UNIVERSIDADE CATÓLICA PORTUGUESA

A APREENSÃO DE CORREIO ELETRÓNICO ENQUANTO MEIO PRIVILEGIADO DE OBTENÇÃO DA PROVA ELETRÓNICO-DIGITAL

(Das incongruências do art. 189.º, do CPP, à sua compatibilização ou "superação" face ao art. 17.º, da Lei n.º 109/2009)

Bruno Filipe Barata de Tavares Queirós

Mestrado em Direito

Faculdade de Direito | Escola do Porto

2020

UNIVERSIDADE CATÓLICA PORTUGUESA

A APREENSÃO DE CORREIO ELETRÓNICO ENQUANTO MEIO PRIVILEGIADO DE OBTENÇÃO DA PROVA ELETRÓNICO-DIGITAL

(Das incongruências do art. 189.º, do CPP, à sua compatibilização ou "superação" face ao art. 17.º, da Lei n.º 109/2009)

Bruno Filipe Barata de Tavares Queirós

Orientador: Dr. Pedro Miguel Freitas

Mestrado em Direito

Faculdade de Direito | Escola do Porto

2020

AGRADECIMENTOS

Ao Dr. Pedro Miguel Freitas pela orientação e disponibilidade ao longo deste processo.

À FDUC e à UCP e a todos os que fizeram parte deste percurso.

A todos os que contribuíram para a elaboração desta dissertação.

Aos companheiros de Coimbra, aos "Capas", e à AAC.

Aos meus pais e à minha irmã por todo o apoio incondicional e exemplo diário.

À Rita, pela paciência e por estar presente em todos os momentos importantes.

A todos eles, o meu sincero agradecimento.

RESUMO

As novas tecnologias de informação e comunicação (TIC´s), precipitaram as sociedades atuais para verdadeiras e permanentes sociedades informacionais e comunicacionais, tendo a tecnologia tomado de assalto todas as facetas do nosso quotidiano.

Para além do "ser social", o Homem passou também a assumir-se como um "ser tecnológico", sedente de informação e comunicação, de tal modo que as redes eletrónicas, publicamente acessíveis, como sejam, nomeadamente, sites, redes sociais e correio eletrónico, surgem como meios indispensáveis à vida humana.

A mudança tecnológica, informacional e comunicacional foi adotada também, e naturalmente, para a prática de novos crimes, designados de informático-digitais, além de conferir nova roupagem à tipologia de crimes já existentes.

O correio eletrónico passou a constituir o expediente técnico que, por excelência, quase em tempo real, nos permite comunicar, aceder ou enviar informação.

As interceções e apreensões de comunicações eletrónicas configuram, atualmente, um dos mais importantes, senão mesmo, ousaríamos dizer, o mais importante dos meios de obtenção de prova no combate à criminalidade altamente organizada, criminalidade económica e corrupção, entre outros. Tal circunstância determina um novo paradigma de investigação criminal forense.

A criminalidade informático-digital, pelas suas características e natureza, não pode mais ser investigada em termos clássicos. É necessário sensibilizar os OPC e os magistrados – judiciais e do MP – para a necessidade da presença do criminólogo forense, isto é, alguém especializado nas várias novas áreas do saber científico, que procure, na cena do crime, "o vestígio".

Neste contexto, o nosso trabalho versa sobre a chamada «cena do crime eletrónico-digital», pretendendo significar-se, não só a Internet e a Intranet, mas ainda, os diversos aparelhos de informação, comunicação e de armazenamento de fluxos informacionais e comunicacionais, eletrónico-digitais.

Com a presente dissertação, pretende-se averiguar como e em que termos deve ser compreendida a obtenção a prova eletrónico-digital, sobretudo aquela que resulta do chamado "correio eletrónico", atenta a desarmonia do nosso paradigma legislativo. Tentando harmonizar alguma desordem jurídica procuraremos compatibilizar os arts. 189.º do CPP; art. 17.º da Lei n.º 109/2009 de 15 de setembro, e, ainda, (face ao regime da retenção de dados de tráfego) a Lei n.º 32/2008, de 17 de julho.

Concluímos pela necessidade de reformulação, atualização, rejuvenescimento e harmonização dos vários regimes existentes de obtenção da prova eletrónico-digital.

Palavras chave: Prova Eletrónico-digital, Correio Eletrónico, Cibercrime, Internet.

ABSTRACT

With new technologies of information and communication, modern communities turned into true societies of information and communication with technology taking control of every aspect of our daily lives.

More than a social animal, man is now a technological being, thirsty for communication and information, in such a way that public networks, from websites to social networks and e-mail work now as a true appendix of the human being. Amid all this evolution, the electronic mail is the technical device that allows us to communicate, access or send information.

This technological, informational and communicational shift is not unknow to criminals who now, not only commit new "technological" crimes, but also gained new tools to use for traditional crimes.

The interception and apprehension of electronical communications configure, in today's age, one, if not the most important way of, gathering evidence to fight, highly organized crime, economical crime, corruption, amongst others. All this directs us to a new paradigm of criminal forensic investigation.

Classical investigation is not enough for today's criminality and this reinforces the need for forensic criminologists, people with a wide range of scientific knowledge that will aid the Police and Magistrates on their pursuit of criminal evidence. In this context, this thesis focus on the digital crime scene, this includes

not only the internet, but also a wide array of devices concerning informatic and digital communication and storage.

With this thesis we pretend to ascertain the terms in which electronic-digital evidence should be perceived, with a special focus on apprehension of electronical mail and the disharmony concerning this topic in our legal system. While trying to solve this legal conundrum we shall try to harmonize the articles 189º of the CPP, article 17º of law 109/2009 of December 15th and, concerning traffic data, law 32/2008 of July 17th.

We shall conclude that the reformulation and harmonization of the existent regimes of apprehension of electronic-digital law is very much needed.

Keywords: Electronic-digital Law, Electronic Mail, Cybercrime, Internet.

