ALBERTO GIL LIMA CANCELA

A PROVA DIGITAL: OS MEIOS DE OBTENÇÃO DE PROVA NA LEI DO CIBERCRIME

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

Orientadora: Professora Doutora Sónia Mariza Florêncio Fidalgo

Coimbra, 2016

*"**A tecnologia é uma faca de dois gumes:***

se pode ser manipulada no âmbito de actividades ilícitas,

***também pode ser utilizada para combater estas últimas**"*

Helena Carrapiço

AGRADECIMENTOS

À FDUC, por todos os ensinamentos de Direito e de vida, que me proporcionou ao longo deste percurso.

Á Doutora Sónia Fidalgo, pela sua constante disponibilidade, simpatia, críticas e conselhos.
Ao Doutor Costa Andrade, por me incutir o gosto pelo Direito Penal, com as suas aulas e intervenções sempre dinâmicas e estimulantes.

À Secção de Defesa dos Direitos Humanos, da Associação Académica de Coimbra, por me fazer crescer como humanista e ser social.

Aos grandes amigos de Coimbra, por fazerem parte da "*minha*" Coimbra. Por estarem presentes em mais uma etapa do meu percurso académico, acreditando e incentivando. Por partilharem comigo esta fantástica montanha-russa que é a cidade dos estudantes.

Ao melhor pai, à melhor mãe e ao melhor irmão que podia ter a sorte de chamar meus, por todo o apoio, sacrifício, estímulo e entusiasmo, mesmo nos gestos mais simples. É o vosso exemplo e força que me faz avançar, e procurar sempre fazer o melhor, e ser melhor.

RESUMO

A Globalização, enquanto elemento de conexão global de aproximação cultural e económica revela-se potenciadora do fenómeno da criminalidade realizada por meios informáticos. Torna-se necessário que o Direito se adapte à nova realidade, não se prendendo a convenções ultrapassadas, estabelecendo um modelo de investigação criminal distinto do modelo tradicional, centrado no mundo físico.

O modelo de investigação policial referente aos crimes praticados através de meios informáticos será sustentado através de um tipo de prova, de particular natureza. A natureza instável, dispersa e imaterial que caracteriza a prova digital, incumbe a investigação a um maior cuidado com a sua recolha, de forma a garantir a sua integridade e força probatória.

Esta necessidade de adequação do direito e do processo penal seria respondida com a emanação da Lei 109/91, de 15 de Setembro, denominada de Lei do Cibercrime, que transporia a Decisão-Quadro n.º 2005/222/JAI, do Conselho da E.U. e as medidas previstas pela Convenção sobre o Cibercrime, do Conselho da Europa. Esta nova lei destaca-se por, pela primeira vez, inserir no ordenamento jurídico português, disposições materiais e de processo penal e medidas de cooperação internacional no combate à criminalidade informática, procurando facilitar a investigação no mundo digital.

No entanto, apesar de ser um diploma inovador, não está imune de problemas e incoerências processuais e lacunas legislativas, fragilizando direitos individuais, e, em situações pontuais, pôr em causa uma ação penal eficaz.

Palavras-chave: Cibercrime, Criminalidade Informática, Prova, Digital, Telecomunicações

ABSTRACT

Globalization, as a global connecting factor of cultural and economic approach, proves to enhance the phenomenon of crime conducted by electronic means. It is necessary that the law adapts to this new reality, not holding to outdated conventions, establishing a criminal investigation model separate from the traditional model, centered in the physical world.

The police investigation relating to crimes committed through electronic means will be sustained through a kind of proof, of a special nature. The unstable, dispersed and immaterial nature that characterizes digital evidence, urges for the investigation a more careful with its obtainment, in order to ensure their integrity and evidential value.

This need for adequacy for the law and criminal procedure would be answered with the emanation of Law 109/91, of September 15, called the Cybercrime Law, which transpose the Framework Decision 2005/222/JHA of the E.U. Council and the measures provided for by the Convention on Cybercrime, of the Council of Europe. This new law is notable for introducing the Portuguese legal system, for the first time, material and criminal procedure provisions and international cooperation measures to combat computer crime, seeking to facilitate the investigation in the digital world.

However, despite being an innovative diploma, it is not immune to procedural problems and inconsistencies and loopholes, weakening individual rights, and, in specific situations, jeopardizing effective prosecution.

Keywords: Cybercrime, Computer Crime, Digital Evidence, Telecomunications

LISTA DE SIGLAS E ABREVIATURAS

ADN – Ácido Desoxirribonucleico
ANACOM – Autoridade Nacional de Comunicações
ASTJ – Acórdão do Tribunal Constitucional
ATRC – Acórdão do Tribunal de Relação de Coimbra
ATRE – Acórdão do Tribunal de Relação de Évora
ATRG – Acórdão do Tribunal de Relação de Guimarães
ATRL – Acórdão do Tribunal de Relação de Lisboa
ATRP – Acórdão do Tribunal de Relação de Porto
BVERFGE – Bundesverfassungsgrericht (Tribunal Constitucional Federal da Alemanha)
CCIBER – Convenção sobre o Cibercrime
CDADC – Código de Direitos de Autor e dos Direitos Conexos
CP – Código Penal
CPP – Código de Processo Penal
CRP – Constituição da República Portuguesa
EUA – Estados Unidos da América
FBI – Federal Bureau of Investigation
IMEI – International Mobile Equipment Identity
IMSI – International Mobile Subscriber Identity
IP – Internet Protocol
IRC – Internet Relay Chat
ISP – Internet Service Provider
JIC – Juiz de Instrução Criminal
LC – Lei do Cibercrime
LCE – Lei do Comércio Eletrónico
LCI – Lei da Criminalidade Informática
MP – Ministério Público
NTIC – Novas Tecnologias de Informação e Comunicação
ONU – Organização das Nações Unidas
OPC – Órgãos de Polícia Criminal

ÍNDICE

I – INTRODUÇÃO

Não será necessária uma pesquisa rigorosa para corroborar a opinião geral: as novas tecnologias de informação e de comunicação vieram, incontestavelmente, facilitar o modo de vida das pessoas.

A Internet é o principal motivo pelo qual denominamos a sociedade atual como "Sociedade da Informação", cabendo-lhe um papel fulcral na vida do cidadão, das empresas e do Estado, que nela apoiam as suas funções. Graças à Internet o dia-a-dia dos cidadãos encontra-se beneficiado, permitindo-lhes, de forma rápida e económica, realizar as tarefas mais simples, no conforto do seu lar.

A massificação da Internet permitiu a aproximação do cidadão mais comum ao resto do mundo, democratizando o acesso à informação.

Por outro lado, com o desenvolvimento tecnológico e a utilização da *World Wide Web*, essa facilidade pode tornar-se um campo minado, sendo cada vez mais instrumentalizada para a prática de atos ilícitos.

Situando-se num espaço virtual, vulnerável, de acesso rápido, a expansão das redes de comunicação serve de veículo a um novo tipo de criminalidade imaterial, transfronteiriça e complexa. Esta nova vaga de criminalidade acusa uma forte probabilidade de impunidade, na execução de novos crimes e ao apoiar crimes já existentes, reforçados com novas técnicas, do planeamento à sua realização.

No entendimento de PEDRO VENÂNCIO (2011: 17 ss.), a criminalidade informática não se restringirá apenas aos crimes que abranjam o elemento digital como parte integradora do seu tipo legal ou objeto de proteção, mas amplia-se a qualquer crime praticado através de meio informático, mesmo que se trate de mero instrumento, sem integrar o seu tipo legal.

Esta realidade já era conhecida pelo legislador, que iniciara o combate a esta criminalidade através da Lei n.º 109/91, de 17/8. No entanto, o legislador não incluiu no texto legal um regime jurídico de recolha da prova digital, não prevendo a sua recolha na investigação, mesmo em situações em que constituem a única prova existente.

Coube à Lei do Cibercrime colmatar essa lacuna, atribuindo aos órgãos de polícia criminal os meios necessários para o combate à criminalidade informática.

Com este estudo, procuraremos dar o nosso humilde contributo ao estudo da Lei do Cibercrime, dando relevo à importância das novas disposições penais materiais e processuais no ordenamento jurídico português. Iremos demonstrar as dificuldades inerentes à investigação forense digital, que carece de correta articulação com esta criminalidade em constante desenvolvimento, e os meios previstos pelo legislador para ultrapassar tais obstáculos.

Analisando o conjunto previsto de medidas de obtenção da prova digital, é nosso intuito indagar sobre as soluções político-criminais estabelecidas, que permitam uma maior articulação entre disposições processuais, com vista ao auxílio das autoridades criminais, e maior eficácia no combate à criminalidade informática.

Realçaremos, ainda, as respostas legislativas para esta temática no panorama legislativo português. Em especial, sobre a obtenção da prova digital, destacam-se a Lei n.º 109/2009 (a Lei do Cibercrime), o Código de Processo Penal e a Lei n.º 32/2008, que se complementam.

Encetamos o estudo desta temática cientes que a relativa novidade da Lei em apreço, traz consigo a necessidade de um estudo doutrinário e jurisprudencial intenso, apenas alcançável com o decurso do tempo, de forma a consolidar procedimentos e solidificar conceitos. Assim sendo, para além de possíveis soluções processuais, abordaremos questões intimamente ligadas ao estudo da Lei e do panorama processual atual.

1. Crime e Justiça na Sociedade Digital

1.1. Criminalidade Informática

Nas palavras de VIEIRA NEVES, o processo penal será efetivamente aplicável quando visar *"essencialmente a realização da justiça e a descoberta da verdade material, a proteção dos direitos fundamentais e o restabelecimento da paz jurídica, através da aplicação de uma sanção penal ao arguido que violou específicos bens jurídicos que ascenderam à discursidade penal"*[1]. Tal aplicação sancionatória depende do desenvolvimento sociocultural da comunidade afetada, das formas de atuação das entidades policiais e do estado de maturidade da consciência jurídica comunitária[2]. Enquanto produto em constante mutação face à evolução, o Direito Processual Penal deverá dar uso dos meios mais atuais e capazes de realizar eficazmente as tarefas condizentes à sua função de administrar a justiça penal.

A evolução tecnológica que marcou o século XX, e continua a acentuar o presente século, estabeleceu no quotidiano um instrumento facilitador dos vários setores da sociedade, desde a defesa, ciência e economia, à saúde, educação e Administração Pública.

No entanto, essa facilidade levaria a um crescimento de práticas criminosas, abrindo caminho para um novo tipo de criminalidade organizada e lesante em campos relevantes para a sociedade[3]. Apesar de os bens jurídicos atacados se manterem inalterados (a vida, a reserva da vida privada, o património, os direitos de autor e os direitos conexos, a honra, a liberdade e autodeterminação sexual, a segurança do Estado, a paz pública, a Humanidade, a segurança das comunicações, entre outros[4]), a sua esfera jurídica passa a ser afetada por novos métodos lesivos, como a reprodução ilegítima de um programa protegido.

---

[1] NEVES, Rosa Vieira, *A Livre Apreciação da Prova e a Obrigação de Fundamentação da Convicção (na Decisão Final Penal)*, Coimbra, Coimbra Editora, 2011, pág. 79.

[2] DIAS, Jorge de Figueiredo, *Clássicos Jurídicos, Direito Processual Penal*, Coimbra Editora, 2004, pp. 59-60.

[3] MARTINS, A.G. Lourenço, *Criminalidade Informática*, vol. IV, Coimbra Editora, 2003, pág. 11.

[4] BARROS, Juliana Isabel Freitas, *O Novo Processo Penal: Os Meios de Obtenção de Prova Digital consagrados na Lei 109/2009, de 15 de Setembro*, Dissertação apresentada no âmbito do 2.º ciclo de Estudos em Direito da Faculdade de Direito da Universidade de Coimbra, com especialização em Ciências Jurídico-Forenses, sob orientação da Prof. Dra. Helena Moniz, Coimbra, 2012, pág. 11.

Assim, e tal como supra referido, a evolução tecnológica irá forçar o Direito Processual Penal a evoluir, criando normas legais e procedimentos, de forma a criminalizar as práticas lesivas realizadas através da informática.

Perante esta necessidade de desenvolvimento, a doutrina divide-se quanto à sua inserção na sociedade do risco, sendo suscetível da tutela do "*Direito Penal do Risco*". Questiona-se se a esta criminalidade deverá corresponder um combate baseado na prevenção, que antecipe a proteção dos bens jurídicos essenciais passíveis de lesão, enquadrando-se como condutas de perigo abstrato[5].

Na esteira de FARIA COSTA, a crescente dependência social quanto aos meios tecnológicos e à informação automatizada e os interesses materiais que se encontram por detrás de tais instrumentos, impõe uma atuação clara do Direito Penal. Não concordando com a tentativa de diabolizar a informática, o autor defende que, apesar das suas particularidades e tratando-se de um canal comunicacional amplo e complexo, não se verifica "*sustentabilidade científica para autonomizar um direito penal da informática".* Assim, esta área de criminalização deverá ser tratada com os meios tradicionais disponibilizados pelo Direito Penal[6]. Tendo em conta as divergências doutrinais, entendemos que as especificidades técnicas que caracterizam a criminalidade informática exigem um reconhecimento de procedimentos de investigação distintos. Assentando numa prova de particular natureza, deverão relevar os cuidados necessários para a sua recolha, conservação, análise e apresentação em juízo, carecendo o processo de investigação de peritos capazes de garantir a integridade da prova. Seguindo o entendimento de ANA RAQUEL LEITE[7], ao ser desconsiderado o caráter especial da investigação, estará em risco o princípio constitucional da igualdade, que prevê que seja tratado igualmente o que seja igual, e diferentemente o que seja diferente. Perante a necessidade de proteção da "*disponibilidade, confidencialidade e integridade da informação, assim como do processamento eletrónico (...) que compreendem o armazenamento e a transmissão dos dados*", tendemos a admitir um Direito Penal da Informática, através um regime autónomo

[5] LEITE, Ana Raquel Gomes; *Criminalidade Informática – Investigação e Meios de Obtenção de Prova*, Dissertação apresentada no âmbito do 2.º Ciclo de Estudos em Direito, Faculdade de Direito da Universidade de Coimbra, com especialização em Ciências Jurídico-Forenses, sob orientação da Professora Doutora Helena Moniz, Coimbra, 2013, pág. 17.

[6] COSTA, José Francisco de Faria, *Algumas reflexões sobre o estatuto dogmático do chamado "Direito Penal Informático"*, Direito Penal da Comunicação, alguns escritos, Coimbra Editora, 1998, pág. 111, 112 e 115 a 119.

[7] LEITE, Ana Raquel Gomes; *ob. cit.*, pág. 17.

referente aos meios de obtenção da prova adequado às exigências instituídas pelas novas tecnologias.

Sendo o Direito da Informática uma realidade aceite por cada vez mais juristas, ROGÉRIO BRAVO[8] questiona a razão da ineficácia da norma penal, enquanto dissuasora e preventiva do ato ilícito, e a desconformidade da legislação "*entre o seu sentido normativo e a sua correspondência com a realidade*". Como resposta, o autor estabelece que deverão ser consideradas quatro ideias: "*o avanço tecnológico; o tempo; a "natureza" do espaço virtual e as relações deste com outros espaços de existência humana*".

As novas exigências do direito penal tornam necessário que o legislador estabeleça formalmente disposições normativas que regulem e facilitem a investigação.

1.2. Evolução Legislativa

O Ordenamento legislativo que regula atualmente a investigação forense digital em Portugal é fruto de uma evolução cautelosa, conseguida através dos contributos europeus no combate à criminalidade informática.

A nível comunitário, Ulrich Sieber estrutura o desenvolvimento legislativo referente à criminalidade informática em várias fases distintas[9]. A primeira fase, ocorre nos anos 70 do século transato, com a criação do primeiro diploma legal visando salvaguardar a proteção da vida privada, posta em risco com os novos métodos de recolha, armazenamento, transferência e interconexão dos dados adquiridos no sistema informático. Com o passar da década, surge uma nova fase, focada nos crimes económicos praticados através da informática. A necessidade de desenvolvimento legislativo nesta segunda fase justificou-se com a dificuldade em atribuir uma definição específica para o conceito de propriedade, que passa a consistir numa realidade imaterial e não tangível, com a inclusão de crimes como a manipulação de computador. A terceira fase acontece na década de 80, onde o legislador procurou, através de emendas, salvaguardar a propriedade intelectual. Já

[8] BRAVO, Rogério, *As Tecnologias de Informação e a Compressão dos Direitos, Liberdades e Garantias – os efeitos das regras "10/10" e "1/1",* Lisboa, 2012, pág. 1.

[9] SIEBER, Ulrich, *Les crimes infomatiques et d'autres crimes dans le domaine de la technologie informatique*, in Revue Internationale de Droit Penel, AIDP, Érès, Colóquio de Wurzbourg, Outubro de 1992, pág. 55. No mesmo sentido, RODRIGUES, Benjamim Silva, *Direito Penal Parte Especial, Tomo I, Direito Penal Informático-Digital, Contributo para a Fundamentação da sua Autonomia Dogmática e Científica à Luz do novo Paradigma de Investigação Criminal: a Ciência Forense Digital e a Prova Digital*, Coimbra Editora, 2009, pp. 510 ss.

a quarta fase de Sieber impulsionou reformas legislativas no direito processual penal, facilitando investigações forenses. Por sua vez, autores como SILVA RODRIGUES alargam o âmbito evolutivo deste estado legislativo para a existência de uma quinta e sexta fases referentes à evolução do Direito Internacional, necessária perante o caráter transnacional da criminalidade informática, onde não existem fronteiras, devendo o direito atuar a nível planetário. Perante disposições globais, tornam-se necessárias alterações em matérias de lei processual penal e a fixação de medidas de segurança, restrição e proibição informáticas. Assim, seguindo o disposto nos quadros europeus para regulamentação interna, o legislador português incluiu no seu ordenamento jurídico-penal a Resolução nº9(89) do Conselho da Europa, sob a égide da Lei da Criminalidade Informática nº 109/91, de 17/8[10].

A criminalidade informática está intimamente relacionada com o pleno exercício de direitos de personalidade e das liberdades individuais. O ordenamento jurídico português prevê no art. 35.º da CRP a proteção das pessoas contra o tratamento de dados pessoais, salvaguardando o direito de acesso aos dados armazenados em registos informáticos, e a proibição de tratamento de dados pessoais específicos, como convicções filosóficas ou políticas. No entanto, a consagração legal desta proteção pode revelar-se insuficiente, levando o legislador a "*transpor estes direitos para leis ordinárias, combinando a evolução tecnológica operada e os direitos dos cidadãos*"[11].

A previsão de crimes praticados por meio informático pelo Código Penal revelar-se-ia insuficiente perante a evolução informática, levando o legislador português a emitir a Lei n.º 10/91, de 29/4, (Lei de Proteção de Dados Pessoais face à Informática), satisfazendo as garantias constitucionais ao determinar um esquema geral de infrações, com "*um domínio mais dilatado que o do artigo 181.º do CP*"[12].

Viria a ocorrer em Budapeste em 23 de Novembro de 2001, a Convenção sobre o Cibercrime do Conselho da Europa, considerada "*o primeiro e mais importante trabalho*

[10] O legislador nacional seguiu o estabelecido no Relatório do Comité Europeu para os Problemas Criminais do Conselho da Europa. cfr. ROCHA, Manuel Lopes, *A lei da criminalidade informática (...), Génese e técnica legislativa*, in Legislação, INA, n.º 8, pág. 65, maxime ponto 4.

[11] SIMAS, Diana Viveiros de; *O Cibercrime*; Dissertação apresentada no âmbito do 2.º Ciclo de Estudos em Direito, no Curso de Mestrado em Ciências Jurídico-Forenses, conferido pela Universidade Lusófona de Humanidades e Tecnologias, sob orientação do Prof. Dr. José Sousa Brito, Lisboa, 2014, pág. 71.

[12] MARQUES, Garcia; MARTINS, Lourenço; *Direito da Informática*, 2.ª Ed., Coimbra, Almedina, 2006, pág. 663.

internacional de fundo sobre crime no ciberespaço"[13]. Procurando uma harmonização legislativa, de forma a facilitar a cooperação internacional na investigação forense digital[14], a Convenção contemplou um conjunto de conceitos informático-jurídicos, de ilícitos criminais, de medidas processuais destinadas a regular a forma de obtenção da prova digital e os mecanismos de promoção da cooperação internacional e regras de aplicação espacial dos crimes aí previstos.

Com a aprovação do relatório resultante da discussão dos vários peritos presentes, definiram-se como objetivos primeiros dessa cooperação "*impedir os atos praticados contra a confidencialidade, integridade e disponibilidade de sistemas informáticos, de redes e de dados informáticos, bem como a utilização fraudulenta desses sistemas, redes e dados, prevendo a criminalização desses comportamentos, tal como se encontram descritos na presente Convenção, e a criação de competências suficientes para combater eficazmente essas infrações, facilitando a deteção, a investigação e a ação penal relativamente às referidas infrações, tanto ao nível nacional como ao nível internacional"*[15].

