, Coimbra Editora, 2003, pp. 191 – 213, ISBN 972-32-1169-6.

MACEDO, João Carlos Cruz Barbosa, *"Algumas considerações acerca dos crimes informáticos em Portugal"*, Direito Penal Hoje – Novos desafios e novas respostas, Organiz. MANUEL DA COSTA ANDRADE e RITA CASTANHEIRA NEVES, Coimbra, Coimbra Editora, 2009, pp. 221 – 262, ISBN 978-972-32-1692-9.

MARTINS, António Gomes Lourenço / MARQUES, J. A. Garcia / DIAS, Pedro Simões, *Cyberlaw em Portugal – O Direito das Tecnologias da Informação e Comunicação*, Famalicão, Edições Centro Atlântico, 2004, ISBN 972-8426-95-X.

MARTINS, António Gomes Lourenço, *"Criminalidade Informática"*, Direito da Sociedade da Informação – Volume IV, APDI – Associação Portuguesa de Direito Intelectual, Coimbra, Coimbra Editora, 2003, pp. 9 – 41, ISBN 972-32-1169-6.

MEDANI, *et al, "Review of mobile short message service security issues and techniques towards the solution"*, Scientific Research and Essays Vol. 6(6), March 2011, pp. 1147 – 1165.

MESQUITA, Paulo Dá, *Processo Penal, Prova e Sistema Judiciário*, Coimbra, Coimbra Editora, 2010, ISBN 978-972-32-1842-8.

MILITÃO, Renato Lopes, "A Propósito da Prova Digital no Processo Penal", Revista da Ordem dos Advogados – ROA, 2012 (Ano 72), nº 1, pp. 247 – 285.

MONTE, Mário Ferreira, *Direito Processual Penal Aplicado*, Braga, AEDUM – Associação de Estudantes de Direito da Universidade do Minho, 2017, ISBN 978-989-95963-9-9.

MONTE, Mário Ferreira e LOUREIRO Flávia Noversa, *Direito Processual Penal – Roteiro de Aulas*, 2.ª ed. revista e atualizada, Braga, AEDUM – Associação de Estudantes de Direito da Universidade do Minho, 2014.

NEVES, Rita Castanheira, *As ingerências nas comunicações electrónicas em processo penal: natureza e respectivo regime jurídico do correio electrónico enquanto meio de obtenção de prova*, Coimbra, Coimbra Editora, julho 2011, ISBN 978-972-32-1942-5.

OUBIÑA, Ana Mercedes da Silva Claro, *"As telecomunicações, a vida privada e o direito penal"*, Direito Penal Hoje - Novos desafios e novas respostas, Organiz. MANUEL DA COSTA ANDRADE e RITA CASTANHEIRA NEVES, Coimbra, Coimbra Editora, 2009, pp. 9 – 41, ISBN 978-972-32-1692-9.

KUROSE, James F., ROSS, Keith W., *Computer networking: a top-down approach*, 6th ed., Pearson Education, Inc., 2013, ISBN 978-0-13-285620-1.

RAMOS, Armando Dias, *A prova digital em processo penal: o correio eletrónico*, 2.ª edição atualizada e ampliada, Lisboa, Chiado Editora, fevereiro 2017, versão e-book, ISBN 978-989-51-2383-4.

RODRIGUES, Benjamim Silva, *Da Prova Penal, Tomo II – Bruscamente... A(s) face(s) oculta(s) dos Métodos Ocultos de Investigação Criminal*, Lisboa, Rei dos Livros, abril 2010, ISBN 978-989-8305-06-0;

_____*Da Prova Penal, Tomo IV – Da Prova-Electrónico-Digital e da Criminalidade Informático-Digital*, Lisboa, Rei dos Livros, abril 2011, ISBN 978-989-8305-18-3;

_____*Das Escutas Telefónicas, Tomo I – A Monitorização dos Fluxos Informacionais e Digitais*, Coimbra, Coimbra Editora, maio 2008, ISBN 978-989-95779-1-6;

_____*Direito Penal – Parte Especial – Tomo I – Direito Penal Informático-Digital*, Coimbra, Coimbra Editora, maio 2009, ISBN 978-989-95779-5-4.