SIGLAS E ABREVIATURAS

Art. – Artigo

Arts. – Artigos

CP – Código Penal

CPP – Código de Processo Penal

CRP – Constituição da República Portuguesa

JIC – Juiz de Instrução Criminal

LC – Lei do Cibercrime

MP – Ministério Público

OPC – Órgão de Polícia Criminal

p. – Página

SMS – *Short Message Service*

STJ – Supremo Tribunal de Justiça

TC – Tribunal Constitucional

TJUE – Tribunal de Justiça da União Europeia

TRC – Tribunal da Relação de Coimbra

TRE – Tribunal da Relação de Évora

TRG – Tribunal da Relação de Guimarães

TRL – Tribunal da Relação de Lisboa

TRP – Tribunal da Relação do Porto

TIC´s – Tecnologias de Informação e Comunicação

ÍNDICE GERAL

AGRADECIMENTOS **4**

RESUMO **5**

SIGLAS E ABREVIATURAS **9**

ÍNDICE GERAL **10**

CAPÍTULO I – NA ERA DA SOCIEDADE INFORMACIONAL E COMUNICACIONAL: A PROVA ELETRÓNICO-DIGITAL EM BUSCA DA CRIMINALIDADE INFORMÁTICO-DIGITAL **13**

1. A REVOLUÇÃO DIGITAL DO NOSSO TEMPO: A SOCIEDADE ELETRÓNICO-DIGITAL E DOS FLUXOS INFORMACIONAIS E COMUNICACIONAIS **13**

2. O FLORESCIMENTO DE UMA NOVA CRIMINALIDADE E NOVAS NECESSIDADES DE INVESTIGAÇÃO CRIMINAL (FORENSE ELETRÓNICO-DIGITAL) **14**

3. A PROVA ELETRÓNICO-DIGITAL: "EM BUSCA" DA CRIMINALIDADE INFORMÁTICO-DIGITAL **15**

3.1. As metamorfoses da criminalidade informático-digital 15
3.2. As novas "exigências" da criminalidade informático-digital ao direito penal 17
3.3. O nascimento da prova eletrónico-digital no contexto de uma nova criminologia forense de investigação criminal 20
3.4. Características essenciais da prova eletrónico-digital e sua relevância no contexto de uma nova criminologia forense de investigação criminal 24

CAPÍTULO II – O ATUAL REGIME DE OBTENÇÃO DE PROVA ELETRÓNICO-DIGITAL PONDERADO E CODIFICADO NO CÓDIGO DE PROCESSO PENAL E NA LEGISLAÇÃO PROCESSUAL PENAL EXTRAVAGANTE **28**

1. EM BUSCA DO PARADIGMA PONDERADO E CODIFICADO, LEGALMENTE, EM MATÉRIA DE OBTENÇÃO DA PROVA ELETRÓNICO-DIGITAL **28**

1.1. A prova eletrónico-digital no contexto da apreensão de correspondência e das escutas telefónicas 29
1.2. A prova eletrónico-digital e o atual regime de retenção de dados de tráfego 33
1.3. A prova eletrónico-digital e os novos métodos de obtenção de prova na cibercriminalidade 34

CAPÍTULO III – AS DIFICULDADES DO ATUAL REGIME DE OBTENÇÃO DA PROVA ELETRÓNICO-DIGITAL EM TEMA DE "CORREIO ELETRÓNICO" 41

1. AS DIFICULDADES DO ATUAL REGIME DE OBTENÇÃO DA PROVA ELETRÓNICO-DIGITAL EM TEMA DE "CORREIO ELETRÓNICO" 41

1.1. A tese da revogação tácita do art. 189.º n.º 1 do CPP, por força do art. 17.º da Lei n.º 109/2019 41
1.2. A tese moderada 43

2. A LEI N.º 109/2009 E A LEI 32/2008: CASAMENTO OU DIVÓRCIO? 46

3. DA CORRESPONDÊNCIA CLÁSSICA À CORRESPONDÊNCIA ELETRÓNICA: UM CASAMENTO (IM)POSSÍVEL (?!) 47

4. QUAL É O REGIME APLICÁVEL AO CORREIO ELETRÓNICO E ÀS COMUNICAÇÕES SEMELHANTES? 54

4.1. O problema relativamente interceção do correio eletrónico ... 54
4.2. O problema do correio eletrónico recebido na "*inbox*" mas não aberto ou lido 56
4.3. O correio eletrónico já aberto 57
4.4. Quantos momentos e quantos regimes para o correio eletrónico? 58
4.5. A questão do conhecimento 64
4.6. Perspetivas "de iure condendo" 69
4.7. Síntese conclusiva 72

BIBLIOGRAFIA 75

JURISPRUDÊNCIA CONSULTADA 83

INTRODUÇÃO

A presente obra encontra-se divida em três Capítulos.

O Capítulo I, intitulado «Na era da sociedade informacional e comunicacional: a prova eletrónico-digital em busca da criminalidade informática digital», identifica as características da prova digital e da criminalidade do século XXI.

O Capítulo II, com o título «o atual regime de obtenção de prova eletrónico-digital ponderado e codificado no código de processo penal e na legislação processual penal extravagante», analisa a legislação aplicável à prova digital.

O Capítulo III, denominado «as dificuldades do atual regime de obtenção da prova eletrónico-digital em tema de correio eletrónico», termina com a análise dos regimes aplicáveis ao correio eletrónico e comunicações de natureza semelhante a par com considerações sobre o futuro da prova digital.

CAPÍTULO I – NA ERA DA SOCIEDADE INFORMACIONAL E COMUNICACIONAL: A PROVA ELETRÓNICO-DIGITAL EM BUSCA DA CRIMINALIDADE INFORMÁTICO-DIGITAL

1. A REVOLUÇÃO DIGITAL DO NOSSO TEMPO: A SOCIEDADE ELETRÓNICO-DIGITAL E DOS FLUXOS INFORMACIONAIS E COMUNICACIONAIS

A partir dos anos 90, do século XX, por força do surgimento da Internet, as formas de comunicação à distância não mais pararam de evoluir, invadindo todo o nosso quotidiano. As alterações económicas, sociais, laborais, entre outras, são imensas e, no presente momento, encontram-se longe de estarem devidamente avaliadas, sobretudo nos seus aspetos negativos para a evolução da espécie humana. O próprio serviço postal universal (entre nós, implementado, sob concessão pelos CTT), foi "seduzido", pelas novas tecnologias de informação e comunicação à distância (TIC´s). Contudo, permanece a dualidade de serviços de comunicação à distância, podendo-se, ainda hoje, sem grande esforço, enviar uma carta, manuscrita ou dactilografada, pelo serviço postal tradicional, mas, de igual modo, essa carta, poderá ser enviada através de um serviço «postal universal eletrónico».