Para a criação da Lei do Cibercrime, devemos atribuir destaque a outro diploma comunitário. O combate a ataques contra sistemas informáticos seria concretamente reforçado com a Decisão-Quadro 2005/222/JAI do Conselho da Europa, de 24/2, dando seguimento às linhas orientadoras estabelecidas pela Convenção do Cibercrime. A "*natureza transnacional e sem fronteiras dos novos sistemas de informação implica que os ataques contra esses sistemas têm frequentemente uma dimensão transfronteiriça*", através da promoção da cooperação entre as autoridades judiciárias competentes, aproximando as leis penais como segurança dos sistemas de informação e combate a ataques como vírus, pirataria ou negação de serviço[16].

A defesa dos direitos e liberdades individuais tem-se patenteado como uma constante preocupação da Comunidade Europeia, através da emissão da Directiva n.º

[13] Exposição dos Motivos da Proposta de Lei nº 289/X/4ª – Lei do Cibercrime.
[14] VERDELHO, Pedro; BRAVO, Rogério; ROCHA, Manuel Lopes; *Leis do Cibercrime*, Vol. 1, pág. 27, disponível em http://www.centroatl.pt/titulos/direito/imagens/excerto-ca-leisdocibercrime1.pdf e acedido a 29-12-2015.
[15] Diário da República, 1.ª série — N.º 179 — 15/9/2009, disponível em https://dre.pt/application/dir/pdf1sdip/2009/09/17900/0635406378.pdf e acedido a 18-12-2015.
[16] Ponto (5) da Decisão-Quadro nº 2005/222/JAI do Conselho, de 24/2, disponível em http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32005F0222 e acedido a 17-01-2016.

95/46/CE do Parlamento Europeu e do Conselho, transposta para o direito interno com a Lei n.º 67/1998 de 26/10, conjugada com a Lei n.º 41/2004 de 18/8.

Referente às questões de proteção da privacidade no setor das comunicações eletrónicas e dados pessoais, devemos destacar a Lei n.º 41/2004, alterada pela Lei n.º 46/2012, reguladora do tratamento e armazenamento dos dados de tráfego relativos aos utilizadores de empresa que disponibilizam serviços de comunicações eletrónicas. Estabelece que tais dados ser eliminados ou tornados anónimos quando deixem de ser necessários para a faturação dos assinantes e pagamentos de interligações.

Assim, cabe ao Estado garantir os direitos de liberdade, segurança e privacidade dos cidadãos, em situações em que a segurança e liberdade de utilização das tecnologias de informação e comunicação se aliam à criminalidade informática, sendo postas em causa.

Transpondo para o ordenamento jurídico nacional a Diretiva n.º 2006/24/CE do Parlamento Europeu e do Conselho, de 15/3, a Lei n.º 32/2008, de 17/7 (Lei da Retenção de Dados de Tráfego), diz respeito à conservação de dados nas comunicações eletrónicas. Estabeleceu um período máximo de 1 ano de conservação dos dados considerados relevantes para investigação e deteção de crimes graves e com autorização por despacho fundamentado do Juiz (artigo 3.º). A Lei n.º 32/2008 será um dos diplomas de aplicação complementar ao regime jurídico aplicável em matéria de obtenção da prova digital, e será especificamente analisado posteriormente.

1.3. Conceitos do Cibercrime

Tratando-se de um crime praticado com o uso da Internet, podemos encontrar várias terminologias como cibercrime, crime informático, *high technology crime*, entre outras. Apesar das disposições legais previstas para a criminalidade informática, não podemos encontrar um consenso na busca de uma expressão, de uma definição, ou uma tipologia e classificação desses crimes[17], forçando uma definição de *"criminalidade*

[17] DIAS, Vera Elisa Marques*; A problemática da investigação do Cibercrime*, pág. 65, disponível em http://www.datavenia.pt/ficheiros/edicao01/datavenia01_p063-088.pdf e acedido a 10-11-2015. A figura de criminalidade informática dispõe de várias classificações de autores de Romeo Casabona, Faria Costa à *National Hi-Tech Crime Unit*. Essas classificações encontram-se descritas em RODRIGUES, Benjamim Silva, *Direito Penal Especial – Direito Penal Informático-Digital*, Coimbra, 2009, pp. 168-194.

informática" baseada na legislação vigente ou na doutrina e jurisprudência subjetivamente relevante[18].

Perante tal indefinição, iremos olhar a criminalidade informática como a criminalidade praticada através de informática, que poderá, por sua vez, ser usada para preencher outro tipo de crime, seja ele ato de execução ou preparatório[19]. Poderemos considerar o conceito amplo defendido por DIAS VENÂNCIO abrangendo *"toda a panóplia de atividade criminosa que pode ser levada a cabo por meios informáticos, ainda que estes não sejam mais que um instrumento para a sua prática, mas que não integra o seu tipo legal, pelo que o mesmo crime poderá ser praticado por recurso a outros meios"* [20], em detrimento de um conceito restrito, correspondente aos crimes em que a informática será apenas parte integradora do tipo legal ou seu objeto de proteção.

Coube á Lei n.º 109/91, de 17/8 dispor um catálogo de crimes ligados à informática: a falsidade informática, o dano relativo a dados ou programas informáticos, a sabotagem informática, o acesso ilegítimo, a interceção ilegítima, a reprodução ilegítima de programa protegido.

Esta lei viria a ser revogada, integrando atualmente a Lei n.º 109/2009 de 15/9, diploma sustentado pela necessidade de um combate homogéneo a nível global, discutida na Convenção sobre a Cibercriminalidade. Com a elaboração de uma nova lei, o legislador português procurou transpor para o seu ordenamento jurídico o disposto na Decisão-Quadro 2005/222/JAI quanto aos tipos legais de crimes. Entre os artigos 3.º e 8.º da LC, o legislador português estabelece como crimes ligados à informática: a falsidade informática, o dano relativo a programas ou dados informáticos, a sabotagem informática, o acesso legítimo, a interseção ilegítima e a reprodução ilegítima de programa protegido. Para além destes crimes, o legislador já havia considerado no Código Penal os crimes de devassa por meio de informática (artigo 193.º), de violação de correspondência (artigo 194.º) e de burla informática e nas telecomunicações (artigo 221.º). Tendo em conta os tipos legais apresentados, a execução dos crimes informáticos será executado por três formas: através

[18] VENÂNCIO, Pedro Dias, *Lei do Cibercrime Anotada e Comentada*, 1.ª ed., Coimbra, Coimbra Editora, 2011, pág. 16.
[19] Por exemplo, um homicídio ser provado em tribunal através deste meio, pois "*a prova digital não se esgota na criminalidade informática em sentido estrito*" in BARROS, Juliana Isabel Freitas, *ob. cit.*; Coimbra, 2012, pp.11-12.
[20] VENÂNCIO, Pedro Dias, *ob. cit.*, pág.17.

de manipulação, ou alteração de dados; de espionagem, com o furto de dados informáticos; e a sabotagem, destruindo ou danificando parte ou totalmente os dados armazenados.

A natureza imaterial e anónima do crime informático, executado à distância do sujeito vitimizado, sem necessidade de presença física nem recurso a violência, facilita a ação do delinquente.

Considerando-se com uma maior tolerabilidade moral como forma de se desculpabilizar dos seus atos, o agente criminoso age pelo desafio de se superar à máquina, com conhecimentos técnicos informáticos acima da média.

A evolução da criminalidade e o constante perfeccionismo técnico dos agentes criminais leva à necessidade de dar relevância no ordenamento jurídico à figura da prova digital, enquanto instrumento fundamental ao bom curso da investigação e de apresentação em julgamento, garantindo que a cadeia de custódia foi cumprida e que esta prova mantém a sua força probatória inicial. Tal realidade será difícil, numa fase inicial, pois o nosso ordenamento jurídico encontra-se fundamentalmente estabelecido para um mundo físico, necessitando de normas que permitam atribuir a essa prova uma certeza absoluta quanto à sua fiabilidade.

Seguindo o entendimento de vários autores, a prevenção constitui a melhor forma de detetar, evitar e lutar contra os efeitos do cibercrime, incrementando a *literacia informática*. A prevenção será alcançada com informação, sensibilização e preparação, através de seminários, campanhas visadas a um público-alvo comum ou específico, alertando para os riscos e perigos do mundo cibernético e os meios de proteção e responsabilidade de utilização[21]. Para além da prevenção pessoal, é necessário um investimento tecnológico e financeiro à investigação e desenvolvimento em segurança e medidas de proteção através do uso de *passwords* e técnicas de proteção, como identificação de assinaturas digitais ou outras soluções que garantam a segurança da informação e da comunicação. Assim, cabe ao Governo, ao sistema educativo e às empresas de segurança informática esse papel de informar os utilizadores e de desenvolver soluções para alcançarmos infra-estruturas seguras[22]. Por outro lado, essa tarefa de segurança permite um estudo mais aprofundado à génese do crime, permitindo a sua antevisão, fundamental como prevenção do aparecimento de novas formas de cibercrime.

[21] RODRIGUES, Benjamim Silva, *Direito Penal Parte Especial, Tomo I, Direito Penal Informático-Digital*, Coimbra Editora, Limitada, 2009, pág. 238; DIAS, Vera Elisa Marques, *ob. cit.*, pág. 77.
[22] DIAS, Vera Elisa Marques, *ob. cit.*, pág. 77.

O conhecimento das causas e origens do crime permite que sejam tomadas medidas eficazes para o seu combate, identificando ameaças, com o mínimo de danos e tempo de reação. Assim, surge também como prioridade, a antecipação do crime, de forma a estabelecer que a prevenção deverá adaptar-se à evolução sociológicas, independentemente da forma como este será cometido.

2. Prova Digital

2.1. Conceitos

Com o desenvolvimento da tecnologia e dos meios técnicos usados para cometer os intitulados crimes informáticos, aos atos dos agentes criminais acrescentam-se uma maior adaptação e facilidade de ação. Assim, aumenta a dificuldade das entidades no exercício de funções de controlo. Mantendo o *status quo* dos seus instrumentos de investigação, estas podem revelar-se obsoletas face à constante inovação da contraparte, quando confrontadas por obstáculos processuais na proteção dos deveres fundamentais.

Tendo em conta a relativa novidade da Lei do Cibercrime, poucos autores se debruçaram sobre esta temática, não havendo uma definição concreta para a figura da prova digital. Apesar dessa escassez conceitual, destacam-se dois autores que apresentaram uma definição consoante o seu estudo. A prova digital é descrita por SILVA RODRIGUES como *"qualquer tipo de informação, com valor probatório, armazenada em repositório eletrónico-digitais de armazenamento, ou transmitida em sistemas e redes informáticas ou redes de comunicações eletrónicas, privadas ou publicamente acessíveis, sob a forma binária ou digital"*[23]. Por sua vez, DIAS RAMOS apresenta uma noção que consideramos mais clara, classificando-a como a *"informação passível de ser extraída de um dispositivo eletrónico (local, virtual ou remoto) ou de uma rede de comunicações. Pelo que esta prova digital, para além de ser admissível, deve ser também autêntica, precisa e concreta"*[24].

Na *International Hi-Tech Crime and Forensic Conference*, realizada em Outubro de 1999, em Londres, o *Scientific Working Group on Digital Evidence* apresentou

[23] RODRIGUES, Benjamim Silva, *Direito Penal Parte Especial, Tomo I, Direito Penal Informático-Digital (…),* Coimbra, 2009, pág. 722.
[24] RAMOS, Armando Dias, *A Prova Digital em Processo Penal*, Chiado Editora, 1.º ed. Novembro 2014, pág. 86.

definições, *standards* e princípios, relevantes para demonstrar à comunidade forense internacional a natureza da prova digital e o caminho investigativo a percorrer, de forma a garantir a sua força probatória[25]. Para garantir a validade da prova digital será necessário considerarmos as suas características e os princípios que a regulam. A prova digital deverá ser consistente com o sistema legal probatório vigente no processo penal português. Sendo uma prova inserida num meio tecnicamente complexo e de difícil apreensão, deverá representar-se com uma linguagem simples, de forma a ser aplicável pela generalidade dos operadores judiciários, mantendo os termos considerados fundamentais para a investigação. Deverá ainda ser uma prova durável, devendo as entidades judiciárias competentes tomar medidas para garantir a sua recolha e conservação. A seguinte característica determinada pelo SWGDE foca-se na necessidade de conformá-la ao modelo vigente internacionalmente em matéria de prova digital, de modo a ser admitida noutros países relacionados com o crime em questão. A prova digital deverá ainda ser produzida seguindo todos os critérios e rigor necessários para garantir a sua integridade da sua força probatória e inspirar confiança ao agente que dela fizer uso para a investigação. Para tal, é fundamental que se verifique uma uniformidade na produção da prova, independentemente da modalidade que a caracterize, devendo haver conformidade no seguimento dos princípios fundamentais da prova digital em todas as fases do processo forense digital. Durante a investigação forense, não está fechada a possibilidade de apelar a outras regras ou princípios que possam revelar-se fundamentais no processo, garantindo a admissão da prova em tribunal e impedir que qualquer falha na sua força probatória ponha em risco a presunção de inocência do arguido.[26]

2.2. Dificuldades Colocadas pela sua Natureza

Enquanto instrumento fundamental para determinar e condicionar um modelo de investigação forense digital, a prova digital será identificada, de forma a reconhecer as várias fases processuais, e qual o conteúdo correspondente a cada uma.

No entanto, apesar do impacto que teve a determinação dos *standards* necessários que devem caracterizar a prova digital, a realidade é que, por se tratar de uma prova

[25] Disponível em https://www.fbi.gov/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm/, acedido a 05-01-2016
[26] RODRIGUES, Benjamim Silva, *ob. cit.*, pág. 722

tecnicamente complexa e de carente de interpretação especializada, esse cenário será difícil de se afirmar.

No vasto mundo cibernético, a prova digital deverá ser recolhida de forma célere, cumprindo todos os cuidados necessários, sob pena de perder integridade. Assim, o investigador deverá considerar a prova pela sua natureza *efémera*, o que dificulta a sua conservação num dispositivo eletrónico-digital que permita aumentar o seu período de utilidade investigativa, para além do naturalmente considerado.

Para além de temporária, a prova digital também é *frágil* e *alterável*, caindo sobre o investigador forense a necessidade de redobrar os cuidados a tomar. Antes de recolher a prova, deverá identificar, de forma ainda mais rigorosa, qual o tipo de prova digital em causa. Apenas com essa identificação, poderá o investigador garantir a força probatória da prova digital, sem perigo de esta ser alterada ou desaparecer.

Havendo esta possibilidade de alteração ou desaparecimento, o investigador deverá ainda considerar a prova digital pela sua natureza *volátil* e *instável*. A instabilidade demonstrada por esta prova, provindo da constante mutabilidade que lhe caracteriza, torna mais difícil a sua apreensão. Tal dificuldade verifica-se em situações em que o investigador se depara inicialmente com uma prova com certas características, e mais tarde, esta se modifica, total ou parcialmente.

A prova digital consiste ainda numa prova *imaterial*. Desta forma, a imaterialidade da prova digital imporá ao investigador forense ser conhecedor de técnicas específicas, sob pena de se perder a força de prova, na eventualidade de o investigador a alterar significativamente, por desconhecer a sua presença.

Esta necessidade de o investigador possuir conhecimentos técnicos e científicos deve-se, particularmente, à *complexidade* e *codificação* caracterizadoras da prova digital. De modo a aceder a sistemas ou redes informáticos, o investigador deverá munir-se de todas as técnicas e conhecimentos científicos, para dar uso de palavras-chave ou servir-se de técnicas de desencriptação.

Em certas situações, a investigação forense deverá ter em conta a dispersão da prova digital, ou seja, esta poderá encontrar-se distribuída por vários "*terminais, computadores e redes que se estendem por uma vasta área espacial ou geográfica*" [27]. Surgindo em ambiente digital, a abordagem da investigação forense deverá fundamentar-se

[27] RODRIGUES, Benjamim Silva, *ob. cit.*, Coimbra Editora, 2009, pág. 726.

com o caráter difuso e disperso da criminalidade informática, não havendo concentração dos seus elementos integrantes do complexo informático.

Como referido, a prova digital abrange impulsos eletromagnéticos momentâneos relevantes para a rede ou sistema informático de comunicações eletrónicas. Por tal, a prova digital caracteriza-se como *dinâmica* e *mutável*. As competências do investigador exigem que este realize uma investigação estruturada temporalmente, comparando vários períodos temporais, permitindo aceder à prova digital de maior utilidade para a investigação.

2.3. Princípios

Seguindo a doutrina defendida por autores como SILVA RODRIGUES, cabe-nos considerar que a obtenção da prova digital deverá seguir determinados princípios orientadores autónomos[28], que se identificarão cumulativamente com os princípios referentes à prova no processo penal. Assim, a prova digital deverá ver também reconhecidos os princípios específicos respeitantes às características da prova concreta, para além dos princípios genéricos, respeitando o *princípio da cumulação dos princípios probatórios do processo penal e da investigação forense*.

De forma a garantir a integridade da prova obtida durante os atos de recolha, armazenamento e tratamento, a prova digital deverá respeitar um *princípio de não alteração da prova no ato de recolha*. Será exigido que, durante o decurso da investigação, o investigador digital exclua da sua conduta qualquer atuação que contamine os dados obtidos com elementos alheios ao sistema ou rede informáticos investigados[29].

Nesta temática, também releva o *princípio da especialização ou qualificação do pessoal adstrito à investigação forense digital*. As fases de acesso, recolha, conservação e análise estarão na esfera de competência de pessoal especializado, que, dotados de conhecimentos técnicos, impedem o corrompimento ou o deficiente manuseamento da prova, e a sua posterior inadmissibilidade. Quanto a questões de fixação de perfis de ADN, e tendo em conta a referida necessidade de reforço da especialização técnica, vêm sendo tendencialmente criados organismos certificados e reconhecidos internacionalmente,

[28] Estabelecidos na *International Hi-Tech Crime and Forensics Conference*. https://www.fbi.gov/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm/, e acedido a 27-12-2015

[29] RODRIGUES, Benjamim Silva, *ob. cit*., pág. 726

competentes para realizar as perícias informáticas, de acordo com os cânones procedimentais internacionalmente reconhecidos em matéria de investigação digital.

Outro princípio claramente relevante consiste na *garantia de documentação em todas as fases processuais (acesso, recolha, armazenamento, transferência, preservação e apresentação ou repetição da prova digital)*. Qualquer investigação forense baseia a sua conclusão na integridade da *"cadeia de controlo"*. Para tal, é indispensável a documentação de todas as etapas da investigação, de forma a tornar viável essa cadeia. Este princípio acarreta uma necessidade de se ver garantido um controlo reforçado dos investigadores responsáveis pela investigação do objeto em causa. Apenas através da *"reversão dinâmica"* será possível repetir a prova, cabendo aos agentes competentes a tarefa de descrever da forma mais detalhada possível os resultados obtidos na fase anterior[30].

Segundo o *princípio de responsabilidade pessoal*, atribui-se pessoalidade à cadeia de controlo. Por outras palavras, cada profissional chamado a intervir na investigação forense digital será responsável por controlar a cadeia de custódia das provas que ele recolher ou produzir, de forma a garantir a força probatória desse material. Desta forma, ficam excluídos do acesso a objetos sob investigação forense qualquer terceiro ou agente alheio à investigação. O caráter tendencialmente pessoal dado à investigação leva a que cada prova seja recolhida, manuseada, analisada e fundamentada por apenas um perito ou conjunto de peritos tecnicamente qualificados e identificados no processo em que a prova fora obtida e analisada.

O derradeiro princípio que deverá reger a prova digital consiste numa *responsabilização repartida dos vários intervenientes na produção da prova no respeito dos princípios forenses digitais*. Caberá a cada agência ou perito a responsabilidade por recolher, aceder, armazenar e transferir a prova sob a sua alçada investigativa. Estando os técnicos e os organismos intervenientes na investigação obrigados a respeitar os princípios relativos à produção e análise forense, assegura-se, de forma complementar e cumulativa, o valor probatório e a integridade da prova objeto da investigação forense digital.

Concluindo, para garantir a validade da prova digital no decurso do processo de investigação, as fases processuais da prova deverão ser regidas por regras de cumprimento

[30] RODRIGUES, Benjamim Silva, *ob. cit.*, Coimbra Editora, 2009, pág. 728

imperativo. Para tal, releva, por exemplo, a documentação de qualquer operação efetuada e a intervenção no processo de peritos tecnicamente aptos para garantir admissão da prova.

2.4. Leis Reguladoras

O panorama processual penal atual em matéria de prova digital engloba, essencialmente, três diplomas legais: a Lei n.º 109/2009, de 15/9, complementada com o Código de Processo Penal e a Lei n.º 32/2008, de 17/7, distintos e aplicáveis para aspetos específicos da mesma realidade. Com a permanência de três diplomas, o Código de Processo Penal vê a sua desejável predominância normativa ameaçada pela constante descodificação causada pela sua dissemelhança, levando, frequentemente à incoerência e o insucesso prático das soluções legais.

Assim, estando *"mergulhada num verdadeiro pântano prático e, sobretudo, normativo"*[31], a prova digital necessitará de uma intervenção legislativamente coerente.