ROXIN, Claus, *Derecho procesal penal/Strafverfahrensrecht*, trad. de la 25ª ed. alemana de Gabriela E. Córdoba y Daniel R. Pastor; Rev. por Julio B. J. Maier, Buenos Aires, Editores del Puerto, s.r.l.2001, ISBN 987-9120-36-1.

SANTOS, Rita Coelho, *O Tratamento Jurídico-Penal da Transferência de Fundos Monetários Através da Manipulação Ilícita dos Sistemas Informáticos*, Studia Iuridica 82, Coimbra, Coimbra Editora, 2005, ISBN 972-32-1300-1.

SOUSA, Marcelo Rebelo de e ALEXANDRINO, José de Melo, *Constituição da República Portuguesa Comentada – Introdução Teórica e Histórica, Anotações, Doutrina e Jurisprudência, Lei do Tribunal Constitucional*, Lisboa, Lex, 2000, ISBN 972-9495-91-2.

SOUSA, Miguel Teixeira de, *"O valor probatório dos documentos electrónicos"*, Direito da Sociedade da Informação – Volume II, FDUL – Faculdade de Direito da Universidade de Lisboa / APDI – Associação Portuguesa de Direito Intelectual, Coimbra, Coimbra Editora, 2001, pp. 171 – 201, ISBN 972-32-0994-2.

TU, Guan-Hua, *et al., "New Security Threats Caused by IMS-based SMS Service in 4G LTE Networks"*, Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2016. pp. 1118 – 1130.

VEIGA, Armando e RODRIGUES, Benjamim Silva, *"A monotorização de dados pessoais de tráfego nas comunicações eletrónicas"*, Raízes Jurídicas, Curitiba, v. 3, n.º 2, jul./dez. 2007, pp. 59 – 108.

VENÂNCIO, Pedro Dias, *"Breve Introdução à Questão da Investigação e Meios de Prova na Criminalidade Informática"*, Verbo Jurídico, dezembro 2006, pp. 1 – 34;

_____ *Lei do Cibercrime – Anotada e Comentada*, Coimbra, Coimbra Editora, fevereiro 2011, ISBN 978-972-32-1906-7.

VERDELHO, Pedro, *"A Convenção sobre o Cibercrime do Conselho da Europa – Repercussões na lei Portuguesa"*, Direito da Sociedade da Informação – Volume VI, APDI – Associação Portuguesa de Direito Intelectual, Coimbra, Coimbra Editora, 2006, pp. 257 – 276, ISBN 978-972-32-1411-3;

_____ *"A nova Lei do Cibercrime"*, Scientia Iuridica – Revista de Direito Comparado Português e Brasileiro, Tomo LVIII, n.º 320, Braga, Universidade do Minho, outubro/dezembro, 2009, pp. 717 – 749;

_____ *"A obtenção de prova no ambiente digital"*, Revista do Ministério Público, Ano 25.º, nº 99 julho-setembro 2004, pp. 117 – 136;

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

_____ *"Cibercrime"*, Direito da Sociedade da Informação – Volume IV, APDI – Associação Portuguesa de Direito Intelectual, Coimbra, Coimbra Editora, 2003, pp. 347 – 383, ISBN 972-32-1169-6;

_____ *"Técnica no Novo C.P.P.: Exames, Perícias e Prova Digital"*, Revista CEJ, nº 9 – Jornadas sobre a Revisão do Código de Processo Penal, 1º Semestre 2008, pp. 145 – 171.

VERDELHO, Pedro / BRAVO, Rogério / ROCHA, Manuel Lopes, *Leis do Cibercrime - vol. I*, Lisboa, Centro Atlântico, julho 2003, ISBN 972-8426-69-0.