O que, aqui, nos vai interessar é, essencialmente, verificar em que termos a "correspondência" clássica, cujo regime de obtenção

da prova encontramos no art. 179.º do CPP, tem a ver com o problema da nova «correspondência eletrónico-digital», em geral, mas, sobretudo, com o chamado correio eletrónico.

O avanço e a modernização das sociedades contemporâneas proporcionou, por parte da criminalidade, também uma atualização dos modos de atuação criminosa. Tudo isto, para efeitos de investigação criminal forense, implica a recolha da dita prova eletrónico-digital, com vista a poderem "ligar-se" determinados efeitos sancionatórios a certas condutas individuais ou de grupos criminosos.

2. O FLORESCIMENTO DE UMA NOVA CRIMINALIDADE E NOVAS NECESSIDADES DE INVESTIGAÇÃO CRIMINAL (FORENSE ELETRÓNICO-DIGITAL)

Com o florescimento de uma nova criminalidade logo surgiram, sob pena de total impunidade, novas necessidades e meios investigatórios. De facto, a investigação criminal forense eletrónico-digital, atento o tipo de prova em causa – a digital – não se compadece com as formas clássicas de investigação criminal.

Importa, contudo, perceber um pouco da fenomenologia de tal tipo de criminalidade.

3. A PROVA ELETRÓNICO-DIGITAL: "EM BUSCA" DA CRIMINALIDADE INFORMÁTICO-DIGITAL

3.1. As metamorfoses da criminalidade informático-digital

Tentar definir o que se deve entender por criminalidade informática, informático-digital, cibercrime ou cibercriminalidade, enquanto realidade reportada a todo o tipo de criminalidade que envolve instrumentos eletrónico-digitais não tem merecido a concordância da doutrina nacional e estrangeira.

Para SILVA RODRIGUES haveria que usar uma terminologia entre crimes informático-digitais próprios ou puros e impróprios ou impuros[1].

Por sua vez, PEDRO VENÂNCIO, propõe o seguinte conceito de criminalidade informática: «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»[2]. Desta definição ficam desde logo claros dois tipos diferentes de criminalidade informática ou cibercriminalidade. De um lado, temos a criminalidade informática em *sentido estrito*, em cujos elementos típicos se faz uso da informática, designadamente como meio de

---

[1] 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.
[2] VENÂNCIO, Pedro Dias, Lei do Cibercrime Anotada e Comentada, 1.ª Edição, Coimbra Editora, 2011, p.16.

execução, objeto da conduta, ou constituindo, ela mesma, o bem jurídico tutelado. Embora alguma doutrina indique que a criminalidade informático-digital não se reconduz apenas ao elenco da Lei 109/2009, o certo é que a mesma lei considera como "cibercrimes" ou "crimes informáticos", em sentido estrito, os crimes de falsidade informática, dano relativo a programas ou outros dados informáticos, sabotagem informática, acesso ilegítimo, interceção legítima e a reprodução ilegítima de programa protegido. Paralelamente, temos a criminalidade informática, *lato sensu*, onde se incluiriam todos os crimes que, embora praticados através de um sistema informático, não têm como elemento típico do crime a componente digital.

Por sua vez, no que à definição de cibercrime respeita, vemos que a Comissão Europeia[3] opta por uma divisão tripartida:

Numa primeira categoria, encontraríamos as formas tradicionais da atividade criminosa, que usariam a *internet* para cometer crimes, como sejam a fraude, falsificação, usurpação de identidade, etc;

Numa segunda categoria, teríamos a criminalidade ligada à publicação de conteúdos ilícitos, como sejam os conteúdos que incitam ao terrorismo, violência, racismo, xenofobia ou abuso sexual de menores;

Por último, numa terceira categoria, haveria que incluir os crimes exclusivos das redes eletrónicas, enquanto nova

[3] Acedido e consultado, em 2020-05-08, na URL: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=LEGISSUM%3Al14560>.

criminalidade, crimes totalmente desconhecidos até ao surgimento da internet.

Como se refere no citado documento "*Rumo a uma política geral de luta contra o cibercrime*", verifica-se que os criminosos atacam sistemas de informação, por vezes ameaçando infraestruturas de informação cruciais do Estado e, consequentemente, ameaçando diretamente os cidadãos.

3.2. As novas "exigências" da criminalidade informático-digital ao direito penal

A cibercriminalidade tem uma multiplicidade de características que a distingue das demais formas clássicas de criminalidade. Nesse sentido, verifica-se que o conceito de temporalidade, para efeitos do início da infração penal, implica que, no momento imediatamente antes do crime, o criminoso tome uma ação que desencadeie essa infração, à luz das regras da causalidade[4].

Na criminalidade informática nada obriga a que o criminoso se encontre, quando o resultado se produz, atrás do computador, visto que o momento do ataque pode ser (e será na maior parte dos casos) desfasado no tempo, ao estilo de «bomba relógio». O que significa que o ataque pode ser planeado para ser executado,

[4] Sem prejuízos do chamado «crime agravado pelo resultado», em que pode existir algum desfasamento relativamente à conduta inicial e ao efeito final produzido, devendo-se, a este propósito, consultar o disposto no art. 18.º do CP.

automaticamente, mediante pré-programação, sem o envolvimento do sujeito nesse preciso momento de efeito (danoso) social e penalmente relevante. Esta circunstância vai criar novos problemas à conceção tradicional do momento da prática do ato.

Também o conceito de espaço perde importância face a este novo tipo de criminalidade, um delinquente consegue tão facilmente provocar um resultado ao fundo da rua, como noutro país ou continente, não se verificando, portanto, uma verdadeira relação de espacialidade.