No entanto, em matéria de prova digital, o panorama legislativo atual revela incoerências, sendo de tal forma complexo, que nos podemos deparar com duas situações aquando do confronto normativo das leis existentes: ou estas se autonomizam ou convergem, superando-se sucessivamente, dificultando a função interpretativa. Ao seguir o caminho legislativo pluralista, o legislador anarquizou o sistema, não permitindo ao espírito e à letra da lei a melhor interpretação, complicando a sua aplicação legal.

2.4.1. Código de Processo Penal

Após a análise do panorama legislativo anterior a 2009, é impossível contestar que a recolha da prova digital não se encontrava prevista. No entanto, a sua consideração legal era demasiado restrita. A versão originária do Código de Processo Penal consagraria uma extensão legal ao regime disposto para as interceções e gravações das conversas telefónicas, como "*comunicações transmitidas por qualquer meio técnico diferente do telefone"*. Tal definição seria alvo de contestação doutrinal, sendo apenas esclarecido o conceito com o artigo 190.º da Lei n.º 59/98, de 25/8, englobando no seu âmbito de

[31] CORREIA, João Conde, *Prova Digital: as leis que temos e a lei que devíamos ter*, RMP, nº 139 (Julho-Set 2014), pág. 30

aplicação as comunicações à distância através de serviços informáticos fornecidos por uma rede de telecomunicações.

A revisão do Código de Processo Penal de 2007 voltaria a alargar o âmbito de aplicação do artigo 190.º, que passaria a 189.º, regulando os dados informáticos armazenados em suporte digital[32].

Sendo considerado o regime das escutas telefónicas como o "*quadro global da regulação da intercepção e registo de telecomunicações*"[33], mais uma vez, o legislador viu-se alvo de críticas doutrinais e jurisprudenciais. DÁ MESQUITA interpreta as alterações a este regime como uma clara falta de exigência conceptual no pensamento sobre a teleologia e a semântica da prova face à evolução tecnológica e à sua relevância na interação comunicacional e registo de dados, e como uma falta de respeito pelas exigências internacionais, que deveriam relevar na atuação legislativa portuguesa.

Denominado por COSTA ANDRADE como *"casa dos horrores hermenêuticos"*[34], o artigo 189º engloba várias realidades distintas, necessitadas de tutela e exigências distintas, causando incerteza e insegurança jurídicas e dificultando o controlo, por parte das instâncias formais competentes. Partilhamos da visão do mesmo autor, pois, ao integrar o *e-mail* guardado no computador no regime das escutas telefónicas, a investigação criminal é posta em causa, visto que passa a garantir ao meio informático um regime mais estável do que ao regime das escutas.

Ambas as provas estariam, assim, analogicamente reguladas pelo mesmo diploma. No entanto, ao acrescentar o preceito *"mesmo que se encontrem guardados em suporte digital"*, o legislador, não só põe em causa a prova telefónica, como desconsidera o interesse investigativo, ao impossibilitar a interceção de comunicações eletrónicas ou a obtenção dos dados de tráfego relativos a crimes informáticos, como a injúria ou a coação[35]. Trata-se, claramente de lapso do legislador que, ao submeter o correio eletrónico ao regime das escutas telefónicas, limita os meios excecionais de investigação, sujeitando-

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

[33] MESQUITA, Paulo Dá, *Processo Penal, Prova e Sistema Judiciário*, 2010, Coimbra, Coimbra Editora, pág. 89

[34] ANDRADE, Manuel da Costa, *"Bruscamente no verão passado", (...)*, Coimbra Editora, 2009., pág. 185

[35] Ibidem, pág 185 e 186

os ao catálogo previsto no artigo 187.º, n.º 1., do CPP e impedindo que, nos crimes em que a intromissão seria mais necessária, a sua investigação seja favorável.

Na crítica jurisprudencial, destacam-se acórdãos como os do Processo n.º 1396/08.1PBGMR – A.G1, do Tribunal da Relação de Guimarães, de 12/10/2012 e do Processo n.º 896/07.5JAPRT.P1, do Tribunal da Relação do Porto, de 27/1/2010[36]. Esses são exemplos de interpretação *contra legem* do preceito, não aplicando o previsto no artigo 189.º, em casos de apreensão de mensagens de telefone (ou *SMS's*) armazenadas após serem lidas pelo destinatário, equiparando-se ao arquivo recebido, lido e guardado.

Assim, estamos perante uma disposição processual demasiadamente limitadora, com natureza restritiva de admissibilidade de utilização, gerando um obstáculo processual na investigação dos crimes informáticos. A utilização dessa prova apenas seria possível em processos correspondentes a crimes previstos no artigo 187.º, n.º 1 do CPP, excluindo-se o seu recurso em processos onde seria essencial a sua recolha. Por exemplo, a investigação forense do crime de *reprodução ilegítima de programa protegido*, previsto na Lei do Cibercrime, não podia fazer uso da prova digital, uma vez que não preenche o requisito legal do artigo 187.º, n.º 1, correspondendo-lhe uma pena de prisão inferior a 3 anos.

2.4.2. Lei nº 32 / 2008, de 17 de Junho

Em 2007, seria alterado o Código de Processo Penal. No entanto, o legislador perde a oportunidade para inserir no novo diploma as medidas previstas pelo Parlamento Europeu e pelo Conselho. Assim, de forma a transpor para a ordem jurídica interna a Directiva n.º 2006/24/CE, do Parlamento Europeu e do Conselho, de 15/3, é emitida a Lei n.º 32/2008, de 17/7, uma lei extravagante, visando regular a conservação e transmissão dos dados de tráfego e localização, e os dados relevantes para a identificação do utilizador, garantindo a investigação e futura repressão de crimes graves.

Na existência de um catálogo restritivo de crimes, a transmissão de tais dados depende de despacho fundamental do juiz de instrução criminal, se este os determinar indispensáveis para a descoberta da verdade, sendo impossível ou bastante difícil de a alcançar sem tais provas. Para tal, o artigo 9.º, n.ºs 1 e 2 da dita Lei defendem a

[36] Também se incluem nesta linha de entendimento o ATRC de 29-03-2006 (Proc. n.º 607/06), da ATRL's, de 20-03-2007 (Proc. n.º 7189/2006 – 7), e de 15-07-2008 (Proc. n.º 3453/2008), consultável em www.dgsi.pt.

necessidade de serem respeitados os princípios da adequação, da necessidade e da proporcionalidade. O número 3 do dito artigo restringe ainda esses dados transmissíveis apenas aos referentes ao suspeito/arguido, ao suspeito de receber ou transmitir as mensagens em causa, ou à própria vítima, mediante o seu consentimento.

Assim, podemos considerar que, ao manter inalterados os requisitos de acesso e ao consagrar normas gerais no Código de Processo Penal e normas especiais na Lei n.º 32/2008, o legislador tornou este regime especial num regime desnecessário, sem motivo para se denominar como autónomo. Esta duplicação de regimes seria solucionada se o acesso aos dados se regulasse pela lei geral, autonomizada da legislação extravagante, que apenas regularia as questões técnicas à sua conservação preventiva, mantendo-se a centralidade normativa da lei processual penal.

2.4.3. Lei nº 109 / 2009, de 15 de Setembro

Em vigor desde 1991, várias foram as vozes criticando a desadequação da Lei da Criminalidade Informática, criada com o objetivo de a combater eficazmente. A inovação da Lei da Criminalidade Informática de 1991 esgotou-se com a passagem do tempo e o desenvolvimento da criminalidade, com o aparecimento de novas formas de atuação[37], revelando-se insuficiente dezoito anos depois.

Revogando a LCI, a Lei do Cibercrime apresenta na sua estrutura normas penais materiais, acabando apenas por adequar a lei precedente às novas exigências internacionais e nacionais. Dentro dessas novas exigências tidas em conta, constava um regime jurídico da obtenção da prova digital, regulando a obtenção da prova no crime informático.

Como referido, para a implementação do regime de obtenção da prova digital em Portugal, relevou a assinatura da Convenção sobre o Cibercrime em 2001, que surgia no panorama internacional como resposta às crescentes preocupações da comunidade internacional ao crescimento de uma criminalidade tecnologicamente avançada, visando uma união de esforços para uniformizar práticas de prevenção e repressão. Seria em 2009 que Portugal ratificaria a matéria disposta na Convenção, com a aprovação da Lei do

[37] MARQUES, Maria Joana Xara-Brasil, *Os Meios de Obtenção de Prova na Lei do Cibercrime e o seu confronto com o Código de Processo Penal*, Dissertação apresentada no âmbito do Curso de Mestrado Forense da Universidade Católica Portuguesa, sob orientação do Prof. Dr. Henrique Salinas, Lisboa, 2014, pág. 8.

Cibercrime, introduzindo no ordenamento jurídico português, o primeiro regime português de recolha da prova digital.

3. Lei do Cibercrime

Com a entrada em vigor da Lei n.º 109/2009, adapta-se o direito interno ao definido pela Convenção sobre o Cibercrime, com a transposição da Decisão-Quadro n.º 2005/222/JAI, do Conselho, de 24/2, relativa a ataques contra sistemas de informação.

Apesar do caráter necessário da Convenção, e de estar imposto aos estados membros legislar sobre matérias transfronteiriças, foram precisos oito anos para que a Convenção fosse oficialmente ratificada no ordenamento jurídico português. Falhando os prazos estabelecidos para a transposição da Convenção e da Decisão-Quadro de 2005 na sua ordem jurídica[38], o legislador precipita-se e cria um diploma extravagante, de aplicação geral, abrangendo as disposições penais materiais, processuais e de cooperação internacional num diploma único, em vez de proceder a uma alteração das fontes normativas no âmbito da cibercriminalidade[39]. Como referimos anteriormente, viria ainda a sobrepor-se ao regime da Lei n.º 32/2008, em matéria de acesso aos dados gerados e tratados relativamente a comunicações eletrónicas, reforçando a ideia de confusão da parte do legislador.

Em matéria de disposições penais materiais, o legislador excluiu o catálogo de crimes informáticos do Código Penal, mantendo o catálogo de crimes de Devassa por meio de informática e de Burla Informática, expostos nos artigos 193.º e 194.º, respetivamente. A Lei do Cibercrime engloba entre os artigos 3.º e 8.º, os crimes de Falsidade Informática, Dano relativo a programa ou outros dados informáticos, Sabotagem Informática, Acesso Ilegítimo, Interceção Ilegítima, e Reprodução Ilegítima de programa protegido. Apesar de ser "*do Cibercrime*", esta lei engloba no seu regime os crimes informáticos *stricto sensu*, já então previstos; aqueles que sejam cometidos por meio de um sistema informático; e aqueles em que seja relevante aceder a métodos de escolha e prova em suporte eletrónico (artigo 11.º, n.º 1).

[38] A Decisão-Quadro 2005/222/JAI deveria ser transposta em 16/3/2007, e o prazo de implementação as medidas da CCIBER terminava em 23/1/2001.
[39] Exposição dos motivos da Proposta de Lei n.º 289/X/4ª.

Assim, a Lei nº 109/2009 passa a ter como foco central a matéria de prova, plasmando as disposições processuais no seu capítulo III, prevendo entre os artigos 12.º e 26.º, o catálogo de meios de obtenção de prova. Com a Lei do Cibercrime, o legislador garante à justiça portuguesa um sistema processual de prova digital capaz de satisfazer as exigências internacionais, pondo de lado o improviso e contradição, que outrora se fazia sentir na busca pela verdade e pela justiça.

O panorama legislativo português exigia do legislador a adaptação do Código de Processo Penal ao desenvolvimento digital, em questões de âmbito processual penal. No entanto, a esperança não trouxe consigo os frutos expectados, mantendo-se a predominância processual penal para o espaço físico, cabendo nesse campo apenas o regime das escutas telefónicas, presente no artigo 189.º do CPP, convocado para todas as comunicações transmitidas por qualquer meio distinto do telefone ou guardado em suporte digital.

Tal como supra referido, o legislador incorria num claro atraso na transposição de Decisão-Quadro de 2005 e da Convenção sobre o Cibercrime de 2001. No entendimento de COSTA ANDRADE, ao ignorar as matérias de criminalidade informática, o legislador falhou ao aproximar o ordenamento jurídico português dos restantes[40]. O legislador viria a expor os motivos dessa "*redutora revisão*"[41] ao Código, alegando que serão as normas de direito processual penal que sofrem de maior desadequação no panorama legislativo internacional. Ao limitar a possibilidade de realizar interceção de comunicações telefónicas e eletrónicas, não incluiu normas especiais para reger as questões de Cibercriminalidade. A opinião do acima mencionado autor,seria um dos fatores de motivação do ordenamento jurídico para cumprir com as suas obrigações internacionais e alcançar os restantes ordenamentos jurídicos.

Esta perceção de que o texto processual penal não se adequa às necessidades e contexto internacional viria a ser limitada por JOÃO TIAGO SILVEIRA, secretário de Estado da Justiça em funções em 2009, ao afirmar a conformidade da lei com a resolução

[40] COSTA ANDRADE (2009; 337) defende ainda que "*foi uma chamada a que o legislador português de 2007 quis faltar, aproveitando a oportunidade para alargar o fosso da divergência face aos avanços de outros ordenamentos jurídicos*".

[41] Opinião partilhada por JULIANA BARROS in *O Novo Processo Penal: Os Meios de Obtenção de Prova Digital consagrados na Lei 109/2009, de 15 de Setembro*, Coimbra, 2012, pág. 44.

prevista no CPP, sem haver necessidade de alteração[42]. Por outro lado, o caráter de aplicação geral destas medidas processuais, por força da alínea c) do n.º 1 do artigo 11.º, encontra-se adequado ao artigo 14.º da CCIBER. Assim, abrange o seu âmbito de aplicação a qualquer crime tipificado na lei e cometido através de um sistema informático, sendo útil para a sua investigação a recolha da prova digital.

Tratando-se de medidas e obrigações de aplicação geral, às regras previstas no diploma não correspondem normas processuais relativas a cibercrimes ou crimes praticados em sistemas informáticos, mas um regime de prova eletrónica em processo penal com maior abrangência sobre qualquer crime[43].

A urgência em ratificar as medidas processuais impostas pela comunidade internacional levou o legislador a invocar princípios de necessidade e proporcionalidade e a admitir medidas mais radicais e inovadoras do que aquelas previstas para os regimes das escutas telefónicas e das ações encobertas, ampliando a sua aplicabilidade a crimes que não constam do seu catálogo. Sendo medidas subsidiárias, de *ultima ratio,* prevendo-se possíveis danos para os visados, deveria ser previsto como um todo, relevará a proteção de valores constitucionais. Não deverá esse regime dispersar-se em leis avulsas, prejudicando o raciocínio analógico, esgotando a sua força probatória (artigos 32.º, nº 8 da CRP e 126.º da CPP).

Devemos, assim, questionar as razões desta dispersão legislativa, onde podemos encontrar um regime de aplicação geral em legislação extravagante, gerando dificuldades de interpretação e aplicação legislativas. Foi no texto de proposta de lei que o legislador enunciou as razões, correspondendo à opção legislativa que mais se aproxima da tradição portuguesa, referindo-se à emanação, especialmente na área penal, de diplomas avulsos estruturantes de matérias especiais, como por exemplo, a criminalidade fiscal ou económica. Advoga ainda ser usual a sistematização de todas as normas referentes a um específico setor de especialidade, em vez de incluir essas normas, que se aplicariam a um grupo restrito, em diplomas estruturantes do ordenamento penal.

No entanto, partilhamos da opinião de autores como JULIANA BARROS ao conotar essas razões de serem vazias de racionalidade lógica[44]. A autora defende que essa prática disposta pelo legislador como justificação de serem estipuladas tais regras

[42] Diário da República, I Série, nº 120/X/4ª, de 10/7/2009.
[43] MESQUITA, Paulo Dá, *ob. cit.*, 2010, pág. 98.
[44] BARROS, Juliana Isabel Freitas, *ob. cit.*, pág. 46.

processuais de obtenção da prova digital em diplomas extravagantes não corresponde a uma realidade tão cabal como defende. Não se estabelecerão regras de aplicação geral, quando referentes a leis especiais como regras especiais, afetas a um tipo particular de crimes.

Quanto ao segundo fundamento apontado, a realidade corresponde à maior conveniência em inserir este regime geral no código, evitando-se um complexo trabalho jurídico, e facilitando o trabalho do operador jurídico. Tal entendimento encontra confirmação em autores como DÁ MESQUITA defendendo que a "*integração das regras no Código de Processo Penal*" deveria seguir o exemplo do ordenamento jurídico italiano[45]. Em Itália, a atuação legal não passou pela criação de um regime jurídico autónomo e específico para o regime da recolha de prova, mas por alterar o Código de Processo Penal, adaptando os meios de obtenção da prova, com a inclusão de disposições processuais. No entanto, o legislador português tendia a inspirar-se na lei alemã. Ao estabelecer um diploma legal, que contivesse as disposições referentes à cibercriminalidade, cria-se um verdadeiro sistema unificando todos os meios de investigação, garante o respeito pela intimidade e não remete o recurso dos meios ocultos de investigação para as leis extravagantes[4647].

3.1. Os Meios de Obtenção da Prova na Lei do Cibercrime

Como supra mencionado, a Lei do Cibercrime abrange um conjunto de disposições penais materiais, processuais e de cooperação internacional. Trata-se de uma lei inovadora, dando, pela primeira vez, relevância ao campo processual no regime da prova digital, deixando a jurisprudência de limitar a recolha de dados de tráfego aos crimes de catálogo, seguindo a intervenção do juiz[48].

---

[45] MESQUITA, Paulo Dá, *ob. cit.*, pág 101.
[46] COSTA ANDRADE, Manuel da, *Bruscamente no Verão Passado (...),* Coimbra Editora, 2009, pág. 24.
[47] A lei alemã viria mesmo a chegar mais longe, admitindo meios ocultos de investigação, mesmo que lesivos, como as buscas online, que ponham em perigo a vida, a liberdade ou a integridade física da pessoa investigada. in NEVES, Rita Castanheira, *As Ingerências nas Comunicações Electrónicas em Processo Penal – Natureza e respectivo regime jurídico do correio electrónico enquanto meio de obtenção de prova*, Coimbra; Coimbra Editora, 2011, pág. 104.
[48] ATRL, de 22-01-2013, que afirma que a LC superou a Lei n.º 109/91, "*que, por não conter essas normas processuais que adequassem o regime legal às particularidades da investigação "empurrou" a jurisprudência para a interpretação de que só em relação a crime de catálogo seria possível a obtenção de certo tipo de dados como os dados de tráfego à mercê da intervenção do juiz de instrução*.".

Foi, assim, relevante para preencher uma lacuna existente no ordenamento processual português, fornecendo ao sistema processual penal normas quanto à obtenção de dados de tráfego e realização de interceções das comunicações e alargando a sua aplicação a crimes cometidos por meio informático ou processo criminal em que seja necessária a obtenção da prova digital[49].

No âmbito das medidas processuais penais para a recolha da prova digital, estabelecidas com a Lei n.º 109/2009, a Convenção sobre a Cibercriminalidade estabelece quatro grupos fundamentais para a realização de uma investigação forense digital eficiente por parte dos Estados-Membros. Entre os títulos 2 e 5 da Secção 2 do relatório da citada Convenção, encontram-se:

1. a "Conservação expedita e divulgação parcial de dados informáticos", que se desdobra em Preservação Expedita de dados (artigo 12.º), Revelação Expedita de dados (artigo 13.º) e Injunção para apresentação ou concessão de acesso a dados (artigo 14.º);
2. a "Injunção", a que correspondem a pesquisa de dados informativos (artigo 15.º), a apreensão de dados informáticos (artigo 16.º) e a apreensão de correio eletrónico e registo de comunicações de natureza semelhante (artigo 17.º);
3. a "Busca e Apreensão de dados informáticos armazenados" e
4. a "Recolha em tempo real de dados informáticos relativos ao tráfego e ao conteúdo, englobando a Interceção de comunicações (artigo 18.º).

O legislador incluiu, ainda um regime inovador, permitindo a abertura de ações encobertas à investigação forense. PEDRO VENÂNCIO defende que este catálogo de medidas processuais deverá ser considerado de forma integrada, "*analisado como um todo, pois em muitos aspectos práticos se relacionam e complementam*"[50], visando o mesmo objetivo de aceder a dados informáticos necessários à investigação.

No entanto, a decisão do legislador português em inserir os preceitos determinados pela Convenção e pela Decisão-Quadro de 2005 numa lei extravagante, em detrimento de os inserir no texto do CPP, levaria que as incongruências normativas fossem camufladas, no decurso do cumprimento formal de transposição.

---

[49] Artigo 11.º da LC.

[50] VENÂNCIO, Pedro Dias, *Lei do Cibercrime Anotada e Comentada*, 1.ª ed., Coimbra, Coimbra Editora, 2011, pág. 99.