JURISPRUDÊNCIA CONSULTADA

Acórdão do Supremo Tribunal de Justiça de 18-02-2009, disponível em http://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/8e0a119937ab01188025757c0052bba3?OpenDocument [Consultado em 17.09.2017].

Acórdão do Supremo Tribunal de Justiça de 27-05-2009, disponível em http://www.pgdlisboa.pt/jurel/stj_mostra_doc.php?nid=27558&codarea=2 [Consultado em 17.09.2017].

Acórdão do Tribunal da Relação de Coimbra de 18-06-2014, disponível em http://www.dgsi.pt/jtrc.nsf/c3fb530030ea1c61802568d9005cd5bb/84f1229d9b11c97680257d00003591fb?OpenDocument [Consultado em 18.07.2017].

Acórdão do Tribunal da Relação de Coimbra de 02-02-2016, disponível em http://www.dgsi.pt/jtrc.nsf/c3fb530030ea1c61802568d9005cd5bb/aba8f7cea02531c180257f4f003e6e54?OpenDocument [Consultado em 25.07.2017].

Acórdão do Tribunal da Relação de Évora de 26-06-2012, disponível em http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/9e4d23e33c93144580257de10056f883?OpenDocument [Consultado em 29.04.2017].

Acórdão do Tribunal da Relação de Évora de 22-05-2014, disponível em http://www.dgsi.pt/jtre.nsf/-/2FF1D3B3BC6D929080257DF100383C04 [Consultado em 18.07.2017].

Acórdão do Tribunal da Relação de Évora de 06-01-2015, disponível em http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/847dae6b85353cb880257de10056ff4c?OpenDocument [Consultado em 25.08.2017].

Acórdão do Tribunal da Relação de Évora de 20-01-2015, disponível em http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/2fbdd21285478f5f80257de10056ff7a?OpenDocument [Consultado em 25.08.2017].

Acórdão do Tribunal da Relação de Guimarães de 30-05-2013, disponível em http://www.dgsi.pt/jtrg.nsf/86c25a698e4e7cb7802579ec004d3832/1964cc05baf5047c80257b900037c92a [Consultado em 18.07.2017].

Acórdão do Tribunal da Relação de Lisboa de 15-07-2008, disponível em http://www.dgsi.pt/jtrl.nsf/0/9182245992c7c5d18025749000503b8c?OpenDocument [Consultado em 23.08.2017].

Acórdão do Tribunal da Relação de Lisboa de 24-09-2013, disponível em http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/c60dfe830c97cf8980257c0000368afa?OpenDocument [Consultado em 22.10.2017].

Acórdão do Tribunal da Relação do Porto de 03-04-2013, disponível em http://www.dgsi.pt/jtrp.nsf/d1d5ce625d24df5380257583004ee7d7/d21c6752627b971780257b4f003caa5d?OpenDocument [Consultado em 23.08.2017].

Acórdão do Tribunal da Relação do Porto de 22-05-2013, disponível em http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/abf6a7fedb6f7ba580257b88004ed413 [Consultado em 22.10.2017].

Acórdão do Tribunal da Relação do Porto de 30-10-2013, disponível em http://www.dgsi.pt/jtrp.nsf/c3fb530030ea1c61802568d9005cd5bb/0fab00c6a2ab290380257c2200521381?OpenDocument [Consultado em 22.10.2017].

Acórdão do Tribunal da Relação do Porto de 08-01-2014, disponível em http://www.dgsi.pt/jtrp.nsf/d1d5ce625d24df5380257583004ee7d7/b54faf2d4330b8d480257c6e004ff2df?OpenDocument [Consultado em 29.04.2017].

Acórdão do Tribunal da Relação do Porto de 17-09-2014, disponível em http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/5fd1df126b7ffe9880257d6600370f95?OpenDocument [Consultado em 29.04.2017].

Acórdão do Tribunal da Relação do Porto de 13-05-2015, disponível em http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/e3e21d9e62cdb86f80257e520037f3a0?OpenDocument [Consultado em 25.08.2017].