Todavia, o problema maior advém, neste contexto, da determinação do "*locus*" do crime, mormente para efeitos de competência territorial, quer para a investigação criminal, quer para o julgamento, podendo, inclusive, surgir conflitos negativos de competência judiciária.

Constata-se ainda que o cibercrime nos surge como um crime de fácil repetição e automatização. O que significa que, não só o agente do crime tem facilidade em programar atividades a serem "anonimamente" tomados por outros sistemas informáticos, como consegue, com grande facilidade, replicar e repetir um ataque bem-sucedido.

Além de tudo isto, verifica-se que estamos perante crimes aos quais estão associados um certo nível de complexidade técnica. O que significa que o seu cometimento implica consideráveis conhecimentos informáticos que, em boa verdade, felizmente, nem sempre se encontram ao alcance do cidadão comum. No

entanto, esta característica tem vindo a ser diluída face à disseminação de programas pré-formatados que permitem, a um utilizador comum, praticar um ataque como é o caso do RAAS (*Ransomware as a Service*). Na verdade, a tecnologia foi descomplexada por meio de "esquemas tecnológicos". É a própria tecnologia que permite a sua democratização, mediante a simplificação dos processos de "ativação".

Verificamos, ainda, que atentas as características dos próprios sistemas informáticos, estes permitem uma anonimização[5] da conduta do agente através de vários meios de ocultação da identidade. Acresce que, para além do anonimato, são crimes de uma especial danosidade social e penal, não só pelos prejuízos que podem causar a sistemas vitais de um Estado, mas também por não se encontrarem circunscritos a nenhuma área geográfica. Não surpreende por isso, que alguma doutrina aluda a um fenómeno de «deslocação criminosa para a internet», já que «as práticas e potencialidades informáticas, quer pela utilização da "Internet" quer através de "Intranet", potenciam exponencialmente a internacionalização da criminalidade informática, tornando mais difícil a reconstituição do percurso das informações entre o ponto emissor e o ponto recetor, permitindo a dissimulação do delinquente»[6].

[5] Importa notar que, na população em geral, existe a ideia de que a navegação anónima não é passível de ser «descoberta» e obtida prova digital. Trata-se de uma falácia completa.

[6] VENÂNCIO, Pedro Dias, «*Breve introdução da questão da investigação e meios de prova na criminalidade informática*», Verbo jurídico, Dezembro de 2006, acedido e consultado, em 2020-05-05, na URL:

3.3. O nascimento da prova eletrónico-digital no contexto de uma nova criminologia forense de investigação criminal

A prova digital ou, de modo mais completo, "eletrónico-digital"[7], configura, hoje, uma adaptação dos meios de obtenção da prova tradicionais (apreensão de correspondência, escutas telefónicas, retenção de dados, etc.) à nova sociedade informacional e comunicacional que os avanços eletrónico-digitais vieram permitir. A prova digital afigura-se, mais do que os meios clássicos, o método insubstituível e mais eficaz de combate ao flagelo da cibercriminalidade (*lato sensu*), introduzindo "novos saberes", como ocorre, por exemplo, com o uso da "geolocalização celular", dos equipamentos móveis de comunicação à distância, para permitir, à hora do homicídio, saber a posição geográfica de um potencial suspeito. O que significa que, num dado caso de homicídio, se o telemóvel, à hora do crime, for "apanhado", numa triangulação geográfica própria, embora não se possa concluir que foi o sujeito que cometeu o crime, certo é que se pode, com certeza absoluta (exceto se o telemóvel foi usado abusivamente), dizer se aquela pessoa esteve nas imediações do local do crime.

Para SILVA RODRIGUES a prova digital deveria ser percebida como «qualquer tipo de informação, com valor

<https://www.verbojuridico.net/doutrina/tecnologia/meiosprovacriminalidadeinformatica.pdf>.

[7] Preconizando tal conceito e justificando-o, em várias das suas obras, veja-se: RODRIGUES, Benjamim Silva, Direito Penal Parte Especial.

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»[8]. E, neste contexto, em 2008 e 2009[9], aduzia vários princípios, relativamente à obtenção da prova eletrónico-digital, em complemento dos vigentes, em matéria de produção probatória penal. Sistematizadamente, os princípios eram os seguintes:

i) Aplicabilidade cumulativa dos princípios gerais da prova em processo penal e ciência forense digital;

ii) Princípio da não alteração da prova eletrónico-digital no ato de recolha;

iii) Princípio da especialização ou qualificação do pessoal de investigação forense digital;

iv) Princípio da documentação de todas as fases de acesso, recolha, armazenamento, transferência, preservação ou apresentação/repetição da prova eletrónico-digital;

v) Princípio da pessoalidade do controlo da cadeia de custódia da produção da prova eletrónico-digital;

vi) Princípio da responsabilização repartida dos vários intervenientes na produção eletrónico-digital no respeito dos princípios forenses digitais.

[8] RODRIGUES, Benjamim Silva, *Direito Penal Parte Especial, Tomo I, Direito Penal Informático-Digital* (…), Coimbra, 2009, p. 722
[9] Escutas telefónicas, 2009, Volume II, p. 577-580.

Posteriormente, em 2015, no contexto da reivindicação da autonomia dogmática e científica da *criminologia forense*, para além de aludir aos clássicos princípios da prova, em processo penal, identifica *princípios criminológico-forenses* próprios que o mesmo pretende usar no seu método específico de investigação criminal forense a que deu o nome de «*Método Ideográfico-Nomotético, Semiótico, Dinâmico-Reversivo e Teleológico-Funcional e Racionalmente Orientado*»[10].

Em março de 2015, a *Europeia Union Agency for Cibersecurity* (ENISA) – Agência da União Europeia para a cibersegurança –, preconizou[11], cinco princípios fundamentais quanto à recolha de prova digital:

i) Princípio da Integridade dos Dados (*Data integrity*): a integridade dos dados deve ser preservada, garantindo que os dados apreendidos não sejam manipulados;

ii) Princípio da Cadeia de Custódia da Prova (*Audit Trail*): deve ser adotada uma cadeia de custódia que permita garantir a autenticidade e integridade da prova;

[10] RODRIGUES, Benjamim Silva, *Criminologia Forense (Forensic Criminology),* Tomo I – *O nascimento e a autonomia dogmático-científica da Criminologia Forense face à "Enciclopédia das Ciências Criminais" e à "Ciência Conjunta do Direito Penal*", *O Criminólogo Forense e o Método ideográfico-nomotético, semiótico, dinâmico-reversivo e teleológico-funcional e racionalmente orientado de investigação Criminal*, Rei dos Livros/Empório do Direito, 2015, p. 51-53.