Tratando-se de métodos ocultos de investigação, que poderão, por vezes, ser intrusivos, será necessário um maior esforço integrativo na ordem jurídica, principalmente para garantir a sua constitucionalidade e a harmonização das fontes normativas já previstas[51]. Seguindo a opinião de autores como MARQUES DA SILVA, poderemos concluir que, a ordem pública sofre maior perturbação com a violação de direitos fundamentais da dignidade e da retidão da atuação judiciária, "*do que pela não repressão de alguns crimes, por mais graves que sejam, pois são sempre muitos, porventura maioria, os que não são punidos, por não descobertos, sejam quais forem os métodos de investigação utilizados*".

Assim, propomos seguidamente a analisar os métodos de obtenção da prova digital presentes na Lei n.º 109/2009, destacando as incongruências da sua aplicação.

3.1.1. Preservação Expedita dos Dados

Face às necessidades de colaboração das autoridades de investigação criminal, as empresas fornecedoras de serviços de telecomunicações requereram à Procuradoria-Geral da República um parecer relativo aos termos e conteúdo em que essa colaboração seria estabelecida.

Para tal, foi emitido o parecer n.º 16/94 e o respetivo parecer complementar, relativo à proteção dos dados informáticos. Inspirada pelas palavras de YVES POULLET e FRANÇOISE WARRANT, a Procuradoria Geral da República distinguiu *"fundamentalmente, três espécies ou tipologias de dados ou elementos; os dados relativos à conexão à rede, ditos dados de base; os dados funcionais necessários ao estabelecimento de uma ligação ou comunicação e os dados gerados pela utilização da rede (p. ex. localização do utilizador, localização do destinatário, duração da utilização, data e hora, frequência), dados de tráfego; dados relativos ao conteúdo da comunicação ou da mensagem, dados de conteúdo"*[52]. Entre os dados afetos a esta medida estão os Dados de

[51] COSTA ANDRADE defende a necessidade destes meios ocultos de investigação se regerem por um conjunto de requisitos, que permitam a sua validade constitucional: o princípio da necessidade, o princípio da reserva de lei, o catálogo de crimes, o princípio da subsidiariedade, o princípio da proporcionalidade, a suspeita fundada do cometimento de certo crime, e a inviolabilidade da intimidade e reserva do juiz. in *Bruscamente no Verão Passado (...)*, Coimbra Editora, 2009, pp. 109 ss.

[52] Parecer P000212000 da PGR, disponível em http://www.dgsi.pt/pgrp.nsf/0/58101f7b2b6fb7818025689e00501437?OpenDocument e acedido a 08-01-2016

Tráfego, definidos no artigo 2.º da Lei 109/2009 como "*os dados informáticos relacionados com uma comunicação efetuada por meio de um sistema informático, gerados por este sistema como elemento de uma cadeia de comunicação, indicando a origem da comunicação, o destino, o trajeto, a hora, a data, o tamanho, a duração ou o tipo do serviço subjacente*".

A obtenção de dados de base como a identificação e a morada do utilizador do serviço deverá iniciar-se com o pedido do Ministério Público. Se pretender obter informação mais alargada quanto ao tráfego, deverá solicitá-lo com autorização judicial[53]. Não será através da identificação do endereço IP, ou da identificação do utilizador em determinado dia ou hora, que o investigador verá revelada informação confidencial ou o percurso da comunicação e eventual tráfego comunicacional do visado. Com esses dados, apenas será possível ao investigador confirmar que determinada comunicação foi efetuada através daquele número técnico de acesso à Internet, estabelecendo ligação entre uma comunicação já conhecida e a sua origem.

Assim, de forma a proteger a investigação face à fragilidade de uma prova instável, o artigo 12.º da Lei n.º 109/2009 prevê a medida da preservação expedita de dados de tráfego, por determinação das autoridades judiciárias a terceiros que cuja esfera jurídica não seja afetada pela Lei n.º 32/2008. Esta medida consiste numa imposição aos fornecedores de serviços de comunicações de conservação dos dados essenciais à descoberta da verdade no processo criminal, para serem utilizados em processo quando o investigador se depare com criminalidade grave, e apenas mediante despacho fundamentado por juiz. Vários autores denominam tal processo de "*quick freeze*"[54], obrigando os fornecedores a "congelarem" os dados perante essa notificação.

Esta trata-se de uma medida cautelar, necessária para o bom decurso da investigação, procurando preservar os dados informáticos armazenados num sistema informático, sejam eles um documento eletrónico (nos termos do DL n.º 290D/99, de 2/8), um programa de computador (nos termos do DL n.º 252/94, de 20/10) dados de conteúdo, pessoais (segundo a Lei 67/98, de 26/10) e dados de tráfego, onde se incluem os dados de

[53] ATRE, de 13 de Novembro de 2012, Processo n.º 315/11.2PBPTG-A.E1, disponível em http://www.dgsi.pt, consultado a 22-01-2016.
[54] RODRIGUES, Benjamim Silva, *Da Prova Penal – Tomo IV, Da Prova Electrónico-Digital e da Criminalidade Informático-Digital*, 1-ª Ed. Rei dos Livros, 2011, pág. 522

localização (de acordo com a Lei n.º 41/2004, de 18/8)[55]. Mesmo tratando-se de dados afetos à privacidade das pessoas visadas e ao direito constitucional de sigilo das telecomunicações, o objetivo da preservação expedita é a sua conservação por parte de quem tenha o seu controlo, e não o seu acesso, salvaguardando-os, sob pena de posterior indisponibilidade.

Omissa quanto à questão da autoridade competente para ordenar a conservação dos dados, à Lei n.º 109/2009 corresponderá, flexivelmente, o disposto na Lei n.º32/2008, recaindo essa competência no Ministério Público. Segundo o disposto no artigo 12.º, n.º 2, o órgão de polícia criminal terá competência para dar essa ordem, devendo estar previamente autorizado pela autoridade judiciária. Está, no entanto, prevista a possibilidade de este órgão de polícia criminal, agir sem essa autorização em situações de urgência ou perigo na demora, devendo notificar imediatamente o Ministério Público, por relatório, de acordo com o artigo 253.º do CPP.

Várias são as vozes críticas à Lei do Cibercrime por atribuir competências específicas aos órgãos de polícia criminal em determinadas matérias. Entre elas, SILVA RODRIGUES (2011: 522) considera serem questões demasiado sensíveis para lhes corresponder uma mera permissão posterior. Para além disso, critica a terminologia contraditória, não sendo aceitável uma permissão *a posteriori*, ou seja, deverá sempre pedir uma permissão antes da ocorrência, não podendo o juiz de instrução remediar uma violação constitucional já cometida.

A ordem de preservação deverá valorar três elementos fundamentais: a natureza, a origem e o destino dos dados, estabelecendo um período de conservação de três meses (n.º 3). Sendo notificado desta obrigação, o fornecedor deverá preservar os dados, garantindo a confidencialidade da aplicação da medida (n.º 4). No entanto, no decurso do artigo 12.º, o legislador não previu qualquer sanção a ser aplicada ao fornecedor que se negar a preservar esses dados, nem remeteu essa situação para alguma disposição de direito substantivo. Questionamos, assim, a atuação do legislador quanto à sanção aplicada aos detentores dos dados que se recusem a cumprir a ordem imposta, afirmando que este poderia ter optado pela solução adotada no número 1 do artigo 14.º, acrescentando "*...sob pena de punição por desobediência*" no número 4 do artigo 12.º.

[55] VENÂNCIO, Pedro Dias, *Lei do Cibercrime Anotada e Comentada*, 1.ª ed., Coimbra, Coimbra Editora, 2011, pág. 99

Após o acórdão do TJUE de 8/4/ 2014, seria declarada a invalidade da Diretiva 2006/24/CE[56], entendendo que estávamos perante a violação de direitos fundamentais da comunidade de cidadãos em geral, que vêem os seus dados conservados, quando apenas um grupo restrito de pessoas cometem tais crimes. Apesar desta declaração, o legislador português previu na Lei n.º 32/2008 requisitos rigorosos de utilização destes dados preservados, de forma constitucionalmente aceitável, abrangendo crimes graves, e exigindo-se despacho fundamentado do juiz. Assim, a lei mantém-se em vigor, graças ao catálogo de crimes e ao período de conservação previstos, e que não seriam afetados pela Diretiva. No entanto, deverá sempre ser tido em conta o princípio da proporcionalidade na medida aplicada. Se os dados não forem conservados pelo período de um ano, ou não forem alcançados em tempo útil, não se criará prova, provocando o insucesso da investigação[57].

No entendimento de COSTA ANDRADE[58], teremos de considerar um último perigo referente à conservação de dados por fornecedores privados. Tendo em conta que o setor das comunicações tem sido "*afectado pela desregulamentação, pela abertura à concorrência e pelas privatizações, a que acrescem os agrupamentos de vocação mundial que se vão constituindo entre os seus operadores*"[59], será relevante observar o impacto dos fornecedores de comunicações na investigação forense. Nas palavras de prezado autor, a privatização generalizada das empresas de telecomunicações, levou a uma "*privatização da investigação"*, confiando-lhes as tarefas de "*intromissão, intercepção e gravação de telecomunicações e, em geral, da produção e armazenamento de dados processualmente relevantes, bem como a sua apresentação ao processo penal*", podendo tratar-se de dados de comunicação ou de localização. Com os novos meios e procedimentos tecnológicos de comunicação, como a produção e transmissão de dados pela Internet, à disposição das entidades privadas, acrescem à sua esfera meios de obtenção de prova como as buscas online, a interceção de comunicações telefónicas através da Internet (VoIP). No entanto, esta inevitável intervenção privada, traz consigo sério risco de excessos aos sistemas de

[56]Disponível em http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054pt.pdf, acedido a 11-01-2016.
[57] RAMOS, Armando Dias, *A Prova Digital em Processo Penal: O correio electrónico*, Chiado Editora, 1.ª Ed., Nov. 2014, pág. 88.
[58] ANDRADE, Manuel da Costa, *Bruscamente no Verão Passado (...)*, Coimbra Editora, 2009, pp. 127-129.
[59] DESGARDINS, Bruno, e LEMAIRE, Jean-Paul, *Desenvolvimento Internacional da Empresa. O Novo Ambiente Internacional*, Lisboa, Instituto Piaget, 1999, pp. 54-55 e 247-248. No mesmo entendimento, MILITÃO, Renato Lopes, *A propósito da Prova Digital no Processo Penal*, pág. 268, disponível em http://www.oa.pt/upl/%7B53f46e96-536f-47bc-919d-525a494e9618%7D.pdf e acedido a 04-10-2015.

contacto entre o público e o privado. O reforço da dimensão das entidades privadas, como a Google, e dos indivíduos que as constituem, traz consigo a agravação destes perigos e da assimetria entre estas empresas e os seus utilizadores ou assinantes, individuais ou coletivos.

3.1.2. Revelação Expedita de Dados de Tráfego

Após ser notificado para preservar os dados de tráfego, o fornecedor de serviços deverá revelar de forma expedita à autoridade judiciária competente, quais os outros fornecedores de serviços envolvidos na comunicação em questão, permitindo uma identificação do serviço e a garantia de preservação dos dados de tráfego referentes à comunicação. Consciente de que, numa comunicação, existem vários fornecedores de serviços possuidores de dados de tráfego autónomos, o legislador exigiria uma coordenação dos dados dos fornecedores citados com os restantes fornecedores, de forma a serem identificados os pólos de comunicação.

Vários seriam os caminhos que o legislador poderia ter seguido, para validar a ordem de preservação dos dados. Segundo o artigo 12.º, estaria aberta a possibilidade de emitir ordem de preservação aos fornecedores, o que acabaria por ser demasiado moroso, face ao grau de mutabilidade do cibermundo; ou emitir uma ordem geral e conjunta, notificando os fornecedores conhecidos. No entanto, esta indicação de fornecedor do serviço, de forma a se estabelecer qual a via utilizada para realizar tal comunicação, leva a destacar no artigo 13.º da LC um pedido legislativo de cooperação dos fornecedores de serviços com a autoridade judiciária competente. Esta colaboração deverá ser feita pelas empresas prestadoras de serviços de telecomunicações em tempo útil, de forma a constituírem elemento relevante para a descoberta da verdade material, no decurso da investigação em curso. Assim, a obrigação do fornecedor que recebera ordem de preservação dos dados consistirá, não somente na proteção dos dados pretendidos, durante um certo período de tempo, mas também, segundo o art. 13.º, de "*indicar de forma expedita à autoridade judiciária ou órgão de polícia criminal, logo que o souber, outros fornecedores de serviços, através dos quais aquela comunicação tenha sido efetuada*."

Também será relevante o cumprimento do princípio da suficiência, salientado por SILVA RODRIGUES que "*de nada valerá a transmissão de dados cuja quantidade não*

seja suficiente para os efeitos de investigação criminal: (i) identificação, pela parte, dos fornecedores de serviços; (ii) dos fornecedores de serviços; e (iii) da via pela qual a comunicação foi transmitida."[60]

De seguida, caberá à autoridade judiciária competente determinar uma cadeia identificadora dos fornecedores visados, com vista a preservarem todos os dados relevantes para o processo, estabelecendo-se o percurso efetuado pela comunicação investigada.

Podemos, concluir, a necessidade de interrelação entre os artigos 12.º e 13.º, pois não bastará para os investigadores a ordem de preservação, sem tomarem conhecimento dos dados preservados. Assim, terão capacidade de decidir quais os dados merecedores de preservação no processo, se serão suficientes para identificar a origem e o destino da comunicação, e identificar a presença de outros fornecedores possuidores de dados de tráfego.

Os dados de tráfego, alvo da notificação de preservação e revelação por parte do fornecedor, não se encontram abrangidos pela defesa e inviolabilidade das comunicações, como se encontram, por exemplo os dados de conteúdo. Por serem considerados necessários para estabelecer o percurso da comunicação pode a ordem de preservação emitida pela autoridade judiciária ser dispensada, permitindo o seu conhecimento quase imediato. No entanto, tal entendimento não é unânime, não sendo mesmo defendido no nosso ordenamento jurídico. GOMES CANOTILHO e VITAL MOREIRA (2007: 213) incluem os dados de tráfego no âmbito de proteção do direito de inviolabilidade das comunicações, assumindo que para obter as informações necessárias para a investigação, bastará um exercício de dedução através dos dados constituintes da comunicação, como a identidade dos interlocutores e a duração e frequência das comunicações. Por sua vez, PEDRO VERDELHO (2004: 126 e 127) distingue dois tipos de dados de tráfego: aqueles registados por uma comunicação telefónica, e aqueles provenientes do acesso à Internet. Na sua esteira, "*o tráfego de comunicações na Internet gera registos e produz dados quanto ao percurso que essas mesmas comunicações utilizam entre o computador que lhes dá origem e aquele a que se destinam*". Aponta como exemplo o endereço IP, que permite ao computador a sua ligação à rede, como informação que não constitui dados de base, por não revelar a identidade ou a localização do titular, nem dados de conteúdo pois "*nada diz quanto ao teor da comunicação nem quanto ao seu emissor ou receptor*".

[60] RODRIGUES, Benjamim Silva, *Direito Penal – Parte Especial, Tomo I, Direito Penal Informático-Digital*, 2011, pág. 616

Assim, deveremos excluir de cogitação a inclusão dos dados de tráfego de uma comunicação efetuada por meio eletrónico no regime dos dados de conteúdo. No seguimento de LOPES e CABREIRO (2006: 75) através dos dados de tráfego, apenas se saberá "*o destino da comunicação electrónica, não se descobrindo nada acerca das pessoas concretas, pelo que não se está a violar o núcleo fundamental do direito à intimidade*." A neutralidade da informação permite adquirir informação concreta, quando confrontada com elementos alheios e anteriores ao estabelecimento da comunicação.

O Ministério Público será a entidade competente para dirigir o inquérito e selecionar os atos necessários para investigar a existência do crime, determinar os sujeitos processuais, quais as suas responsabilidades, e recolher as provas relevantes para o exercício da ação penal. Assim, a competência atribuída ao Ministério Público de exigir a revelação expedita de tais dados, exclui a possibilidade de esta medida se sobrepor ao direito constitucional de inviolabilidade das comunicações.

3.1.3. Injunção para Apresentação dos Dados

A Injunção, prevista no artigo 14.º da LC, corresponde a um mecanismo mais flexível, de menor intrusão nos direitos dos fornecedores de serviços, melhorando os resultados da investigação[61].

Deparando-se com ISP não cooperantes, a autoridade competente apresenta à entidade ou pessoa singular que tenha a disponibilidade dos dados necessários para a produção de prova, a imposição de os fornecer ao processo criminal a decorrer, "*sob pena de punição por desobediência*" (art. 14.º, n.º 1).

A figura de dados, aqui referida, transporta um conceito demasiado abrangente, chegando a revogar o artigo 9.º da Lei n.º 32/2008, por esgotar a sua utilidade[62], e englobando na sua esfera conceptiva o conceito de "dados informáticos específicos e determinados armazenados num determinado sistema informático" e o conceito de "dados relativos aos seus clientes ou assinantes". O artigo 14.º expõe no seu número 4 os vários

[61] No ponto 167 do Relatório Explicativo da CCIBER, verificamos que "*Por vezes, os dados de tráfego ou, pelo menos, alguns tipos de dados de tráfego, são partilhados entre os fornecedores de serviços envolvidos na transmissão da comunicação, para fins comerciais, técnicos ou de segurança. (…) Cada um deles tem em sua posse uma parte do puzzle, e cada uma destas partes necessita de ser examinada de forma a detectar-se a sua origem ou o seu destino.*", disponível em http://conventions.coe.int e acedido a 16-12-2015.
[62] BARROS, Juliana Isabel Freitas, *O Novo Processo Penal: Os Meios de Obtenção de Prova Digital consagrados na Lei 109/2009, de 15 de Setembro*, Coimbra, 2012, pág. 62.

tipos de dados que relevarão no decurso da investigação: "*o tipo de serviço de comunicação utilizado, as medidas técnicas tomadas a esse respeito e o período de serviço; a identidade, a morada postal ou geográfica e o número de telefone do assinante, e qualquer outro número de acesso, os dados respeitantes à faturação e ao pagamento, disponíveis com base num contrato ou acordo de serviços; ou qualquer outra informação sobre a localização do equipamento de comunicação, disponível com base num contrato ou acordo de serviços*". Tais dados denominam-se de dados de base, não sendo passíveis de salvaguarda por qualquer interesse público que assegure a proteção dos segredos profissionais ou do sigilo das telecomunicações. Porém, podem abranger uma relação contratual entre o utente e a operadora de telecomunicações, potenciando a quebra das bases de confiança que deverá fundamentar uma relação contratual.

Caberá ao Ministério Público a tarefa de analisar se a medida poderá ou não conter a revelação de dados de base. Se essa medida se revelar indispensável para a investigação, deverá solicitar ao juiz de instrução que a ordene, procedendo a uma ponderação de valores, procurando salvaguardar o direito constitucional do sigilo das comunicações.

De forma a proteger o processo de investigação do incumprimento desta ordem por parte do possuidor dos dados, o legislador incluiu "*medidas necessárias*", correspondendo a esse comportamento um crime de desobediência simples, punível com pena de prisão até um ano ou de multa até 120 dias. No entanto, concordamos com o entendimento de DÁ MESQUITA, quando critica o exagero do legislador em punir pelo crime de desobediência, considerando que, para os fins pretendidos, corresponde a uma medida processualmente desadequada, defendendo a aplicação de sanções pecuniárias compulsórias, favoráveis às exigências de celeridade do procedimento processual[63], repercutindo-se, adequada e proporcionalmente, de acordo com os interesses económicos e a capacidade financeira dos visados pela injunção.

Prevenindo a auto-incriminação do visado ou uma atuação processual desleal, que pusesse em causa o princípio da presunção da inocência, o legislador incluiu, no artigo 14.º, n.º 5, a proibição de dirigir a injunção ao suspeito ou arguido no processo[64]. A injunção visará os fornecedores de serviços, instituindo que sejam comunicadas ao

[63] MESQUITA, Paulo Dá; *Processo Penal, Prova e Sistema Judiciário*, Coimbra, 2010, pág 113.
[64] RODRIGUES, Benjamim Silva, *Da Prova Penal – Tomo IV, Da Prova Electrónico-Digital e da Criminalidade Informático-Digital*, 1-ª Ed. Rei dos Livros, 2011, pág. 524

processo qualquer informação relevante, contida sob a forma de dados informáticos ou qualquer outra forma, que detenha e que permita determinar o tipo de serviço de comunicação utilizado as medidas técnicas tomadas, o período de serviço e a localização do equipamento de comunicação.

O legislador português limita o uso da injunção no artigo 6.º da LC, excluindo o seu uso quanto a sistemas informáticos utilizados no exercício de atividades como a advocacia, médica, jornalística e bancária. Esta norma permite, tal como afirma SILVA RODRIGUES, esta imposição pretende defender profissionais, "*em nome dos valores ligados ao direito de defesa ou plenitude das garantias de defesa processuais penais, à privacidade ou reserva da intimidade ligada à saúde e que implica o sigilo dos dados "sensíveis" da saúde das pessoas, o sigilo bancário e o sigilo profissional do jornalista e a respectiva liberdade de informação e expressão implicadas, todos direitos com assento constitucional, nomeadamente, nos artigos 26.º, 34.º, 35.º, 37.º e 64.º da CRP 1976*"[65].