Acórdão do Tribunal da Relação do Porto de 26-05-2015, disponível em http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/aa9d0fb297dcca7880257e62003a86e4?OpenDocument [Consultado em 29.04.2017].

Acórdão do Tribunal da Relação do Porto de 13-04-2016, disponível em http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/ef54d51d3972157d80257fa4002e2d75?OpenDocument [Consultado em 14.05.2017].

Acórdão do Tribunal da Relação do Porto de 01-06-2016, disponível em http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/1f85e373f004b9fd80257fd5004eda69?OpenDocument [Consultado em 22.10.2017].

ENDEREÇOS ELETRÓNICOS CONSULTADOS

http://app.parlamento.pt/webutils/docs/doc.pdf?path=6148523063446f764c324679626d56304c334e706447567a4c31684a53556c4d5a5763765130394e4c7a464451554e45544563765247396a6457316c626e5276633056756476c6b5957526c6330563464475679626d467a4c7a557a595455304e5463784c546b784d5449744e4451774d6931685a6a41784c5751315a545269596a45335954646b4d7935775a47593d&fich=53a54571-9112-4402-af01-d5e4bb17a7d3.pdf&Inline=true [Consultado em 10.09.2017].

http://carlospintodeabreu.com/public/files/CPA_prova_meios_obtencao_prova.pdf [Consultado em 17/09/2017].

http://cibercrime.ministeriopublico.pt/pagina/o-que-fazemos-0 [Consultado em 14.05.2017].

http://cibercrime.ministeriopublico.pt/pagina/quem-somos [Consultado em 14.05.2017].

http://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/relatorio_anual_gabinete_cibercrime2015_02-03-2017.pdf [Consultado em 14.05.2017].

http://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/plano_acao_cibercrime_2015-2016.pdf [Consultado em 14.05.2017].

http://cibercrime.ministeriopublico.pt/sites/default/files/protocolo_comunicacoes.pdf [Consultado em 14.05.2017].

http://europa.eu/rapid/press-release_IP-17-16_en.htm [Consultado em 10.01.2017].

http://malware.wikia.com/wiki/Worm [Consultado em 15.04.2017].

http://observador.pt/2016/01/22/burla-taxas-moderadores-atraves-sms/ [Consultado em 18.07.2017].

http://searchenterprisedesktop.techtarget.com/tip/The-difference-between-hackers-and-crackers [Consultado em 15.04.2017].

http://searchenterpriselinux.techtarget.com/definition/script [Consultado em 15.04.2017].

http://searchmobilecomputing.techtarget.com/definition/pager [Consultado em 15.07.2017].

http://searchmobilecomputing.techtarget.com/definition/SIM-card [Consultado em 15.07.2017].

http://searchsecurity.techtarget.com/definition/Trojan-horse [Consultado em 15.04.2017].

http://whatis.techtarget.com/definition/IMEI-International-Mobile-Equipment-Identity [Consultado em 15.07.2017].

http://www.3gpp.org/news-events/3gpp-news/1614-sa_5g [Consultado em 12.10.2017].

http://www.apav.pt/cibercrime/ [Consultado em 15.10.2017].

http://www.computerworld.com.pt/2017/03/17/hacker-suspeito-de-danos-acima-de-400-mil-euros/ [Consultado em 15.04.2017].

http://www.dn.pt/sociedade/interior/ss7-a-porta-dos-hackers-para-controlar-a-nossa-vida-no-telemovel-5136137.html [Consultado em 18.07.2017].

http://www.erodocdb.dk/Docs/doc98/official/pdf/ECCRep052.pdf [Consultado em 08.07.2017].

http://www.history.com/topics/inventions/invention-of-the-internet [Consultado em 02.07.2017].

http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1137&tabela=leis [Consultado em 29.04.2017].

http://www.proselex.net/Documents/The%20New%20Hacker's%20Dictionary.pdf [Consultado em 15.04.2017].