[11] No seu «*Electronic Evidence – a Basic Guide for Firts Responders, Good Practice material for CERT first responders*», 2014, p. 5-8, acedido e consultado, em 2020-04-23, na URL: <https://www.enisa.europa.eu/publications/electronic-evidence-a-basic-guide-for-first-responders>.

iii) Princípio do Apoio Especializado (*Specialist Support*): o apoio técnico especializado deve ser requerido sempre que o âmbito da prova ultrapasse os conhecimentos do investigador;

iv) Princípio da formação profissional apropriada (*Appropriate Training*): os OPC e os magistrados devem ter formação contínua e apropriada para garantir uma apreensão de prova digital correta e eficiente;

v) Princípio da Legalidade (*Legality*): o responsável pela investigação deve garantir o respeito dos princípios aqui referidos e o cumprimento da lei.

Todos estes modelos e princípios, para a investigação forense eletrónico-digital, encontram-se justificados a partir da constatação que este tipo de prova contém características essenciais que, na sua produção e reprodução, no decurso do inquérito criminal e na audiência de julgamento, devem ser tidas em conta para garantir a veracidade e autenticidade da mesma. Urge, por isso, ganhar alguma densidade dogmática, acerca das características da prova digital.

3.4. Características essenciais da prova eletrónico-digital e sua relevância no contexto de uma nova criminologia forense de investigação criminal

A prova digital, enquanto meio de obtenção da prova, caracteriza-se, principalmente, pela sua imaterialidade, efemeridade e volatilidade[12].

A sua imaterialidade implica, desde logo, uma capacidade técnica, que não é necessariamente encontrada no cidadão comum, de tal modo que se afigura imprescindível, para o investigador criminal forense digital, uma formação técnica constante e o apoio qualificado por técnicos especializados e altamente qualificados. De igual modo, afiguram-se necessários programas e material informático sofisticado.

Por sua vez, a volatilidade da prova digital refere-se ao facto de este ser um tipo de prova facilmente manipulável e, portanto, a necessidade de garantir uma identificação clara da prova e dos procedimentos que foram efetuados e o uso de técnicas para

[12] Não obstante isso, alguns autores advogam outras características, como é o caso de SILVA RODRIGUES, que vai ao ponto de identificar: *i*) A efemeridade ou não durabilidade da prova eletrónico-digital; *ii*) A fragilidade e alterabilidade da prova eletrónico-digital; *iii*) A aparente imaterialidade ou não visibilidade da prova eletrónico-digital; *iv*) A complexidade ou codificação da prova eletrónico-digital; *v*) A dispersão da prova eletrónico-digital; *vi*) O "dinamismo" e "mutabilidade" da prova eletrónico-digital. 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*, Com Prefácio da D.ra SARA ANTUNES, Coimbra, 2009,720-726.

preservar a prova no seu estado ao tempo da apreensão, já que esta é, também ela, uma prova efémera.

Como meio de obtenção da prova facilmente manipulável e de alta complexidade técnica, afigura-se imprescindível garantir recursos próprios e adequados, para a sua "apreensão" (cópia ou documentação) e preservação, com todas as garantias do direito processual penal, por forma a salvaguardar a sua integridade e confiança, por parte de todos os operadores judiciários, permitindo a sua compreensão, mesmo ao mais infoexcluído dos cidadãos.

A investigação criminal já percorreu um longo caminho desde os estudos criminológicos de EDMOND LOCARD e a sua teoria da "troca" ou do "toque", a significar que o homem, no seu atuar diário, deixa sempre algum vestígio encontrável ou recuperável. Além disso, a racionalidade, a lógica técnico-científica, bem como a mais pura "experiência de vida", possibilitou, por parte da investigação criminal, deduções brilhantes, tão eloquentemente ilustradas pela figura de SHERLOCK HOLMES, a personagem de Sir ARTHUR CONAN DOYLE[13].

Mais do que nunca, o criminólogo forense, o investigador da cena do crime, deve ser alguém que tem, em termos de saberes, um alargado horizonte, visto que, aqui, a multidisciplinariedade dos saberes é algo que se impõe, já que novas ciências se convocam para a investigação criminal do século XXI.

[13] Outras poderiam ser citadas, de muitas outras séries, como POIROT, MAIGRET, CRIMINAL MINDS, CSI, etc.

O aparecimento de novos meios de investigação, como é o caso das perícias de ADN, por força do conhecimento do genoma humano e desenvolvimento da genética, a análise de impressões digitais e genéticas, bem como da psicologia forense ("*profiling*") e a localização de um sistema telemático ("georreferenciação eletrónica"), obrigam hoje os OPC a usar e conhecer um conjunto de técnicas científicas e a ter, nos seus quadros, recursos humanos altamente especializados, para fazerem face a uma criminalidade também ela, mais sofisticada.

No contexto do cibercrime, a necessidade de dotar os OPC das competências tecnológicas, seja na obtenção de prova digital ou na investigação do cibercrime em sentido estrito, obrigou os OPC a uma relação estreita entre os técnicos e os inspetores responsáveis pela investigação e que, ao nível do MP, culminou na criação do Gabinete de Cibercrime, a 7 de dezembro de 2011.

Uma vez identificado o tipo e características essenciais da criminalidade informático-digital, afigura-se necessário proceder à identificação dos principais aspetos do atual regime processual penal de obtenção de prova eletrónico-digital, na sua diversidade e multiplicidade de localizações legais.