3.1.4. Pesquisa de Dados Informáticos

O artigo 18º da CCIBER recomendaria aos Estados-Membros a uniformização legislativa dos regimes de buscas e apreensão da prova no ambiente digital, salvaguardando-se do facto de esses dados informáticos não consistirem em provas tangíveis, necessitando de uma investigação criminal e ação penal distinta dos bens corpóreos[66].

Tratando-se de dados informáticos já armazenados, já não fazem parte de uma comunicação em curso, estando a autoridade policial competente autorizada a aplicar medidas como a apreensão do correio eletrónico, a interceção de comunicações (arts. 17.º e 18.º, respetivamente) ou a pesquisa de dados informáticos, prevista no art. 15.º.

Com esta medida de pesquisa dos dados informáticos, o legislador visa tornar o processo de acesso aos dados armazenados mais ágil, evitando possíveis consequências sofridas pelos visados face à entrada coerciva e à apreensão dos computadores e outras máquinas, para recolha da informação que estas contenham.

---

[65] RODRIGUES, Benjamin Silva, *Da Prova Penal, Tomo II, Bruscamente, A(s) Face(s) Oculta(s) dos Métodos Ocultos de Investigação Criminal*, 1.ª Edição, Rei dos Livros, 2010., pág. 445

[66] Ponto 184 do Relatório Explicativo da CCIBER, disponível em http://conventions.coe.pt e acedido a 11-01-2016.

Quanto ao objeto visado por esta medida, deixa de relevar o computador ou os repositórios eletrónicos digitais, como as *pen's* ou *CD's* (correspondentes à busca), pretendendo-se o acesso aos dados armazenados num sistema informático. Pelo regime das buscas, presente no CPP, a aplicação das regras dependeria da localização do objeto físico, adaptando-se consoante se encontrasse num domicílio ou num local reservado ou não se encontrasse acessível ao público. Por exemplo, se houvesse a suspeita de que o sistema informático em causa pertencesse a um cibercafé, não se trataria de uma busca domiciliária, aplicando-se o artigo 174.º. Por outro lado, se recaísse a suspeita sob um endereço *IP*, que levasse a uma determinada morada, será necessária a verificação dos requisitos da busca domiciliária presentes no artigo 177.º, cumprindo-se o princípio da proporcionalidade e evitando os possíveis danos causados com a intrusão coerciva no domicílio.

Assim, a possibilidade de aceder ao espaço digital, sem necessidade de intrusão no domicílio do visado esbate esta distinção, deixa de relevar a localização física do computador, visando as buscas a mera recolha dos dados contidos nos sistemas informáticos.

A aplicação do artigo 15.º deve, assim, ter em conta o regime previsto no artigo 174.º do CPP, para as buscas domiciliárias. Sempre que seja necessário para a produção de prova e descoberta da verdade material, a autoridade judiciária competente poderá autorizar, através de despacho, a pesquisa a um sistema informático e a recolha de dados nele armazenados, devendo presidir à diligência. No entanto, SILVA RODRIGUES admite que tal norma deverá ser restritamente interpretada, abrindo a possibilidade de se proceder à operação sem ser presidida pela autoridade ordenadora. Tratando-se de "*uma vasculhagem oculta de dados informáticos*", será necessário o cumprimento do artigo 32.º, n.º 4 da CRP, devendo a autorização ser sempre judicial[67].

O regime previsto no CPP transporia o número 4, do artigo 174.º, fixando o prazo de validade máximo da medida, estabelecido no artigo 15.º, n.º 2 em 30 dias, sob pena de tornar a prova inútil no processo judicial[68]. A autoridade deverá indicar na autorização qual o momento de início de contagem, evitando que o órgão de polícia criminal execute a ordem em momentos arbitrários ao processo, desrespeitando os princípios da legalidade e da atualidade. A Lei n.º 109/2009 transporia, ainda, no art. 15.º, n.º 3, a possibilidade de

[67] RODRIGUES, Benjamim Silva, *ob. cit.*, pág 525.
[68] *Ibidem.*

esta medida ser efetuada pelos órgãos de polícia criminal, sem autorização judicial, em situações especiais de urgência ou *periculum in mora*[69]. Possibilitando esta medida, através do consentimento do visado, não será permitido ao legislador inquinar a investigação consentida por escrito. Assim, coloca-se a possibilidade de o visado alegar não ter compreendido o que estaria a consentir ou má conduta por parte da autoridade policial, invocando os meios legais necessários para defender a sua posição e a proibição da prova obtida. Na alínea b), releva ainda o facto de os bens jurídicos em causa (vida, ou integridade pessoal) são irreparáveis, uma vez lesados.

A natureza excecional deste regime impõe o cumprimento dos requisitos previstos no art. 15.º, n.º 4. Tratando de criminalidade grave (como a prevista na alínea b) já citada), a diligência deverá ser imediatamente comunicada à autoridade judiciária competente, que apreciará a sua validação. Por outro lado, em qualquer situação, deverá seguir-se a elaboração de um relatório, dirigido à autoridade judicial competente (art. 253.º do CPP). Encontra-se legalmente previsto para o incumprimento destes requisitos a nulidade da atuação, afirmando SILVA RODRIGUES (2011: 527) a insustentabilidade da valoração, por se tratar de uma prova proibida.

Concluindo, o art. 15.º, n.º 5 estabelece a possibilidade de autorização de extensão da pesquisa inicial a outro sistema informático ou parte diferente do sistema já pesquisado, possibilitando o acesso legítimo aos dados a partir de um sistema inicial. Nestas situações, releva a agilização, particularmente em caso de perigo na demora, especialmente quando se considera a instabilidade da informação pretendida.

3.1.5. Apreensão de Dados Informáticos

Durante a supra mencionada pesquisa legítima a um sistema informático, o investigador pretende a descoberta de dados ou documentos relevantes e com força probatória para a descoberta da verdade material. A autorização, ordenação e validação da apreensão desses dados serão decretadas por despacho do Ministério Público, enquanto autoridade judiciária competente (art. 16.º, n.º 1). No entanto, o artigo 16.º prevê situações

[69] O legislador previu no artigo 15.º, n.º 3 as situações de exceção:
a) A mesma for voluntariamente consentida por quem tiver a disponibilidade ou controlo desses dados, desde que o consentimento prestado fique, por qualquer forma documentado;
b) Nos casos de terrorismo, criminalidade violenta ou altamente organizada, quando haja fundados indícios da prática iminente de crime que ponha em grave risco a vida ou integridade de qualquer pessoa.

excecionais, estando o órgão de polícia criminal autorizado a apreender os dados sem prévia autorização da autoridade judiciária, se durante o decurso da pesquisa legitimamente ordenada (art.º 15) se deparar com urgência ou *periculum in mora* (n.º 2).

Na eventualidade de tais dados serem reveladores de dados pessoais e íntimos, suscetíveis de pôr em causa a privacidade do suspeito ou de terceiro, constituindo um obstáculo à ponderação dos valores, independentemente do método de investigação aplicável, estes deverão ser analisados por um juiz, que irá ponderar a sua junção aos autos, tendo em conta os interesses do caso concreto e a sua força probatória. DÁ MESQUITA entende que a exigência recai sobre a cominação da proibição da prova relativa a dados afetos ao núcleo mais profundo da privacidade do visado.

Analisando as várias alíneas constituintes do artigo 16.º, a apreensão da prova, afeta aos n.ºs 1.º a 3.º, deverão ser apresentadas à autoridade judiciária num prazo máximo de 72 horas, para que esta proceda à sua validação. Para este regime de proteção de dados pessoais serão, ainda, relevantes os regimes diferenciados referentes às atividades de advocacia, bancária, médica e jornalística, estipulados nos estatutos profissionais correspondentes e nos artigos 180.º e 181.º do CPP. Assim, o artigo 16.º prevê ainda a salvaguarda do segredo profissional ou segredo de Estado (182.º do CPP), perante a apreensão de dados informáticos.

O n.º 7.º consagra a necessidade de serem satisfeitos os princípios da proporcionalidade e da adequação no decurso da investigação, como proteção dos interesses do caso concreto. Para tal, elenca as diferentes formas de atuação apreensiva, podendo: ser apreendido o "*suporte onde está instalado o sistema ou (...) estão armazenados os dados informáticos, bem como os dispositivos necessários à respetiva leitura*" (alínea a)); realizar-se uma "*cópia dos dados, em suporte autónomo*", incluindo-se no processo (alínea b)); preservar-se a integridade dos dados, "*por meios tecnológicos (...) sem realização de cópia nem remoção dos mesmos*" (alínea c)); ou eliminar-se de forma não reversível ou bloquear-se o acesso aos dados (alínea d)). Este catálogo de medidas permitirá que o princípio da proporcionalidade seja respeitado, permitindo que os investigadores escolham a medida mais adequada ao caso concreto. As medidas apresentadas nas alíneas c) e d) são, particularmente, relevantes, quando nos deparamos com dados nocivos para a sociedade, como programas de vírus ou de promoção de terrorismo, ou dados de conteúdo ilegal, como a pornografia infantil. O suspeito estará

temporariamente impedido de aceder aos dados, através de técnicas como a encriptação informática. Posteriormente, se a utilidade dos dados se esgotar no processo, poderá recuperar o acesso aos dados, ou estes serão eliminados, caso constituam perigo para terceiros.

Deverá, ainda, defender o princípio da presunção de inocência, dando preferência aos meios menos onerosos ao investigado. Isto é, se o computador, que constitui objeto de busca, se tratar de material de trabalho e modo de subsistência do arguido, a autoridade judiciária deverá devolver-lho com a maior brevidade possível.

O legislador consagrou, ainda, a imposição de os dados apreendidos serem certificados através de uma assinatura digital. Ora, tal matéria afasta-se do contexto da obtenção da prova digital, sendo a sua imposição alvo de discussão doutrinal. SILVA RODRIGUES (2011, 530-531) discorda com a aposição da assinatura digital, defendendo que a integridade da prova depende do "*seguimento das corretas etapas do método de obtenção de prova eletrónico-digital*, consagradas para manter a sua capacidade probatória. Em sentido contrário, PEDRO VENÂNCIO (2011: 114 e 115) interpreta a assinatura digital como uma medida de preservação, garantindo a integridade dos dados apreendidos relativamente a alterações posteriores à apreensão.

Se a apreensão for realizada através de cópia dos dados em suporte autónomo, o n.º 8.º impõe que esta seja feita em duplicado. SILVA RODRIGUES defende a necessidade de serem feitas cópias em triplicado, acrescentando-se às cópias entregues ao suspeito ou arguido, para a sua defesa, e às autoridades judiciárias, para a audiência de julgamento, uma terceira cópia, para reserva e salvaguarda[70]. Por sua vez, DIAS RAMOS propõe a alteração da palavra "cópia" por expressões como "clonagem" ou "cópia de imagem", por existirem ferramentas informáticas forenses para o efeito, evitando futuras alterações, não se pondo em causa a valoração da prova em futura sede de julgamento[71]. Já no entendimento de PEDRO VERDELHO, ROGÉRIO BRAVO e LOPES ROCHA[72], deve ser tido em conta o artigo 19.º da CCIBER, estabelecendo que todas as medidas aí presentes, com a exceção da "*mera apreensão de dados no seu suporte", são medidas*

[70] RODRIGUES, Benjamin Silva, *Da Prova Penal, Tomo II, Bruscamente, A(s) Face(s) Oculta(s) dos Métodos Ocultos de Investigação Criminal*, 2010, pp. 452-453

[71] RAMOS, Armando Dias, *A prova digital em processo penal: o correio electrónico*, Chiado Editora, 1.º ed. Novembro 2014, pág. 90

[72] VERDELHO, Pedro, BRAVO, Rogério, ROCHA, Manuel Lopes; *Leis do Cibercrime*, Vol. I, 2003, pág. 18, disponível em http://www.centroatl.pt/titulos/direito/imagens/excerto-ca-leisdoCibercrime1.pdf e acedido em 28-12-2015

específicas do espaço virtual", não se enquadrando nos "*conceitos actuais da lei processual*".

3.1.6. Apreensão de Correio Eletrónico e Registos de Comunicações de Natureza Semelhante

Outro ponto carecido de reforma no regime atual legal da prova digital recai sobre a tutela processual penal atribuída à figura do correio eletrónico e à sua apreensão, sendo alvo de vasta divergência doutrinal. Questiona-se se, tal como o correio tradicional, o correio eletrónico já recebido e lido, deveria ser tratado como um simples documento.

No entendimento de COSTA ANDRADE e RITA CASTANHEIRA NEVES, *"depois de recebido, lido e guardado no computador do destinatário, um e-mail deixa de pertencer à área de tutela das telecomunicações*"[73], passando a ser um ficheiro digital, estabelecendo-se como meio idóneo da busca em sentido tradicional, e sujeitando-se ao regime correspondente àquele a que ficam sujeitos os documentos que o visado cria e arquiva no seu computador. Até aí, enquanto comunicação poderia ser intercetado, tendo em conta os critérios de admissibilidade e formalismo exigidos para a interceção de comunicações, salvaguardando-se o direito de inviolabilidade das comunicações.

Por sua vez, PEDRO VERDELHO defendeu a aplicação do "*regime estabelecido para as escutas telefónicas para a fase de transmissão do e-mail, o regime da apreensão de correspondência para a fase em que o e-mail já chegou ao destino mas ainda não foi lido pelo destinatário e o regime da apreensão de normais ficheiros escritos quando o e-mail já foi aberto e lido pelo destinatário*"[74]. Por ter proferido tais considerações antes da ratificação da Lei do Cibercrime, será natural considerarmos que tiveram influência na formulação do atual artigo 17.º.

A nível jurisprudencial, várias foram as decisões judiciais em que este tratamento diferenciado foi destacado. Entre estas, encontramos o Acórdão do Tribunal da Relação de Guimarães de 12-10-2009[75], que afirma que a mensagem já recebida mas não aberta se distingue daquela recebida e aberta (assemelhando-se ao regime da correspondência por

---

[73] ANDRADE, Manuel da Costa, *Bruscamente no Verão Passado (...),* Coimbra Editora, 2009, pág. 157.
[74] VERDELHO, Pedro, *Apreensão do Correio Eletrónico em processo Penal*, RMP, Ano 25.º, n.º 100, Outubro-Dezembro, 2004, pp. 153-154; e *Técnica no novo C.P.P.: Exames, Perícias e Prova Digital*, Revista CEJ, 1.º Semestre 2008, n.º 9 (Especial), pp. 145-171.
[75] Processo n.º1396/08.1PBGMR-A.G1, disponível em http://wwwdgsi.pt.

correio tradicional). Ao contrário da não aberta, a mensagem recebida e aberta terá a mesma proteção que as cartas recebidas, abertas e já guardadas. Analisando coerentemente a referida norma legal, será possível considerar semelhantes os dois tipos de correspondência. No entanto, e apesar do seu elemento gramatical, o correio eletrónico aberto e armazenado será considerado um mero documento, semelhante a uma carta recebida, tornando mais fácil a sua apreensão[76]. Será essa semelhança que permitirá convocar as normas gerais, presentes no artigo 17.º da Lei nº 109/2009, de apreensão da correspondência para obter as restantes comunicações[77].

Presume, ainda, o mesmo regime para a mensagem recebida em telemóvel, pois, tendo em conta "*a natureza e finalidade do aparelho e o seu porte pelo arguido no momento da revista*", será natural que seja lida logo após a sua receção. À mensagem preservada em suporte digital, depois da sua receção e leitura, corresponderá a mesma proteção prevista para a carta em papel recebida, aberta e arquivada. "*Sendo meros documentos escritos, estas mensagens não gozam de aplicação de regime de protecção da reserva da correspondência e das comunicações*".

A falta de clareza do legislador com a criação do regime regulador da prova digital leva a dúvidas, que, de outra forma, seriam claramente dispensáveis, pondo em causa a autoridade atribuída aos defensores e, por sua vez, a referida doutrina[78]. A inclusão do artigo 17.º no ordenamento jurídico português, não traria consigo qualquer distinção entre as mensagens de correio eletrónico e registos de comunicações de natureza semelhante, armazenados num sistema informático, podendo já ter sido acedidas ou não pelo destinatário; e entre as mensagens a abrir ou abertas, e entre comunicações e arquivo informático. Tratando-se de uma clara interpretação analógica, a falta de distinção legal entre as duas figuras, não cabendo ao intérprete a tarefa de as separar, acaba por levar à prevalência do regime da correspondência aberta e lida face ao restante regime. Estas alterações legislativas valeram ao legislador críticas de alterações feitas incorretamente e abstenções legislativas. Segundo COSTA ANDRADE, "*o legislador deve resistir à tentação e ao primeiro impulso de responder com leis (...) ao primeiro sinal de surpresa,*

[76] Segundo o artigo 16.º da LC, para tal apreensão, bastará a intervenção legitimadora do magistrado do Ministério Público. Cfr. CORREIA, João Conde, *Prova Digital: as leis que temos e a lei que devíamos ter*, Revista do Ministério Público, nº 139 (Julho-Set 2014), pág. 41.

[77] Aos dados que não possam ser convocados, corresponderá o seu regime restritivo. in MESQUITA, Paulo Dá, *Processo Penal, Prova e Sistema Judiciário*, Coimbra, Coimbra Editora, 2010, pág. 118

[78] CORREIA, João Conde, *ob. cit.*, pág. 40

de factos ou de problemas para os quais pareça não haver resposta na lei. Como de todos os lados se reconhece, a criminalização deve ser sempre o ponto de chegada de uma determinada reflexão sobre a dignidade penal e a carência de tutela penal do facto[79].

Procurando atribuir ao correio eletrónico armazenado uma tutela superior a outros escritos, o legislador português previu a necessidade de proteger privacidade de autodeterminação informacional, reforçando a proteção dos arquivados que foram comunicação. O artigo 17.º remeterá para o regime de apreensão de correspondência previsto no artigo 179.º do CPP. Para a apreensão legítima do correio, estabelece-se a imposição de tais apreensões por despacho judicial, sob pena de nulidade expressa, cabendo ao juiz que autorizar a diligência, a primeira tomada de conhecimento do conteúdo da correspondência apreendida. Dentro deste regime, podemos encontrar o correio eletrónico já convertido em ficheiro autónomo, cabendo-lhe um ato da competência exclusiva do Juiz de Instrução Criminal. Segundo o artigo 268.º n.º 1 alínea d) do CPP, competirá ao juiz de instrução tomar conhecimento do conteúdo da correspondência apreendida, estendendo ao conteúdo do correio eletrónico. A sua violação constitui a nulidade da prova, remetendo ao regime da proibição da prova.

Na eventualidade de, por demora dos agentes envolvidos, serem perdidas informações úteis à investigação de um crime, o juiz poderá autorizar a abertura imediata do correio eletrónico pelo órgão de polícia criminal. De acordo com o disposto nos n.ºs 2 e 3 do art.º 252.º do CPP, poderá ainda ser suspensa a remessa de qualquer correspondência da estação de correios e fornecedor de serviço de telecomunicações, convalidando-se a ordem policial até 48 horas, sob pena de tal revalidação ser rejeitada. No entanto, SILVA RODRIGUES critica esta norma, afirmando que a remissão do art. 17.º para o art.º 179.º, n.º 3 do CPP padece de "*confusão legislativa*", pois "*já que a não ser que se admita uma (desproporcional) apreensão massiva dos correios eletrónicos, já que o juiz não está presente e somente pode seleccionar após leitura, então, verifica-se que foi infeliz o legislador ao esquecer a regulamentação complexa do artigo 179.º, n.º 3, do CPP, e ao esquecer a regulamentação inversa, a esta, consagrada no artigo 189.º, n.º 1 do CPP*"[80].

[79] ANDRADE, Manuel da Costa, *Bruscamente no Verão Passado (...)*, Coimbra Editora, 2009., pág. 37.
[80] RODRIGUES, Benjamim Silva, *Da Prova Penal, Tomo II, Bruscamente, A(s) Face(s) Oculta(s) dos Métodos Ocultos de Investigação Criminal*, 2010, pág. 454

Concordando com a premissa de CONDE CORREIA, a proteção da vida privada não constitui razão suficiente para privilegiar essa correspondência em relação à restante[81]. A partir da conclusão efetiva da transmissão, o destinatário poderá evitar legalmente a intromissão por parte do Estado[82], deixando de estar vulnerável e protegendo-se da curiosidade do Estado, especialmente em questões em que não corresponde a sua reserva. Assim, para ambos os casos, às necessidades de tutela basta o controlo judicial posterior (art. 16.º, n.º 3, da LC): por exemplo, o Ministério Público tem a possibilidade de apreender uma carta guardada, mas o mesmo não se passa quanto a um *e-mail* armazenado num computador.

3.1.7. Interceção de Comunicações

O art.º 18.º da Lei do Cibercrime prevê como medida de obtenção da prova digital a interceção de comunicações eletrónicas em processos correspondentes 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 electrónico, quando tais crimes se encontrem previstos no artigo 187.º do Código de Processo Penal*". No número 4 do artigo 34.º do CRP, o legislador limita a aplicação desta ingerência nas telecomunicações aos processos de natureza penal. Serão admitidas como meio de obtenção de prova para "*um determinado conjunto de crimes previamente definido por lei*"[83]. Tais interceções são consideradas num restrito âmbito de aplicação, devendo corresponder a um crime informático ou cometido por meio de um sistema informático ou em que seja necessário recolher prova em suporte digital, estando previstos no artigo 187.º do CPP.