http://www.stj.pt/ficheiros/coloquios/coloquios_STJ/V_Coloquio/maria_glria_leito.pdf [Consultado em 17/09/2017].

http://www.verbojuridico.net/doutrina/penal/penal_meiosprova.pdf [Consultado em 17/09/2017].

https://books.google.pt/books?redir_esc=y&hl=pt-PT&id=6XQNJe8-OdEC&q=gr#v=onepage&q=gr&f=false [Consultado em 17/09/2017].

https://definitions.uslegal.com/b/blue-hat-hacker/ [Consultado em 15.04.2017].

https://pplware.sapo.pt/informacao/ataque-de-phishing-chega-via-sms-em-nome-do-seu-banco/ [Consultado em 18.07.2017].

https://pplware.sapo.pt/informacao/ransomware-jogar-desbloquear-ficheiros/ [Consultado em 15.04.2017].

https://pplware.sapo.pt/internet/cibercrime-portugal-fez-8-mil-pedidos-ao-facebook/ [Consultado em 15.04.2017].

https://pplware.sapo.pt/internet/pop-ou-imap-qual-o-melhor/ [Consultado em 08.07.2017].

https://pplware.sapo.pt/microsoft/windows/seguranca-informatica-malware-virus-spyware-trojans/ [Consultado em 15.04.2017].

https://pt.slideshare.net/brunoms18/apresentao-novas-tecnologias-e-a-internet [Consultado em 08.07.2017].

https://support.microsoft.com/pt-pt/help/129972/how-to-prevent-and-remove-viruses-and-other-malware [Consultado em 15.04.2017].

https://techterms.com/definition/malware [Consultado em 15.04.2017].

https://www.anacom.pt/render.jsp?categoryId=346972 [Consultado em 08.07.2017].

https://www.anacom.pt/render.jsp?contentId=964154 [Consultado em 29.06.2017].

https://www.anacom.pt/streaming/DavidPernes_CongressoURSI2012.pdf?contentId=1148345&field=ATTACHED_FILE [Consultado em 16.07.2017].

https://www.computerhope.com/jargon/h/hyperlin.htm [Consultado em 02.07.2017].

https://www.fbi.gov/investigate/white-collar-crime [Consultado em 15.04.2017].

https://www.gta.ufrj.br/grad/09_1/versao-final/umts/lte.html [Consultado em 15.07.2017].

https://www.hmailserver.com/documentation/v4.3/?page=whatis_pop3imapsmtp [Consultado em 08.07.2017].

https://www.infopedia.pt/dicionarios/siglas-abreviaturas/MMS [Consultado em 08.07.2017].

https://www.noticiasaominuto.com/tech/377668/cibercrime-com-maior-crescimento-no-crime-economico [Consultado em 10.09.2017].

https://www.policiajudiciaria.pt/PortalWeb/page/%7BEC96A2D3-BA0F-4F51-9A3A-5BA3D222FE8B%7D [Consultado em 14.05.2017].

https://www.priberam.pt/dlpo/apreens%C3%A3o [Consultado em 21.08.2017].

https://www.priberam.pt/dlpo/interce%C3%A7%C3%A3o [Consultado em 21.08.2017].

https://www.publico.pt/2017/05/12/tecnologia/noticia/ataque-informatico-internacional-afecta-empresas-e-hospitais-1771939 [Consultado em 12.05.2017].

https://www.rtp.pt/noticias/pais/unidade-de-combate-ao-cibercrime-e-criminalidade-tecnologica-da-pj-entra-em-funcionamento_n965660 [Consultado em 14.05.2017].

https://www.techopedia.com/definition/10349/white-hat-hacker [Consultado em 15.04.2017].

https://www.techopedia.com/definition/15450/gray-hat-hacker [Consultado em 15.04.2017].

https://www.tutorialspoint.com/lte/lte_network_architecture.htm [Consultado em 15.07.2017].

https://www.webhs.pt/dicas/smtp-imap-pop3-explicacao/ [Consultado em 08.07.2017].