Na verdade, como se referiu, a prova eletrónico-digital deve, hoje em dia, ser obtida, em termos de contextualização legal, por meio da mobilização dos regimes processuais penais da apreensão de correspondência e das escutas telefónicas, consagrados, respetivamente, nos arts. 179.º e 187.º a 190.º do CPP. Haverá ainda que ter em conta a legislação processual penal

extravagante ligada à retenção de dados de tráfego, que encontramos na Lei n.º 32/2008, bem como os instrumentos específicos e inovadores, de investigação criminal forense digital, a que se reportam os arts. 11.º a 19.º da Lei n.º 109/2009.

CAPÍTULO II – O ATUAL REGIME DE OBTENÇÃO DE PROVA ELETRÓNICO-DIGITAL PONDERADO E CODIFICADO NO CÓDIGO DE PROCESSO PENAL E NA LEGISLAÇÃO PROCESSUAL PENAL EXTRAVAGANTE

1. EM BUSCA DO PARADIGMA PONDERADO E CODIFICADO, LEGALMENTE, EM MATÉRIA DE OBTENÇÃO DA PROVA ELETRÓNICO-DIGITAL

Na ânsia de encontrarmos os contornos essenciais do atual paradigma ponderado e codificado, legalmente, em matéria de obtenção da prova eletrónico-digital, analisaremos o atual regime das escutas telefónicas[14] (com alguma intercorrência com o da apreensão de correspondência[15]), tido ainda como modelo-base da ingerência nas comunicações privadas. Iremos depois, voltar o nosso olhar para a matéria da retenção de dados de tráfego[16] e dos novos meios de obtenção da prova eletrónico-digital[17], em contexto de combate ao cibercrime.

[14] Constante dos arts. 187.º a 190.º, do CPP.
[15] Presente, essencialmente, no art. 179.º, do CPP.
[16] Deitando um olhar sobre a Lei n.º 32/2008, de 17 de julho.
[17] Sobretudo, o disposto nos arts. 11.º a 19.º, da Lei n.º 109/2009.

1.1. A prova eletrónico-digital no contexto da apreensão de correspondência e das escutas telefónicas

O Código de Processo Penal, no título III, reservado aos meios de obtenção da prova, prevê os vários meios de obtenção da prova suscetíveis de serem usados na investigação criminal, prevendo, como se referiu, no art. 179.º, a apreensão de correspondência, ao passo que, nos arts. 187.º a 190.º, aborda a matéria do regime das escutas telefónicas.

A escuta telefónica, enquanto meio de obtenção da prova, surge como um dos mais gravosos e de alta danosidade social, invadindo a esfera de direitos dos cidadãos, correndo-se o risco de lesar o chamado «âmbito mínimo ou nuclear» da intimidade; e, com isso, a própria dignidade humana. Não admirará, por isso, que o seu uso seja restrito à investigação criminal de crimes mais graves ou cuja investigação, por outro meio, não se afigura possível. O legislador ensaia, no art. 187.º, segundo SILVA RODRIGUES, três critérios diferenciados, o critério da moldura[18], do catálogo[19] e da dupla indexação.

Importa sublinhar, para o objeto do presente estudo, que, na sua redação originária, o art. 190.º[20], hoje substituído,

---

[18] Veja-se o art. 187.º, n.º 1, alínea *a*), do CPP.
[19] Veja-se o art. 187.º, n.º 1, alíneas *b*) a *g*), do CPP.
[20] «*O disposto nos arts. 187.º, 188.º e 189.º é correspondentemente aplicável às conversações ou comunicações transmitidas por qualquer meio técnico diferente do telefone, designadamente correio eletrónico ou outras formas de transmissão de dados por via telemática, bem como à interceção das comunicações entre presentes*».

integralmente, após as Reformas de 1998 e 2007, pelo art. 189.º, dispunha, no que ao regime de "Extensão" das escutas telefónicas, a outros meios de obtenção da prova, diz respeito, o seguinte: «(…) às conversações ou comunicações transmitidas por qualquer meio técnico diferente do telefone». Esta extensão afigura-se, em termos hermenêutico-jurídicos e constitucionais, verdadeiramente censurável, pois, na verdade, o regime processual penal da obtenção da prova mediante escutas telefónicas configura uma restrição do direito à palavra, inviolabilidade do sigilo das comunicações privadas e da correspondência, privacidade, direito à autodeterminação informacional e comunicacional, pelo que não se pode entender que em contexto de restrição de direitos fundamentais, onde a máxima é de que a restrição deve ser a menor possível, o legislador, dentro da restrição, realiza ao invés uma ampliação.

Não admirará, por isso, que alguma doutrina se tenha pronunciado no sentido da inconstitucionalidade, como foi o caso de SILVA RODRIGUES[21] e de FARIA COSTA, este último indo ao ponto de precisar que «o regime excecional, porque excecional, não pode alargar-se, sob pena de contradição palmar e insanável»[22]. Verifica-se, assim, que, com a alteração operada, o art. 189.º, passou, no seu n.º 1, a referir: «*O disposto nos arts.*

[21] RODRIGUES, Benjamim Silva, *Das Escutas Telefónicas*, Tomo II, p. 425-427.

[22] COSTA, José de Faria, «*As telecomunicações e a privacidade: o olhar (in)discreto de um penalista*», *in*: As telecomunicações e o direito na sociedade da informação, Atas do Colóquio organizado pelo IJC em 23 e 24 de abril de 1998, IJC, 1999, p. 76-77

187.º e 188.º é correspondentemente aplicável às conversações ou comunicações transmitidas por qualquer meio técnico diferente do telefone, designadamente correio eletrónico ou outras formas de transmissão de dados por via telemática, mesmo que se encontrem guardadas em suporte digital, e à interceção das comunicações entre presentes». E, por seu turno, o n.º 2, refere: «*A obtenção e junção aos autos de dados sobre a localização celular ou de registos da realização de conversações ou comunicações só podem ser ordenadas ou autorizadas, em qualquer fase do processo, por despacho do juiz, quanto a crimes previstos no n.º 1 do art. 187.º e em relação às pessoas referidas no n.º 4 do mesmo art.*».