Assim, a letra da lei leva à exclusão dos crimes que não entrem nos limites abrangidos por este catálogo legal, tratando-se, portanto, nas palavras de DÁ MESQUITA, de uma aplicação *"esquizofrénica da lei"*, demonstrando que a tentativa de adequar a ordem jurídica nacional às novas realidades não é exequível quando esta não se

[81] CORREIA, João Conde, *ob. cit,.* pág 41. O autor defende que "*Invocar o ritualismo da apreensão de correspondência quando já não há correspondência é um contra-senso*."
[82] ANDRADE, Manuel da Costa, *ob. cit.*, pp. 159-160; NEVES, Rita Castanheira; *As Ingerências nas Comunicações Electrónicas em Processo Penal (*…), Coimbra; Coimbra Editora, 2011, pp. 262-263
[83] SANTOS, Cristina Máximo dos, *As novas tecnologias da informação e o sigilo das telecomunicações*, Lisboa, 2004, separata da Revista do Ministério Público, n.º 99, pág. 96

autonomiza das normas legais anteriores (artigo 189º do CPP)[84]. Portanto, será inadmissível a manutenção formal do artigo 189.º CPP, por acarretar uma inoperatividade na interceção das comunicações. O artigo 18º da Lei do Cibercrime autonomizou duas cláusulas no seu número um, especificando na alínea a) que, nos casos previstos, a interceção não depende de qualquer requisito adicional, referente a qualquer moldura penal abstrata ou catálogo legal. Por sua vez, a alínea b) elenca requisitos adicionais, aplicáveis aos casos aí previstos. Por outro lado, da remissão para essa alínea b) deverá fazer parte os crimes de injúria, ameaça, coação ou devassa da vida privada cometidos por meio informático, alargando para o âmbito dos crimes praticados através do telefone, a investigação dos crimes praticados através de um meio informático.

Na sua máxima boa vontade, o legislador falhou em demonstrar a sua intenção, que se tratava de autorizar que a interceção das comunicações eletrónicas e a obtenção de dados de tráfego se realizem na investigação de crimes cometidos através de meios informáticos. Ao aludir para a alínea b) do número 1 do artigo 18.º, a remissão cai obrigatoriamente sobre o crime em causa (e não sobre a forma em que este é praticado).

Segundo os números 2 e 3 do artigo 18.º, as exceções ao sigilo que caracteriza as comunicações devem revestir forma de lei, devendo ser aplicadas por um magistrado judicial (artigo 32.º, n.º 4 da CRP).

Se as provas forem obtidas através de abuso de intromissão na vida privada ou nas telecomunicações, do artigo 32.º, n.º 8 da CRP prevê que seja declarada a sua nulidade.

Em matéria de interceção e registo de transmissões de dados informáticos, o legislador estabeleceu regras relativas às escutas telefónicas no art. 18.º, n.º 4, remetendo para os artigos 187.º a 190.º do CPP. Assim, aplicam-se os procedimentos e autorizações judiciais previstas para as escutas telefónicas às comunicações eletrónicas. Nas palavras de PEDRO VENÂNCIO, "*falamos da intercepção de mensagens de correio eletrónico em tempo real, ou seja, no seu trajecto do computador do emissor para o computador do receptor através da rede de servidores. Ou ainda a intercepção de mensagens trocadas através de processos de comunicação instantânea (usualmente designados por serviços de "chat", como são os casos do "IRC", do "MSN Messenger", ou do "ICQ"*[85].

Tratando-se de uma medida de ingerência nas comunicações, afetando o direito constitucional de sigilo que delas advêm, o artigo 384.º do CP prevê punição para a

[84] MESQUITA, Paulo Dá, *ob. cit.*, pág. 97
[85] VENÂNCIO, Pedro DIAS, *Lei do Cibercrime: Anotada e Comentada*, pág. 119

violação do segredo das comunicações por entidades públicas. Contrariamente ao estabelecido na criação da norma, em que as comunicações eram tuteladas por entidades públicas, atualmente o fenómeno da privatização atribuiu essa tutela a entidades privadas. No entanto, o artigo 194.º prevê a punição daquele que violarem a correspondência ou as telecomunicações, intrometendo-se e divulgando o conteúdo da comunicação a terceiro.

A Lei n.º 41/2004, reguladora a proteção de dados pessoais e privacidade nas comunicações eletrónicas, estabelece nos números 1 e 2 do artigo 4.º, a imposição de inviolabilidade das comunicações e dos dados de tráfego, por parte dos fornecedores de serviço. No entanto, o número 2 proíbe a interceção e a vigilância, sem consentimento.

Por sua vez, para aquele que detiver instrumentos destinados à montagem de escuta telefónica ou violação de telecomunicações, a lei prevê a sua punição no art. 276.º do CP. No entanto, estabelece um regime excecional nos 187.º, 188.º, 189.º e 190.º do CPP e o art. 18.º da LC, admitindo a interceção e gravação, mediante o cumprimento de requisitos e condições, sob pena de nulidade. O artigo 187.º determina que a sua autorização durante o inquérito dependerá de haver "*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*".

Tal intromissão encontra-se legitimada constitucionalmente pela negativa, ou seja, a Constituição não prevê a proteção das formas da proteção do direito fundamental à privacidade, quando se encontram integradas num ilícito criminal[86]. Não estando previstas na Constituição as formas de utilização abusiva deste direito, quando um caso hipotético compromete intoleravelmente o conteúdo essencial de outro direito, valor comunitário ou princípio fundamental da ordem constitucional, "*deverá resultar para o intérprete a convicção de que a proteção constitucional do direito não quis ir tão longe"*[87]. Assim, de forma a proteger o direito ao sigilo das comunicações, para que este não seja um mero instrumento para o insulto, a ameaça, a coação ou a devassa da vida privada, deverá caber ao Estado a tarefa de intervir, não devendo conceder aos crimes cometidos por telefone uma tutela processual penal superior aos crimes cometidos por via informática.

---

[86] CORREIA, João Conde, *Qual o significado de abusiva intromissão na vida privada, no domicilio, na correspondência e nas telecomunicações (art. 32.º, n.º 8, 2ª parte da CRP)?*, RMP (1999), 79, pp. 55-56

[87] ANDRADE, José Carlos Vieira de, *Os Direitos Fundamentais da Constituição Portuguesa de 1976*, Coimbra, Almedina, 2001, pág. 287

3.1.8. Ações Encobertas

O legislador português de 2009 alarga, ainda, as disposições sobre as ações encobertas, previstas na Lei n.º 101/2001, de 25/8 às tidas em ambiente digital[88].

O regime das ações encobertas é consagrado no artigo 19.º para os crimes previstos na Lei n.º 109/2009 e para crimes cometidos através de meio informático, correspondente a uma pena de prisão superior a 5 anos, ou inferior, se se revelarem dolosos como crimes contra a liberdade e a autodeterminação sexual de menores ou incapazes, a burla qualificada, a burla informática e nas comunicações, a discriminação racial, religiosa ou sexual e as infrações económico-financeiras. Para além destes, também serão abrangidos os crimes contra direitos de autor, visados no título IV do CDADC.

DÁ MESQUITA apresenta duas críticas referentes a esta norma. Se por um lado, o legislador ampliou de forma contundente o catálogo de crimes previsto no artigo 2.º do Regime Jurídico das Ações Encobertas, por outro, passa a prever uma medida excecional para um vasto conjunto de crimes, alguns de pequena criminalidade, sem aprofundar normativamente os princípios da proporcionalidade e da necessidade[89].

A realidade jurídico-criminal distingue duas condutas a adotar, sob as figuras do agente infiltrado e do agente provocador.

FERNANDO GONÇALVES, MANUEL JOÃO ALVES e MANUEL GUEDES VALENTE estabelecem o agente infiltrado como o funcionário de investigação criminal ou o terceiro, que atua sob a supervisão da Polícia Judiciária, ocultando a sua identidade, de forma a obter provas para incriminar o suspeito, visando a prevenção ou repressão criminal, através da obtenção de informações pessoais relativas à atividade criminosa por ele praticada[90]. O agente infiltrado visa, com a sua atuação, obter a confiança do suspeito, tornando-se um criminoso, conseguindo aceder a planos e informações, e retirar dados que consubstanciem prova de atos ilícitos.

---

[88] RODRIGUES, Benjamim Silva, *Da Prova Penal, Tomo II, Bruscamente, A(s) Face(s) Ocultas(s) dos Métodos Ocultos de Investigação Criminal*, pág. 456

[89] MESQUITA, Paulo Dá, *ob. cit.*, pág. 126

[90] GONÇALVES, F., ALVES, M. J., VALENTE, M. G, *O novo regime jurídico do agente infiltrado (Comentado e Anotado – Legislação Complementar),* Coimbra, Livraria Almedina, 2001, pp. 91-93. LAVOURA, Tiago Santos, *O agente infiltrado e o seu contributo para a investigação criminal*, Dissertação para obtenção de grau de Mestre em Ciências Jurídico-Forenses, orientado pelo Prof. Dr. Figueiredo Dias, e co-orientado pela Mestre Ana Pais, Coimbra, Instituto Superior Bissaya Barreto, pág. 35

O regime das ações encobertas previsto em vários países europeus consagra a figura do agente provocador, que visa combater crimes, como a pedofilia. Este cria o próprio crime, instigando o suspeito à sua prática[91]. No entanto, o ordenamento jurídico português não a consagra como prova admissível de valoração, por ocorrer á margem do paradigma previsto constitucionalmente, no nosso sistema jurídico[92].

Segundo SUSANA AIRES DE SOUSA (2004: 1233), esta distinção releva a dois níveis: quanto à "*determinação da responsabilidade penal substantiva daqueles sujeitos*"; e quanto "*tratamento jurídico-processual das provas obtidas e recolhidas*", tendo em consideração o consenso doutrinal e jurisprudencial admitindo as provas obtidas pelo agente infiltrado, mas considerando inválidas, incorrendo de nulidade, aquelas obtidas pelo agente provocador[93]. No entanto, a Lei de 2001 não esclarece a diferença entre ambos os agentes, focando apenas na responsabilização penal do agente instigador ou autor mediato, quando pratique atos preparatórios ou executórios. Assim, sendo essas provas nulas, o legislador estará, consequentemente, a declarar inconstitucional a Lei n.º 101/2001, por violar os artigos 25.º, n.º 1 e 32.º, n.º 8 da CRP[94].

COSTA ANDRADE defende a inclusão de uma terceira figura, o Homem de Confiança, que consiste no terceiro, não agente de polícia criminal, que atua no meio criminoso, sob orientação desses órgãos. Nessa figura, podemos incluir "*todas as testemunhas que colaboram com as instâncias formais de perseguição penal, tendo como contrapartida a promessa da confidencialidade da sua identidade e actividade. Cabem aqui tanto os particulares (...) como os agentes das instâncias formais, nomeadamente da polícia (...), que disfarçadamente se introduzem naquele submundo ou com ele entram em contacto; e que quer se limitem à recolha de informações (...), quer vão ao ponto de provocar eles próprios a prática do crime*"[95].

[91] LAVOURA, Tiago Santos, *ob. cit.*, pp. 21-22
[92] RODRIGUES, Benjamim Silva, *Da Prova Penal, Tomo II, Bruscamente*, 1.ª Edição, Rei dos Livros, 2010, pág. 130.
[93] SOUSA, Susana Aires de; *Agent Provocateur e meios enganosos de prova - Algumas reflexões, Liber Discipulorum* para Figueiredo Dias, 2003, pág. 1235.
[94] *Ibidem*.
[95] ANDRADE, Manuel da Costa, *Sobre as proibições de prova em processo penal*, Coimbra, Coimbra Editora, 1992, pág. 220.

4. Conjugação das Leis

Apesar do progresso verificado com a Lei do Cibercrime, o legislador coibiu-se de revogar as leis que lhe precederam, mantendo a sua existência formal, gerando um confronto desnecessário. Face à diferença de técnicas e à multiplicidade de objetos afetos ao caso, perante a diversidade processual penal, a não articulação entre as três normas dificulta a descoberta da norma jurídica passível de ser aplicada no caso concreto.

De um ponto de vista doutrinal, podemos considerar que a criação da Lei nº 32/2008 e nº 109/2009 levam a uma revogação tácita das normas do Código de Processo Penal que regulam a prova digital. Ao serem sobrepostas as leis extravagantes à lei geral, o âmbito de aplicação é restringido, sendo esta última apenas aplicável nas matérias não reguladas. Por essa situação, questionamos a decisão do legislador de não revogação.

Coloca-se, entretanto, outra questão, referente à relação entre as Leis n.ºs 32/2008 e 109/2009. Para esta relação, surgem duas teorias, uma minoritária, defendida por autores como Dá Mesquita, e outra aceite maioritariamente, defendida por autores como Benjamim Silva Rodrigues e Rita Castanheira Neves.

Para a tese minoritária, a Lei do Cibercrime veio revogar a norma legal referente ao acesso aos dados informáticos, apenas sendo relevante a Lei n.º 32/2008 em matéria de *"estabelecimento dos deveres dos fornecedores de serviços e prestação desses dados"*[96]. Assim, considera que esse seria o sentido útil da ressalva do legislador ao emitir o artigo 11.º, n.º 2 da LC, pois aquela lei apenas subsiste de modo a regular questões não salvaguardadas pela Lei do Cibercrime. No entanto, tal não será motivo suficiente para manter vários regimes de acesso como atualmente se verifica, sendo que estes regimes são diversificados e até contraditórios, comprometendo a investigação de crimes mais graves com a aplicação de exigências injustificadas.

Por outro lado, a tese dominante admite que ambas as leis se complementam (art. 11.º, n.º 2), cabendo ao intérprete delimitar os âmbitos de aplicação, em campos sobrepostos, mas contíguos[97]. Assim, passa a ser exigível um maior cuidado na investigação dos crimes mais graves, face a uma maior dificuldade de salvaguardar o acesso às informações obtidas com a conservação dos dados de tráfego, localização e de

[96] MESQUITA, Paulo Dá, *ob. cit.*, pág. 123

[97] NEVES, Rita Castanheira, *As Ingerências nas Comunicações electrónicas em processo Penal (...)*, Coimbra, Coimbra Editora, 2011, pp. pág 234; MILITÃO, Renato Lopes, *ob. cit.*, pág 275.

identificação do assinante ou utilizador registado. Por tal motivo, à imposição legislativa de conservação preventiva desses dados deveria corresponder uma restrição a esse acervo de informações, permitindo-se o acesso e utilização apenas aos casos em que um juiz o considere indispensável.

Debruçando-nos sobre a tese maioritária, deparamo-nos com a redução de protagonismo do Código de Processo Penal na investigação criminal, concluindo que as Leis n.ºs 32/2008 e 109/2009 acabaram por suplanta-la na maioria das matérias[98] em que tal nos deparamos com esse confronto, havendo entre ambas uma mútua complementaridade. Face à situação concreta, caberá ao julgador a tarefa de identificar, e posteriormente interpretar, o regime processual aplicável.

4.1. Incoerências e Omissões Legislativas

Ao implementar no panorama legislativo português técnicas de "*duvidosa legitimidade teórica e de nula eficácia prática*"[99], o legislador incorreu em omissões e lacunas inaceitáveis que surgem no decurso do processo, reforçando a sua inconsistência por estarem erradamente reguladas.

De seguida, exporemos essas questões que, não fazendo parte do catálogo de medidas previsto pela Lei do Cibercrime, merecem a nossa atenção e estudo, por levantarem dúvidas relevantes, necessitando de actualização da estrutura legislativa do Cibercrime.

4.1.1. Buscas *Online*

Segundo o ordenamento jurídico português, os dados contidos num computador podem ser acedidos por meio eletrónico pelo Estado. Assim, o Estado pode aceder a um computador alheio, verificando as informações que nele se encontram, sem ser necessário o consentimento do visado para observar, monitorizar e copiar.

---

[98] Apesar de ser "ultrapassado", o CPP será sempre implícito em matérias onde as leis de 2008 e de 2009 a ele se referirem, como os arts. 15.º, n.ºs 5 e 6, 17.º, 18.º, n.º 1, al. b), 19.º, n.º2 e 28.º), estando o seu intérprete sujeito à interpretação contínua das três leis, para alcançar a solução pretendida.

[99] CORREIA, João Conde, *Prova Digital: as leis que temos e a lei que devíamos ter*, RMP, nº 139 (Julho-Set 2014), pág. 56

Previstas no artigo 15º, n.º 5 da LC, as buscas *online* encontram-se consagradas legislativamente para situações em que surjam razões, durante a pesquisa, "*para crer que os dados procurados se encontram noutro sistema informático ou numa parte diferente do sistema pesquisado*", e que sejam acessíveis a partir do sistema inicial, estendendo a pesquisa mediante "*autorização ou ordem da entidade* competente". Assim, não estamos perante uma diligência oculta, desconhecida pelo visado, permitindo que o acesso ao primeiro sistema informático ponha em causa o secretismo da diligência e o assentindo o controlo da legalidade pelo visado.

Por outro lado, ao permitir ações encobertas através de meios informáticos, a letra da lei restringe, inequivocamente, o âmbito de aplicação das buscas *online* a estas ações, a título excecional.

Perante esta situação, partilhamos a questão colocada por CONDE CORREIA[100], e questionamos a razão de este mecanismo não ser utilizável noutras situações devidamente delimitadas, não estando prevista a consagração legal deste instrumento enquanto meio ordinário de prova. Assim, para ocorrências que ameacem a sobrevivência do Estado de direito deverá, de igual modo, estar disponível este meio excecional de intromissão.

A garantia constitucional de sigilo das telecomunicações[101] não abrange questões de confidencialidade ou integridade do sistema informático, limitando-se a proteger a transferência dos dados. Não estamos, assim, perante uma intromissão de telecomunicações, mas perante a esfera privada digital, pondo em causa a integridade e confidencialidade do sistema informático[102].

O caráter excecional e intrusivo previsto para estes novos procedimentos serão favoráveis para o visado. Ao serem realizadas diligências com o seu conhecimento, este terá a possibilidade de boicotar tal operação, através da entrega da coisa procurada ou controlo legal da duração, intensidade e respeito pelos pressupostos legais dessa autorização, através da intervenção de advogado. Por outro lado, esse controlo deixa de existir se a diligência lhe for oculta. A falta de autorização legal deste tornaria a busca *online* inadmissível, esgotando a sua força probatória com a ilicitude.

---

[100] *Idem*, pág. 43
[101] Art. 34.º, n.º 4 da CRP
[102] ANDRADE, Manuel da Costa, *Bruscamente no verão passado (...)*, Coimbra Editora, 2009, pp. 168-169

Apesar desse controlo, é possível um meio-termo, havendo margem de manobra constitucional na aplicação processual de tais medidas. Segundo o BVERFGE, a leitura e monitorização de dados através da infiltração oculta de sistemas informáticos alheios será constitucionalmente admissível em situações de perigo concreto para bens jurídicos individuais ou coletivos, que ameacem a sobrevivência do Estado de direito ou a própria existência humana, mediante a autorização judicial para esse efeito[103]. Tratando-se de uma estreita margem de disponibilidade constitucional, de caráter urgente e suplementar por parte do legislador, deverá abrir-se o âmbito de aplicação destas medidas para as formas de criminalidade mais extremas, de forma a garantir a manutenção do Estado de direito. Assim, o sistema processual penal terá possibilidade de resolver os problemas mais graves com que se depara.

4.1.2. Troca de Comunicações entre Máquinas

Apesar das aparentes inovações previstas pelo legislador português, não foi desenvolvido ordenamento relativo às comunicações entre máquinas, não expondo termos de investigação claros e relevantes para a segurança jurídica. Releva a não nitidez da distinção legal entre os dados de comunicação previstos no artigo 14.º da LC, não sujeitos a intervenção humana, e os dados referentes a comunicações falhadas ou realizadas, sujeitos a maior reserva legal. Por exemplo, o sigilo das informações disponibilizadas pelos aparelhos de telecomunicações não abrange a mera comunicação entre máquinas, por não ser considerado perigo potencial, passível da proteção do artigo 10.º da CRP. Tal artigo afeta, essencialmente, o portador de tal direito e a carência de tutela de terceiros intervenientes na dita comunicação. Ao ser identificado o IMSI ou o IMEI, não só é posta em causa a utilização de um telemóvel, como não concretiza o perigo para a privacidade ocorrente da utilização desse meio comunicativo[104].

Assim, não existe qualquer troca de informação, feita por um ser humano em relação ao conteúdo ou ao tráfego de uma comunicação, não se justificando a proteção desses dados para garantir a inviolabilidade das telecomunicações. Estas destinam-se a assegurar a capacidade de resposta do operador, ocorrendo a transmissão

[103] *Ibidem*.
[104] ANDRADE, Manuel da Costa, *ob. cit.*, pág. 162.

independentemente da ocorrência de qualquer comunicação. Os dados de tráfego passam a incluir apenas o registo dos impulsos comunicativos desencadeados por humanos, independentemente de ser certos ou falhados, excluindo-se desse conjunto os *"procedimentos de identificação do número de um aparelho de telemóvel ou do respetivo cartão"* e *"os dados de localização logrados através destes procedimentos"*, como por exemplo, os dados registados com o pagamento automático de portagens[105].