Presentemente, por força do teor dado, por aquelas Reformas, ao novo art. 189.º, em substituição do originário, com a manutenção da epígrafe «Extensão», verifica-se que este regime (n.os 1 e 2) de obtenção da prova pode ser agora estendido:

i) Às conversações ou comunicações transmitidas por qualquer meio técnico diferente do telefone, designadamente:

ia) Correio eletrónico;

ib) Outras formas de transmissão de dados por via telemática:

ib1) guardadas em suporte digital;

ib2) não guardadas em suporte digital;

ii) À interceção das comunicações entre presentes;

iii) À obtenção e junção aos autos de dados:

iiia) sobre a localização celular da realização de conversações ou comunicações;

iiib) sobre registos da realização de conversações ou comunicações.

Verifica-se, assim, que há três categorias[23], com algumas subespécies de comunicações a que, extensivamente, é alargado o regime processual penal das escutas telefónicas.

Este preceito, segundo COSTA ANDRADE, afigura-se como uma verdadeira «casa de horrores hermenêuticos»[24], visto que não veio, de forma alguma, resolver ou solucionar as críticas que já vinham desde a versão original deste artigo, misturando conceitos e situações diferentes e remetendo, preguiçosamente, tudo para o regime das escutas telefónicas.

Na verdade, o que constitui uma conversa transmitida por qualquer meio técnico diferente do telefone? Em 1987, a expressão «meio diferente do telefone», poderia ter um âmbito de aplicação mais reduzido (fax, etc.). No entanto, nos dias de hoje e na falta de uma maior delimitação, estariam incluídos não só o correio eletrónico, como todo o tipo de comunicações instantâneas via internet como o "WhatsApp" ou o "Facebook Messenger".

[23] Embora alguns autores aludam a cinco dimensões. É o caso de: JESUS, Francisco Marcolino de Os *meios de obtenção de prova em processo penal*, 2.ª Edição, Reimpressão, 2016, 319-328

[24] ANDRADE, Manuel Da Costa, *Bruscamente no verão passado, a Reforma do Código de Processo Penal-Observação críticas sobre uma lei que podia e devia ter sido diferente*, Coimbra Editora, 2009

1.2. A prova eletrónico-digital e o atual regime de retenção de dados de tráfego

Em 2008, o legislador português adotou a Lei n.º 32/2008, de 17 de julho, que visou transpor, para a ordem jurídica interna a Diretiva n.º 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de março, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações.

Para efeitos do nosso estudo, ganham especial importância os arts. 3.º a 11.º, deste diploma. Na verdade, o art. 3.º, n.º 1, da lei não deixa dúvidas acerca dos seus intentos, visto que ela tem «*(…) por finalidade exclusiva a investigação, deteção e repressão de crimes graves por parte das autoridades competentes*».

O preceito mais problemático e pertinente, para o nosso tema, é o que encontramos no art. 6.º, em que se obriga (os fornecedores de serviços de comunicações eletrónicas publicamente disponíveis ou de uma rede pública de comunicações) a conservar os dados de tráfego pelo período de um ano. Naturalmente, esta indexação temporal é imposta pelo princípio da proibição de excesso, contudo e não obstante, poderá configurar uma situação materialmente inconstitucional, já que funcionaria como uma base de dados generalizada, relativamente à atividade no ciberespaço, pondo em causa a reserva da intimidade pessoal e familiar (e informático-digital), bem como a sua autodeterminação informacional e comunicacional, totalmente

devassada, sem ser em contexto de investigação criminal ou de qualquer processo criminal. Aliás, face a desenvolvimentos legislativos internacionais e posicionamentos do TJUE[25] e da CNPD[26], tal preceito está condenado, a breve trecho[27], ao fracasso ou, no limite, vir invocar-se a inconstitucionalidade material de tal prova, por se encontrar fora de um processo criminal, em violação do disposto no art. 34.º n.os 1 e 4, da CRP, e, ainda, ao arrepio do princípio da proibição de excesso (adequação, necessidade e proporcionalidade *stricto sensu*), ínsito no art. 18.º, n.º 2, da CRP. E, para agravar tudo isto, o legislador, passado um ano, em 2009, viria a adotar a Lei n.º 109/2009 onde não cuidou, como veremos, de harmonizar o que já estava legislado, quer no CPP, quer na Lei n.º 32/2008.

1.3. A prova eletrónico-digital e os novos métodos de obtenção de prova na cibercriminalidade

A Lei n.º 109/91, de 17 de agosto, foi a primeira tentativa de o legislador nacional fazer face a um problema emergente, a

[25] Estamos a pensar no Acórdão *Digital Rights Ireland Ltd*, proferido pela Grande Secção, nos Processos n.os C-293/12 e C-594/12, em 8 de Abril de 2014, que decidiu pela invalidade da diretiva 2006/24.

[26] Na sua Deliberação nº 1008/2017, de 18 de julho, a CNPD resolveu «desaplicar aquela lei [a Lei n.º 32/2008] nas situações que lhe sejam submetidas para apreciação», por entender que, sendo as normas nela inscritas lesivas, de acordo com o seu juízo, da Carta dos Direitos Fundamentais da União e da Constituição da República Portuguesa, deveria agir «em cumprimento do primado do Direito da União e da prevalência da Constituição

[27] Veja-se, a Recomendação n.º 1/B/2019, da Provedora de Justiça MARIA LÚCIA AMARAL), relativamente à Lei n.º 32/2008 consultado, em 2020-04-01, na URL: <https://www.provedor-jus.pt/site/public/archive/doc/Rec_1B2019_2019_01_22_Recomendacao_da_Protecao_de_dados_Ministra_Justica.pdf>.

criminalidade informática ou cibercriminalidade. Preocupando-se apenas com a tipificação de crimes informáticos, em sentido próprio, bem como as respetivas penas acessórias, rapidamente ficou claro que esta lei não era suficiente para o mundo digital do século XXI. Não será alheio a tal, o facto de que a mesma nem sequer foi contemporânea da internet, com a amplitude e a complexidade que hoje conhecemos, ainda a viver os seus primeiros dias e sem a «democratização» social a que, presentemente, assistimos.