4.1.3. Pesquisa de Dados Informáticos, Perícias e Exames

A relação entre os textos legais vigentes para a temática da investigação no cibercrime é de uma evidente dificuldade de articulação. Entre os exemplos mais evidentes destaca-se a articulação entre a pesquisa dos dados informáticos, prevista no artigo 15.º da LC, e as perícias e exames, previstos respetivamente nos artigos 151.º e ss. e 171.º do CPP. Pendendo a escolha aplicativa no regime especial, em detrimento do geral, presume-se que a pesquisa dos dados informativos se sobrepõe ao regime dos meios de obtenção de prova previstos na lei processual penal, por se tratar da única forma legitima de aceder ao conteúdo do computador.

Apesar de a Lei do Cibercrime prever no artigo 11.º a aplicação processual do regime especial, excluindo a aplicação de outro preceito legal, tal não se verifica na realidade. O regime especial não invalida o regime geral, pois existem pressupostos e objetivos referentes à pesquisa informática, como a obtenção de dados informáticos específicos armazenados no computador, que poderão carecer de perícias ou exames ao mesmo, concordando com PEDRO VERDELHO, quando afirma ser "*errado ver nesta figura (pesquisa de dados informáticos), algum tipo de substituto para os exames"*[106]. A própria Lei do Cibercrime reconhece a possibilidade de aplicação de outras leis, ao regular nos arts. 16º e 17º a *"pesquisa informática ou de outro acesso legítimo a um sistema informático"*. Como tal, não será a única lei reguladora em matéria de aquisição processual de dados, afastando a exclusividade, *ab initio*, ao admitir outras leis.

4.1.4. Pesquisa Informática Consentida por quem dispõe ou controla os Dados

[105] *Ibidem*.
[106] VERDELHO, Pedro, *A nova lei do Cibercrime*, Scientia Juridica, LVIII, Braga, 2009, pag. 740

Perante o contexto jurídico-processual explanado, surge uma nova questão: o consentimento para a pesquisa informática necessário por parte daquele que obtenha a disponibilidade ou o controlo dos dados em questão. Este direito encontra-se previsto no art. 15.º, n.º 3 da LC, distinguindo-se do acordo prévio do visado pelo art. 174º, número 5, alínea b) do CPP. Apesar de auxiliar as funções das entidades formais de controlo, acaba por restringir o direito de respeito da vida privada, que deverá ser protegida constitucionalmente, de forma a não permitir que um terceiro possa aceder aos dados guardados no computador, independentemente da sua natureza.

Aqui, a alínea b) do n.º 5 do artigo 174.º CPP acaba por se revelar mais vantajoso por referir o "Visado" em lugar de "quem tem disponibilidade sobre a coisa"[107]. Por se tratar de um computador pessoal, exclui-se essa legitimidade de intromissão no seu conteúdo a que lhe tem mera disponibilidade, cabendo ao seu portador concreto o direito de prescindir do bem jurídico de reserva da intimidade da vida privada em prol do sucesso da investigação.

Tendo cada vez mais uma importância relevante na vida das pessoas, o computador acaba por ser depósito de informações pessoais como escritos, imagens ou outros registos íntimos, servindo, nas palavras de COSTA ANDRADE como *"diário, biblioteca, arquivo, repositório de gestos, acções, planos, gostos, etc."*[108], justificando a natureza intrusiva da pesquisa informática. Assim, afetando a intimidade do visado, apenas ele poderá decidir se aceita tornar público o seu conteúdo.

No entanto, tal não exclui a possibilidade de o computador ser acedido, sendo necessário uma maior cautela face à não autorização legal do visado. Deverá ser-lhe permitido exigir da parte do Estado, a intromissão do conteúdo do seu computador apenas perante o seu consentimento ou mediante mandado oficial regularmente emitido.

Na eventualidade de o recetor visado voluntariamente disponibilizar as comunicações em causa, a jurisprudência distingue as regras referentes à sua apreensão. Sendo fornecidos de forma espontânea por quem delas dispor, as normas reguladoras do correio eletrónico recebido, equivale analogicamente à de entrega da carta recebida ou da disponibilização de uma mensagem presente em *voice-mail*. Tal analogia reforça-se, pois, a partir do momento em que se remeta uma carta, grave uma mensagem ou envia um *e-mail*

[107] CORREIA, João Conde, *Qual o significado….,* pág. 54; ANDRADE, Manuel da Costa, *ob. cit.*, Coimbra Editora, 2009, 1992, pág. 51.
[108] ANDRADE, Manuel da, *ob. cit.*, pág. 167.

perde-se o sigilo das comunicações, passando para a esfera do destinatário, que, por sua vez, poderá dispor desta como bem entender.

4.1.5. Revelação Coativa da *Password*

A pesquisa e revelação dos dados pesquisados trazem consigo uma última questão, carecida de clarificação legislativa: a revelação coativa da password. Mesmo havendo várias opiniões doutrinais e jurisprudenciais sobre o tema[109], não se encontra uma clara solução, que as harmonize.

CONDE CORREIA (2014: 58) questiona se poderão os órgãos de polícia criminal, o Ministério Público ou o Juiz de Instrução notificar os possuidores de computadores, a fim de revelarem as *passwords* de acesso ao seu conteúdo. No entendimento do citado autor, sendo o visado o próprio arguido, deparamo-nos com perante uma verdadeira omissão legislativa, não existindo qualquer norma habilitante, pondo em causa a sua proteção face aos constrangimentos causado pelo princípio *nemo temetur se ipsum accusare*. Apesar de este não ser forçado a contribuir com a sua própria condenação, o texto legal previsto para estas situações encontra-se estabelecido de tal forma que o arguido se sente constrangido a colaborar. Entre outros exemplos, destacamos situações em que sem a *password* certas informações revelantes para a salvaguarda de bens jurídicos fundamentais, poderão ser obtida em tempo útil.

Por outro lado, se o visado se tratar de uma testemunha, a sua recusa em prestar declarações deverá abranger os requisitos previstos nos artigos 132.º, n.º 2, e 134.º do CPP. Se não se verificarem tais pressupostos, a recusa será ilegítima, passível de ser sancionada.

5. Cooperação Internacional

Impõe-se uma breve referência às medidas de cooperação internacional, propostas pelos arts. 23.º a 35.º da CCIBER, com o objetivo de uniformizar as legislações dos

[109] PINTO, Lara Sofia, *Privilégio contra a auto-incriminação versus colaboração do arguido*, *AA.VV.*, *Prova Criminal e Direito de Defesa*, Coimbra, Almedina, 2010, pp. 91 e ss.

Estados subscritores, estreitando uma cooperação internacional eficiente entre autoridades nacionais no combate ao crime informático.

Enquanto entidade de supervisão central, a LCE atribui à ANACOM competências específicas no domínio da cooperação com as entidades de supervisão central dos Estados membros da União Europeia.

Assim, entre os artigos 20.º e 26.º da LC, o legislador previu as medidas específicas de cooperação internacional em matéria de obtenção da prova digital, presentes na CCIBER.

Apesar de não se tratar de uma medida inovadora, o artigo 21.º da LC estabelece a necessidade de organização de uma estrutura centralizadora e permanente, acessível à cooperação no combate ao crime informático. Esse ponto de contacto será a Polícia Judiciária, através da "*Rede 24/7*"[110], localizada na Secção de Investigação da Criminalidade Informática (9.ª Secção da Diretoria de Lisboa e Vale do Tejo). Perante o pedido de cooperação de outro Estado, o OPC prestará a assistência prevista do artigo 21.º, n.º 3, com aconselhamento técnico, preservando ou recolhendo dados, ou localizando suspeitos. Por força do artigo 21.º, n.º 4, caberá à PJ notificar de imediato tal pedido, através de relatório ao Ministério Público, descrevendo as *"investigações levadas a cabo, os resultados das mesmas, a descrição dos factos apurados e as provas recolhidas"* (art. 253.º do CPP).

Os artigos 22.º e 23.º visam o estabelecimento de regras respeitantes à preservação expedita dos dados informáticos, auxiliando mutuamente em matéria de medidas cautelares. Um Estado poderá solicitar a outro a preservação imediata de determinada prova, devendo, para tal, requerer formalmente tal apreensão ou cooperação na investigação. Perante tal ordem, caberá ao fornecedor do serviço preservar os dados solicitados, pelo período previsto. Ao período de três meses, pode ser ordenada renovação, por períodos de três meses, até ao limite máximo de um ano (art. 22.º, n.º 7).

No entanto, o pedido de auxílio judiciário poderá ser recusado se houverem razões fundadas para se crer previamente no seu indeferimento por não se verificar o "*requisito da dupla incriminação*" (art. 23.º, n.º2).

[110] Estando disponíveis 24 horas, 7 dias por semana. Contacto: contacto24.7@pj.pt.

Por sua vez, o artigo 24.º, prevê a possibilidade de a autoridade judiciária nacional pesquisar, recolher e divulgar os dados informáticos, quando se trate de "*situação em que a pesquisa e apreensão são admissíveis em caso nacional semelhante*".

O artigo 25.º prevê o acesso transfronteiriço a dados informáticos armazenados quando publicamente disponíveis ou com consentimento. O legislador consagra a possibilidade de as autoridades estrangeiras competentes aceder a dados armazenados em sistema informático localizado em Portugal, sem necessidade de pedido prévio às autoridades portuguesas, quando estes dados se encontrem publicamente disponíveis ou "*mediante consentimento legal e voluntário de pessoa legalmente autorizada a divulgá-los*".

Consagrado no artigo 26.º, a intercepção de comunicações em cooperação internacional, prevendo a autorização pelo juiz da interceção de transmissão de dados informáticos realizada através de um sistema informático localizado em território português. Para tal, será necessária a existência de um acordo, tratado ou convenção

Podemos, então, afirmar a relevância da Lei do Cibercrime para agilizar e facilitar os mecanismos de cooperação internacional entre os países subscritores da Convenção do Cibercrime.

II. CONCLUSÃO

Como pudemos verificar pelo estudo apresentado, a inclusão do mundo digital no âmbito da investigação criminal obrigou a uma maior preocupação com as características da prova digital.

A natureza complexa e instável da prova obriga o investigador a maiores cuidados para garantir a sua integridade em julgamento, através da criação de uma metodologia específica de investigação. As inovações legislativas em matéria de prova digital no processo penal permitiram uma ampliação e agilização de medidas de investigação criminal e da cooperação internacional.

Coube à Lei n.º 109/2009, de 15 de Setembro aproximar o lado imaterial e virtual da criminalidade no processo penal. No entanto, as limitações e omissões da Lei do Cibercrime demonstrariam a precipitação legislativa, ao colidir com normas legais pré-existentes como o Código de Processo Penal e a Lei n.º 32/2008.

A Lei do Cibercrime resulta da imposição de transposição das medidas previstas pela Convenção sobre o Cibercrime e a Decisão-Quadro 2005/222/JAI, visando uniformizar legislação reguladora de criminalidade informática e incrementar a cooperação internacional.

No entanto, o necessário esforço de adaptação e adequação deu lugar à conceção precipitada de uma lei ambígua, pondo em causa a eficiência do combate ao crime informático e a integração de medidas passíveis de auxiliar a investigação.

Importa questionar a razão da consagração do regime de obtenção da prova em lei avulsa. Resultando num maior esforço interpretativo e perda de unidade sistemática, afirma-se favorável que o novo regime seja integrado no Título III ("Meios de Obtenção da Prova") do Livro II ("Da Prova"), no Código de Processo Penal.

Quanto aos métodos de obtenção da prova digital previstos pela lei, os artigos 12.º a 14.º trazem consigo medidas úteis de prevenção, permitindo uma expedita preservação e revelação dos dados. Assim sendo, quem detenha ou controle os dados informáticos, passa a estar abrangido por várias obrigações, que se acumulam às previstas na Lei n.º 32/2008. No entanto, apesar do previsto no artigo 11.º, n.º 2 da LC, ser complementar com a Lei n.º 32/2008, esta acaba praticamente por se revogar, se esvaziar face à maior amplitude das normas mais recentes.

A Lei do Cibercrime prevê no artigo 17.º o regime da apreensão do correio eletrónico, remetendo para o regime de apreensão do correio tradicional do artigo 179.º do CPP. Devemos considerar esta medida como outra precipitação do legislador, pois coloca a norma em conflito com o Código de Processo Penal. Essa remissão leva, inadvertidamente, à revogação parcial da norma de extensão do artigo 189.º, referente à aplicação do regime das escutas telefónicas em casos particulares. Apesar de ser a solução correta perante esta lacuna, e tendo em conta que a norma de extensão fora integrada no Código em 2007, o legislador falhou em não transpor as normas delimitadas pela Convenção sobre o Cibercrime e simplificar a estrutura judiciária.

Numa tentativa de originalidade nacional, o legislador português incluiu o regime das ações encobertas com o artigo 19.º. No entanto, o excessivo alargamento do regime abriu o seu âmbito de aplicação a crimes informáticos específicos e crimes cometidos por meio de sistemas informáticos, sem aprofundar e fundamentar normativamente. Descaracterizando o regime das ações encobertas, que deveria ter natureza excecional, o legislador viria a pôr em causa o princípio da proporcionalidade em sentido amplo.

Procurando aclarar as contradições mostradas pelos textos legais que lhe antecederam, a Lei do Cibercrime viria a agravar dilemas técnico-legislativos já existentes, levando a um aumento da agressão na investigação criminal, em comparação com a investigação com recurso às chamadas "*provas tradicionais*". As características das novas tecnologias, em constante mudança e desenvolvimento, leva à lesão de direitos, liberdades e garantias dos suspeitos visados, sejam eles criminosos ou inocentes, e até de terceiros.

Direitos pessoalíssimos considerados indispensáveis como garantia da afirmação do direito à autodeterminação informacional, como o direito à palavra, o direito à imagem, o direito à autodeterminação informacional, o direito à reserva da intimidade da vida privada e familiar, o direito à inviolabilidade do domicílio informático (art. 34.º da CRP) e o direito de propriedade serão em regra lesados por essas medidas. Tratam-se de medidas ocultas, aplicadas seguindo critérios definidos pelos órgãos de polícia criminal responsáveis pela investigação forense, e, por vezes, sem consentimento ou participação dos visados. A prova digital deverá ser obtida em sistemas informáticos de terceiros, sobretudo de fornecedores de comunicação, podendo ofender os direitos do visado, enquanto assinante do serviço, pois põe em causa obrigações contratuais, e enquanto

cidadão, degradando o dever de sigilo, protegido constitucionalmente. Acresce o facto da informação obtida através das medidas aplicadas pelo investigador estar disponível para um grupo de pessoas incertas, correndo-se o risco de serem expostas e utilizadas, para finalidades alheias ao processo.

Estabelecendo-se numa génese de inspiração liberal, caberá ao Direito Processual Penal defender acerrimamente os direitos dos cidadãos. Para tal, encontra-se previsto no art. 17.º da CRP o princípio da proibição do excesso, que estabelece que qualquer limitação deverá cumprir critérios de adequação, necessidade e proporcionalidade, não podendo as normas restritivas dos direitos, liberdades e garantias "*diminuir a extensão e o alcance do conteúdo essencial dos preceitos constitucionais que os consagram*" (art. 18.º, nº 3 da CRP). Tais limitações incorrem de justificação, como salvaguarda dos direitos e liberdades sob proteção constitucional, e apenas, em situações de clara e indispensável necessidade.

Restringindo direitos fundamentais acarreta um conflito positivo de normas constitucionais entre duas normas consagradoras de direitos de interesse constitucional, que apenas se solucionará com a máxima observância dos direitos fundamentais em causa, restringindo o mínimo possível, adequando ambas as normas no conflito. GOMES CANOTILHO e VITAL MOREIRA (1991: 133-134, 143) apelam a uma concordância prática dos direitos ou interesses em conflito. Portanto, estamos perante uma tarefa de conciliação entre o interesse objetivo de eficácia da investigação criminal, obtendo a prova relevante para tal efeito, e o interesse de proteção dos direitos fundamentais afetados, sendo considerados pelo legislador face às possíveis agressões sofridas com a investigação. Para tal, deverão ainda ser tidas em conta, a natureza imaterial e instável da prova digital e a eficácia dos meios tradicionais de obtenção da prova. Os autores reforçam o seu entendimento, prevalecendo a interpretação que favorecer os direitos fundamentais em conflito, e consequentemente, lhe oferecer maior proteção.

Apesar desta conjetura, a importância da Lei do Cibercrime no panorama português é inegável, pois surge como ponto de partida de um caminho a seguir.

O regime regulador da prova digital necessitará de uma intervenção legislativamente coerente e cientificamente sustentável. Torna-se fundamental a implementação de um modelo regulativo, capaz de conjugar técnica e substância, conseguido através da reflexão doutrinal, consolidando conceitos e práticas jurídicas. Tal

modelo deverá pautar-se, prático e dogmaticamente, como potenciador de um sistema justo e satisfatório do contexto legislativo atual.

No entanto, antes de uma análise crítica e alteração do texto legal vigente (que são, indiscutivelmente, bem vindos), será necessária uma alteração sociocultural de perceção, mudar o modo como as tecnologias são vistas e as potencialidades criminosas que se escondem por atrás de um ecrã de computador, de forma a permitir alcançar no futuro a segurança e paz jurídica propostas pelo Direito Processual Penal.

Assim sendo, esperamos que a inovação que pautou o legislador em matéria de obtenção da prova digital não se tenha esgotado com a Lei do Cibercrime, e que as várias opiniões, que darão lugar a vasta doutrina e jurisprudência, ajude a um "abrir de olhos" por parte do legislador, levando a uma maior eficiência e agilização no combate ao crime informático.

III. BIBLIOGRAFIA

Referências bibliográficas

- ALBUQUERQUE, Paulo Pinto de, "*Comentário do Código de Processo Penal à luz da Constituição da República Portuguesa e da Convenção Europeia dos Direitos do Homem"*, 3.ª ed. atualizada, Lisboa, Universidade Católica, 2009, ISBN 978-972-54-0202-3;
- ALBUQUERQUE, Paulo Pinto de, "*Comentário do Código Penal à luz da Constituição da República Portuguesa e da Convenção dos Direitos do Homem*", 2.º ed. actualizada, Lisboa: Universidade Católica Editora, 2010. ISBN 978-972-54-0272-6;
- ANDRADE, José Carlos Vieira de, "*Os Direitos Fundamentais na Constituição Portuguesa de 1976*", 4.ª Edição, Coimbra, Almedina, 2009;
- ANDRADE, Manuel da Costa, *"Métodos Ocultos de Investigação: Plädoyer para uma teoria geral" Que Futuro para o Direito Processual Penal? Simpósio em Homenagem a Jorge de Figueiredo Dias*, 2009, pp. 525 ss.;
- ANDRADE, Manuel da Costa, "*Sobre as proibições de prova em processo penal"*, Coimbra, Coimbra Editora, 1992, ISBN 972-32-0613;
- ANDRADE, Manuel da Costa, "*Bruscamente no verão passado", a Reforma do Código de Processo Penal - Observações críticas sobre uma lei que podia e devia ter sido diferente"*, Coimbra, Coimbra Editora, 2009; ISBN 978-972-32-1726-1;
- ARZAMENDI, José Luis de la Cuesta; "*Derecho Penal Informático*", Primera edicíon, 2010. Editorial Aranzadi, SA. ISBN: 978-84- 470-3429-1;
- ASCENÇÃO, José de Oliveira, "*Criminalidade Informática*", Estudos sobre Direito da Internet e da Sociedade da Informação, Almedina, 2001;
- BARROS, Juliana Isabel Freitas, "*O Novo Processo Penal: Os Meios de Obtenção de Prova Digital consagrados na Lei 109/2009, de 15 de Setembro*", Dissertação apresentada no âmbito do 2.º ciclo de Estudos em Direito da Faculdade de Direito da Universidade de Coimbra, com especialização em

Ciências Jurídico-Forenses, sob orientação da Professora Doutora Helena Moniz, Coimbra, 2012;

- BRAVO, Rogério, "*As Tecnologias de informação e a Compressão dos Direitos, Liberdades e Garantias - os efeitos das regras 10/10 e 1/1*", Lisboa, 2012;
- BRAVO, Rogério, "*Equiparação do correio electrónico ao conceito tradicional de correspondência por carta*", Polícia e Justiça - Revista do Instituto Superior de Polícia Judiciária e Ciências Criminais, III Série, n.º 7, Janeiro-Junho 2006, Coimbra Editora;
- CANOTILHO, J. J. Gomes; MOREIRA, Vital, "*Constituição da República Anotada"*, Vol. I, 4ª Edição Revista, Coimbra, Coimbra Editora, 2007;
- CANOTILHO, J. J. Gomes; MOREIRA, Vital, "*Fundamentos da Constituição*", 2.ª ed., Coimbra, Coimbra Editora, 1991.
- CASEY, Eoghan, "*Digital Evidence and Computer Crime, Forensic Science Computers and the Internet*" Academic Press, 2000;
- CARRAPIÇO, Helena, "*O Crime Organizado e as Novas Tecnologias: Uma faca de dois gumes*", Disponível em http://www.idn.gov.pt/publicacoes/nacaodefesa/textointegral/NeD111.pdf e acedido a 11-12-2015;
- COGAR, Stephen W., "*Obtaining admissible evidence from computers and Internet Service Providers"*, FBI-Law Enforcement Bulletin, Washington, V. 72, n. 7 (July 2003). Disponível em http://www.questia.com/library/1G1-107121941/obtaining-admissible-evidence-from-computers-and-internet e acedido a 17-12-2015;
- CORREIA, João Conde, "*Prova Digital: as leis que temos e a lei que devíamos ter*", Revista do Ministério Público, nº 139 (Julho-Set 2014), pp.29-59;
- CORREIA, João Conde, *"Qual o significado de abusiva intromissão na vida privada, no domicilio, na correspondência e nas telecomunicações (art. 32.º, n.º 8, 2ª parte da CRP)?"*, Revista do Ministério Público, nº 79 (1999);

- COSTA, José Francisco de Faria, *"Algumas reflexões sobre o estatuto dogmático do chamado "Direito Penal Informático""*, Direito Penal da Comunicação, alguns escritos, Coimbra Editora, 1998, ISBN 972-32-0805-4;
- COSTA, José Francisco de Faria, "*Direito Penal e Globalização, Reflexões não locais e pouco globais*", Wolkers Kluwer, Coimbra Editora, 2010;
- COSTA, José Francisco de Faria, "*Direito Penal Económico*", Quarteto, Coimbra, 2003, ISBN 989-558-004-5;
- DESGARDINS, Bruno, e LEMAIRE, Jean-Paul, "*Desenvolvimento Internacional da Empresa. O Novo Ambiente Internacional*", Lisboa, Instituto Piaget, 1999;
- DIAS, Jorge de Figueiredo, "*Clássicos Jurídicos, Direito Processual Penal*", Coimbra Editora, 2004, pp. 59 e 60;
- DIAS, Jorge de Figueiredo, "*Direito penal, parte geral tomo I, 2ª Edição, Questões fundamentais, a doutrina geral do crime*", Coimbra Editora, 2007. ISBN 978-972-32-1523-6;
- DIAS, Jorge de Figueiredo, "*Princípios estruturantes do processo penal", Código de Processo Penal – processo legislativo*, vol. II, tomo II, Lisboa, Edição da Assembleia da República, 1999, pp. 23 e 24;
- DIAS, Vera Elisa Marques, "*A problemática da investigação do Cibercrime*". DataVenia Revista Jurídica Digital. N.º1, Julho-Dezembro, 2012. ISSN 2182-8242. Disponível em http://www.datavenia.pt/ficheiros/edicao01/datavenia01_p063-088.pdf e acedido a 10-11-2015;
- DÍAZ, Leyre Hernández, "*Aproximación a un concepto de derecho penal informático*", in Derecho Penal Infformatico, Primera edición, 2010, Civitas, Editorial Aranzadi, ISBN 978-84-470-3429-1;
- GAMEIRO, Carlos, "*O Risco da Informação em Ambiente Eletrónico*", Estudos de Direito e Segurança, Faculdade de Direito da Universidade Nova de Lisboa, Almedina, 2007;
- GONÇALVES, Fernando, ALVES, Manuel João, VALENTE, Manuel Guedes, "*O novo regime jurídico do agente infiltrado (Comentado e Anotado – Legislação Complementar)*", Coimbra, Livraria Almedina, 2001;

- HAGY, David W.; "*Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors*" *in National Institute of Justice, Janeiro 2007, U.S. Department of Justice, 2007.* Disponível em https://www.ncjrs.gov/pdffiles1/nij/211314.pdf e acedido a 05-01-2016;
- JESUS, Francisco Marcolino de, "*Os Meios de Obtenção da Prova em Processo Penal"*, Almedina, Coimbra, 2011, ISBN 978-972-40-4428-6;
- LAVOURA, Tiago Santos, "*O agente infiltrado e o seu contributo para a investigação criminal*", Dissertação para obtenção de grau de Mestre em ciências jurídico-forenses, Orientador Professor Doutor Figueiredo Dias, Co-orientador: Mestre Ana Pais, Coimbra, Instituto Superior Bissaya Barreto;
- LEITE, Ana Raquel Gomes, "*Criminalidade Informática: Investigação e Meios de Obtenção de Prova*". Dissertação apresentada no âmbito do 2.º Ciclo de Estudos em Direito, da Faculdade de Direito da Universidade de Coimbra, com especialização em Ciências Jurídico-Forenses, sob orientação da Professora Doutora Helena Moniz, Coimbra, 2013;
- LOPES, José Mouraz; CABREIRO, Carlos Antão; "*A emergência da prova digital na investigação da criminalidade informática*", inSub Judice - Justiça e Sociedade, Almedina, Lisboa, 2006;
- MACEDO, João Carlos Cruz Barbosa de, "*Algumas Considerações Acerca dos Crimes Informáticos em Portugal*", Direito Penal Hoje Novos desafios e novas respostas, Organizado por Manuel da Costa Andrade e Rita Castanheira Neves, Coimbra, Coimbra Editora, 2009; ISBN 978-972-32-1692-9;
- MARQUES, Garcia, MARTINS, Lourenço, "*Direito da Informática"*, 2.ª Ed.., Coimbra, Almedina, 2006;
- MARQUES, Maria Joana Xara-Brasil, "*Os Meios de Obtenção de Prova na Lei do Cibercrime e o seu confronto com o Código de Processo Penal*", Dissertação apresentada no âmbito do Curso de Mestrado Forense da Universidade Católica Portuguesa, sob orientação do Professor Doutor Henrique Salinas, Lisboa, 2014;
- MARTIN, Daniel; MARTIN, Fréderic-Paul, *Nouvelles technologies de l'information et criminalité*, in Revue du Marché Commun et de l'Únion européenne, n.º 421, 1998 ;

- MARTINS, A. G. Lourenço, "*Criminalidade Informática*", Direito da Sociedade da Informação, vol. IV, Coimbra Editora, 2003. ISBN 972-32-1169-6;
- MATA, Ricardo M. y Martín, "*Criminalidad Informática: una introducción al Cibercrime*", Temas de Direito da Informática e da Internet, Ordem dos Advogados (Conselho Distrital do Porto), Coimbra Editora, 2004;
- MESQUITA, Paulo Dá, "*Processo Penal, Prova e Sistema Judiciário*", 1.ª ed:, Coimbra, Coimbra Editora, Setembro 2010. ISBN 978-972-32-1842-8;
- MILITÃO, Renato Lopes, "*A Propósito da Prova Digital*", disponível em http://www.oa.pt/upl/%7B53f46e96-536f-47bc-919d-525a494e9618%7D.pdf e acedido a 04-10-2015;
- MONIZ, Helena; FIDALGO, Sónia; "*Cybercrime Legislation in Portugal - Portuguese Report*" in Regulating Internet Crime - Fragmented International Instruments and the Harmonazation of National Criminal Law in the Global Cyberspace, 18.º Congresso Internacional de Direito Comparado da International Academy of Comparative Law, 2009. Disponível em http://www.wcl.american.edu/events/2010congress/welcome.en.cfm e acedido em 14-01-2016;
- NEVES, Rita Castanheira, "*As Ingerências nas Comunicações Electrónicas em Processo Penal – Natureza e respectivo regime jurídico do correio electrónico enquanto meio de obtenção de prova"*, Coimbra; Coimbra Editora, 2011; ISBN 978-972-32-1942-5;
- NEVES, Rosa Vieira, "*A Livre Apreciação da Prova e a Obrigação de Fundamentação da Convicção (na Decisão Final Penal)*", Coimbra Editora, 2011, ISBN 978-972-32-1929-6;
- PINTO, Lara Sofia, "*Privilégio contra a auto-incriminação versus colaboração do arguido*", in *Prova Criminal e Direito de Defesa, estudos sobre teoria da prova e garantias de defesa em processo penal*, Reimpressão, coord. Teresa Pizarro Beleza e Frederico de Lacerda da Costa Pinto, Coimbra, Almedina, 2011, ISBN 978-972-40-4090-5;

- POULLET, Yves, WARRANT, Françoise, "*Noveaux compléments au service teléphonique et protection des donnés: à la recherche d'un cadre conceptuel*", Droit de l'Informatique et des Télécoms, 7 ème année, 1990/91;
- RAMOS, Armando Dias, "*A prova digital em processo penal: o correio electrónico*", Chiado Editora, 1.º ed. Novembro 2014, ISBN 978-989-51-2383-4;
- ROCHA, Manuel Lopes, "*A lei da criminalidade informática (Lei nº 109/91 de 17 de Agosto) – Génese e técnica legislativa*", Legislação – Cadernos de Ciência de Legislação (INA – Instituto Nacional de Administração), nº 8 (Outubro-Dezembro de 1993);
- RODRIGUES, Benjamim Silva, "*Da Prova Penal – Tomo IV, Da Prova Electrónico-Digital e da Criminalidade Informático-Digital*", 1-ª Ed. [S.L]: Rei dos Livros, 2011. ISBN 978-989-8305-18-3;
- RODRIGUES, Benjamim Silva, "*Da Prova Penal, tomo II, Bruscamente… A(s) Face(s) Ocultas dos Métodos Ocultos de Investigação Criminal*", 1.ª Edição, Rei dos Livros, 2010. ISBN 978-989-8305-06-0;
- RODRIGUES, Benjamim Silva, "*Direito Penal Parte Especial, Tomo I, Direito Penal Informático-Digital, Contributo para a Fundamentação da sua Autonomia Dogmática e Científica à Luz do novo Paradigma de Investigação Criminal: a Ciência Forense Digital e a Prova Digital*", Coimbra Editora, Limitada, 2009. ISBN: 978-989-95779-5-4;
- RODRIGUES, Benjamim Silva, *Das Escutas Telefónicas – À Obtenção da Prova [Em Ambiente] Digital*, TOMO II, Coimbra Editora, 2009;
- SANTOS, Cristina Máximo dos, "*As novas tecnologias da informação e o sigilo das telecomunicações*", Separata da Revista do Ministério Público n.º 99, Lisboa, 2004;
- SANTOS, Paulo; BESSA, Ricardo; PIMENTEL, Carlos; "*Cyberwar: O fenómeno, as tecnologias e os actores*". Janeiro 2008. FCA - Editora de Informática Lda. ISBN: 978-972-722-597-2;
- SIEBER, Ulrich, "*Criminalidad Informática: Peligro y Prevención*", Delincuentia Informática, IURA-7, PPU, Barcelona, 1998 (trad. Elena Farré Trepat);

- SIEBER, Ulrich, "*Les crimes infomatiques et d'autres crimes dans le domaine de la technologie informatique*", in Revue Internationale de Droit Penel, AIDP, Érès, Colóquio de Wurzbourg, Outubro de 1992 ;
- SILVA, Germano Marques da, "*Curso de Processo Penal*", vol. II, 5.ª ed. revista e actualizada, Lisboa, Editorial Verbo / Babel, 2011;
- SIMAS, Diana Viveiros de; *"O Cibercrime*"; Dissertação apresentada no âmbito do 2.º Ciclo de Estudos em Direito, no Curso de Mestrado em Ciências Jurídico-Forenses, conferido pela Universidade Lusófona de Humanidades e Tecnologias, sob orientação do Professor Doutor José Sousa Brito, Lisboa, 2014;
- SOUSA, Susana Aires de; "*Agent Provocateur e meios enganosos de prova - Algumas reflexões*", *Liber Discipulorum para Figueiredo Dias*, 2003, pp. 1207 ss.;
- VENÂNCIO, Pedro Dias, "*Lei do Cibercrime Anotada e Comentada"*, 1.ª ed., Coimbra, Coimbra Editora, 2011. ISBN 978-972-32-1906-7;
- VENÂNCIO, Pedro Dias, "*A Intercepção de Comunicações e Acções Encobertas na Lei do Cibercrime*", JusJornal, N.º 1184, 25 de Fevereiro de 2011, Editora Coimbra Editora, grupo Wolters Kluwer;
- VERDELHO, Pedro, "*A nova lei do Cibercrime*", Scientia Juridica, Tomo LVIII, Braga, 2009, ISSN 0870-8185;
- VERDELHO, Pedro, *"Cibercrime", Direito da Sociedade da Informação*, Vol. IV, Coimbra Editora, 2003. ISBN 972-32-1169-6;
- VERDELHO, Pedro, *"Lei n.º 109/2009", de 15 de Setembro, in Comentário das leis penais extravagantes*, vol. 1, coordenação de Paulo Pinto de Albuquerque: Universidade Católica Editora, 2010. ISBN 978-972-54-0282-5;
- VERDELHO, Pedro, "*A Convenção sobre Cibercrime do Conselho da Europa - Repercussões na Lei Portuguesa*", Direito da Sociedade da Informação, vol. VI Coimbra Editora, 2006. ISBN 978-972-32-1411-3;
- VERDELHO, Pedro, "*A obtenção de prova no ambiente digital"*, Revista do Ministério Público, Ano 25.º, nº 99 Julho-Setembro 2004 pp. 117-136;

- VERDELHO, Pedro, *"Apreensão de Correio Electrónico em Processo Penal"*, Revista do Ministério Público, Ano 25.º, nº 100, Outubro-Dezembro, 2004, pp. 153-164;
- VERDELHO, Pedro, *"Técnica no Novo C.P.P.: Exames, Perícias e Prova Digital"*, Revista CEJ, 1º Semestre 2008, nº 9 – Jornadas;
- VERDELHO, Pedro; BRAVO, Rogério; ROCHA, Manuel Lopes, "*Leis do Cibercrime*", Vol. I, 2003. Disponível em http://www.centroatl.pt/titulos/direito/imagens/excerto-ca-leisdoCibercrime1.pdf e acedido a 28-12-2015.

Outros Documentos e Links relevantes

- "*O Tribunal de Justiça declara inválida a diretiva sobre a conservação de dados*". Disponível em http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054pt.pdf e consultado em 11-01-2016
- Curso de formação avançada à distância *CIBERCRIME E PROVA DIGITAL*, organizado pela e-UNIFOJ do centro de Estudos sociais (CES) da Universidade de Coimbra e coordenado por Pedro Verdelho, decorreu entre 06 de Outubro e 05 de Dezembro Modulo II, Cibercrime, Os crimes Informáticos ou Cibercrimes, pp.1-6. Disponível em http://opj.ces.uc.pt/e-learning/moodle/course/view.php?id=10 e acedido em 10-01-2016;
- Decisão-Quadro nº 2005/222/JAI do Conselho, de 24 de Fevereiro, disponível em http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32005F0222
- Definições presentes em www.informatica-juridica.com, acedido em 05-01-2016;
- Diário da República, I Série, nº 120/X/4ª, de 10 de Julho de 2009;
- Diário da República, 1.ª série — N.º 179 — 15 de Setembro de 2009, disponível em https://dre.pt/application/dir/pdf1sdip/2009/09/17900/0635406378.pdf e consultado em 18-12-2015;

- "*High Tech Crimes within the EU: Old crimes New Tools, New Crimes New Tools*", Threat Assessment 2007 High Tech Crime Centre 2007. Disponível em https://www.enisa.europa.eu/activities/cert/events/files/ENISA_Europol_threat_assessment_2007_Dileone.pdf e acedido a 27-12-2015;
- Exposição dos Motivos da Proposta de Lei nº 289/X/4ª;
- Forensic Examination of Digital Evidence: A Guide for Law Enforcement. Disponível em https://www.ncjrs.gov/pdffiles1/nij/199408.pdf e acedido a 02-01-2016;
- https://www.fbi.gov/about-us/lab/forensic-science-communications/fsc/april2000/swgde.html, acedido em 05-01-2016;
- https://www.ncjrs.gov/pdffiles1/nij/199408.pdf, e consultado em 02-01-2016
- Minuta em português do Relatório Explicativo da Convenção sobre o Cibercrime. Disponível em http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/ETS_185_Portugese-ExpRep.pdf, e acedido em 10-01-2016;
- Parecer consultivo da Procuradoria Geral da República, n.º convencional PGRP00003238, com relator Paulo Dá Mesquita, disponível em http://www.dgsi.pt/pgrp.nsf/7fc0bd52c6f5cd5a802568c0003fb410/a734913d16b0f89480257af 00043b68a, acedido em 26-01-2016;
- Parecer do Conselho Consultivo da PGR com o n.º P000792008, disponível em http://www.dgsi.pt/pgrp.nsf/0/b90edf9f8e8a47e480257515003eb4e8 e consultado em 08-01-2016;
- Relatório Explicativo da Convenção sobre a Cibercriminalidade, disponível em http://conventions.coe.pt e acedido a 11-01-2016;
- Site oficial da Procuradoria Geral da República, pareceres VII, utilização da informática, disponível em http://www.pgr.pt/pub/Pareceres/VII/2.html e acedido em 24-01-2016.

Jurisprudência Nacional e Internacional

- Acórdão do Tribunal da Relação de Coimbra, de 26-02-2014, Processo nº 559/12.0GBOBR-A.C1, disponível em *http://www.dgsi.pt/jtrc.nsf/c3fb530030ea1c61802568d9005cd5bb/0e255b331c5eaecd80257c91005ae8bf?OpenDocument*, e acedido a 22-01-2016;
- Acórdão do Tribunal da Relação de Coimbra, de 29-03-2006, Processo n.º 607/06, disponível em *http://www.dgsi.pt/jtrc.nsf/0/553a95b9c55abec18025716800494c3d?OpenDocument*, e acedido em 22-01-2016;
- Acórdão do Tribunal da Relação de Évora, de 13-11-2012, Processo nº315/11.2PBPTG-A.E1 disponível em *http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/d147ed8908009d4980257de10056f9c9?OpenDocument&Highlight=0,cibercrime*, e acedido em 22-01-2016;
- Acórdão do Tribunal da Relação de Évora, de 7-12-2012, Processo nº 3142/09.3PBFUN-A.L1-5, disponível em *http://www.dgsi.pt/jtrl.nsf/e6e1f17fa82712ff80257583004e3ddc/0e870e9e2782243380257839005785c2?OpenDocument*, e acedido em 22-01-2016;
- Acórdão do Tribunal da Relação de Guimarães, de 12-10-2009, Processo nº 1396/08.1PBGMR-A.G1, disponível em *http://www.dgsi.pt/jtrg.nsf/86c25a698e4e7cb7802579ec004d3832/4c03909839f95d5f8025767e004f83fe?OpenDocument*, e acedido em 22-01-2016;
- Acórdão do Tribunal da Relação de Guimarães, de 29-03-2011, Processo nº 735/10.0GAPTL-A.G1, disponível em *http://www.dgsi.pt/jtrg.nsf/86c25a698e4e7cb7802579ec004d3832/6aa96edf91e899b2802578a00054631f?OpenDocument&Highlight=0,cibercrime*, e acedido em 22-01-2016;
- Acórdão do Tribunal da Relação de Lisboa, de 11-01-2011, Processo nº 5412/08.9TDLSB-A.L1-5, disponível em *http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/e5ed1936deb44eb180257824004ab09d?OpenDocument*, e acedido em 22-01-2016;

- Acórdão do Tribunal da Relação de Lisboa, de 15 de Julho de 2008, Processo n.º 3453/2008-5, disponível em *http://www.dgsi.pt/jtrl.nsf/0/9182245992c7c5d18025749000503b8c?OpenDocument*, e acedido em 22-01-2016;
- Acórdão do Tribunal da Relação de Lisboa, de 18-01-2011, Processo nº 3142/09.3PBFUN-A.L1-5, disponível em *http://www.dgsi.pt/jtrl.nsf/e6e1f17fa82712ff80257583004e3ddc/0e870e9e2782243380257839005785c2?OpenDocument*, e acedido em 22-01-2016;
- Acórdão do Tribunal da Relação de Lisboa, de 19-06-2014, Processo nº 1695/09.5PJLSB.L1-9, disponível em *http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/eb1460fa14510bf380257d080036a9b9?OpenDocument*, e acedido em 22-01-2016;
- Acórdão do Tribunal da Relação de Lisboa, de 22-01-2013, Processo n.º 581/12.6PLSNT-A.L1-5, disponível em *http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/7bd2dd8af10b34c380257b27003a5697?OpenDocument*, e acedido em 22-01-2016;
- Acórdão do Tribunal da Relação do Porto, de 12-09-2012, Processo nº 787/11.5PWPRT.P1, disponível em *http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/877e0322acde18d080257a8300393cc6?OpenDocument&Highlight=0,cibercrime*, e acedido em 22-01-2016;
- Acórdão do Tribunal da Relação do Porto, de 27-01-2010, Processo n.º 896/07.5JAPRT.P1, disponível em *http://www.dgsi.pt/jtrp.nsf/c3fb530030ea1c61802568d9005cd5bb/68fdcdf35dc62b6e802576c40041c799*, e acedido em 22-01-2016.