Importa notar que, no contexto internacional, a Convenção sobre o cibercrime, também conhecida como a convenção de Budapeste, elaborada pelo Conselho da Europa, visava três objetivos principais. Em primeiro lugar, a criação e harmonização da legislação, entre os vários países signatários, que punisse os crimes informáticos ou ligados ao cibercrime. Em segundo lugar, conferir, aos OPC e aos Tribunais, os meios adequados à investigação criminal forense digital (e respetiva viabilização do seu julgamento) dos crimes cometidos através de meios informáticos. Por fim, a criação e fomento da cooperação internacional para o combate a um tipo de criminalidade que, pelas suas características, em não poucas vezes, também se afigura transfronteiriça e, por isso, convoca a chamada cooperação judiciária e policial internacional.

A Decisão Quadro n.º 2005/222/JAI do Conselho da Europa[28], que viria a ser substituída pela Diretiva 2013/40/UE do Parlamento Europeu e do Conselho, de 12 de agosto de 2013, relativa a ataques contra os sistemas de informação[29], veio introduzir fortes alterações, não só ao nível da criminalidade informática, mas, de igual modo, ao provocar grandes mudanças ao nível da apreensão e preservação de dados informáticos. Na verdade, esta decisão tinha como objetivo a:

i) Definição de conceitos jurídicos e informáticos;

ii) Tipificação de crimes informáticos;

iii) Previsão de medidas de obtenção e preservação de prova digital e de medidas de cooperação internacional tendo em visto o combate da criminalidade informática.

Com vista a implementar alguns dos objetivos da Convenção do Cibercrime e da Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de fevereiro, o legislador português viria a adotar a Lei n.º 109/2009, de 15 de Setembro, cujo objetivo, logo denunciado no art. 1.º, visava o estabelecimento das «*disposições penais materiais e processuais, bem como as disposições relativas à cooperação internacional em matéria penal, relativas ao domínio do cibercrime e da recolha de prova em suporte*

[28] Decisão-Quadro 2005/222/JAI do Conselho, de 24 de fevereiro de 2005, relativa a ataques contra os sistemas de informação, Jornal Oficial, L 69, 16.3.2005, p. 67–71.

[29] Jornal Oficial da União Europeia, L 218, de 14/08/2013: [8-14], acedida e consultada, em 2020-05-05, na URL: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32013L0040&from=EN>.

eletrónico». Os arts. 3.º a 10.º, da Lei n.º 109/2009, tratam das chamadas «Disposições penais materiais»[30]. Por sua vez, com especial importância para o nosso tema, surgem as chamadas «Disposições processuais», em que encontramos, como novas e variadas formas de obtenção da prova eletrónico-digital, para certo tipo de criminalidade, os seguintes mecanismos:

i) A preservação expedita de dados – art. 12.º;

ii) A revelação expedita de dados de tráfego – art. 13.º;

iii) A injunção para apresentação ou concessão do acesso a dados – art. 14.º;

iv) A pesquisa de dados informáticos – art. 15.º;

v) A apreensão de dados informáticos – art. 16.º;

vi) A apreensão de correio eletrónico e registos de comunicações de natureza semelhante – art. 17.º;

vi) A interceção de comunicações – art. 18.º;

vii) As ações encobertas – art. 19.º.

No contexto do deslindar do nosso problema, isto é, saber qual o regime processual penal que devemos aplicar, hoje em dia, à obtenção da prova eletrónico-digital a partir do correio eletrónico, ganham especial importância os arts. 17.º e 18.º, da Lei n.º 109/2009, conexionados com os arts. 179.º e 189.º, n.º 1, do CPP.

[30] Aí se prevendo a falsidade informática (art. 3.º), o dano relativo a programas ou outros dados informáticos (art. 4.º), a sabotagem informática (art. 5.º), o acesso ilegítimo (art. 6.º), a intercepção ilegítima (art. 7.º), a reprodução ilegítima de programa protegido (art. 8.º), a responsabilidade penal das pessoas colectivas e entidades equiparadas (art. 9.º) e a perda de bens (art. 10.º).

O teor do art. 17.º (Apreensão de correio eletrónico e registos de comunicações de natureza semelhante), da Lei do Cibercrime é o seguinte: «*Quando, no decurso de uma pesquisa informática ou outro acesso legítimo a um sistema informático, forem encontrados, armazenados nesse sistema informático ou noutro a que seja permitido o acesso legítimo a partir do primeiro, mensagens de correio eletrónico ou registos de comunicações de natureza semelhante, o juiz pode autorizar ou ordenar, por despacho, a apreensão daqueles que se afigurem ser de grande interesse para a descoberta da verdade ou para a prova, aplicando-se correspondentemente o regime da apreensão de correspondência previsto no Código de Processo Penal*». Por sua vez, o art. 18.º (Interceção de comunicações), refere:

«*1 – É admissível o recurso à interceção de comunicações em processos relativos a crimes:*

a) Previstos na presente lei; ou

b) Cometidos por meio de um sistema informático ou em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico, quando tais crimes se encontrem previstos no art. 187.º do Código de Processo Penal.

2 – A interceção e o registo de transmissões de dados informáticos só podem ser autorizados durante o inquérito, se houver razões para crer que a diligência é indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter, por despacho fundamentado do juiz de instrução e mediante requerimento do MP.

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

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

Questiona-se, à luz dos citados preceitos, qual será o regime processual penal de obtenção da prova digital aplicável à apreensão de correio eletrónico: se segue o mesmo regime do que a apreensão de correspondência, posta no art. 179.º do CPP, ou, é lhe aplicável o regime processual penal das escutas telefónicas, nomeadamente, o art. 189.º, n.º 1 do CPP e, ainda, se exclusivamente lhe deverá ser aplicável, após 2009, o regime do art. 17.º, da Lei n.º 109/2009?

Como se relacionam e harmonizam tais regimes?

Do teor do art. 11.º, da Lei do Cibercrime, parece resultar a ideia de que o art. 17.º, somente se aplicaria para os casos de obtenção da prova eletrónico-digital para os crimes previstos nesta lei especial, cometidos por meio de um sistema informático ou em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico acabando, neste preceito, por permitir o uso de prova eletrónico-digital fora dos crimes

informáticos, já que o que importa é que «seja necessário proceder à recolha de prova em suporte eletrónico».

Importa notar que este regime de ingerência nas comunicações privadas e na correspondência, acaba por renegar a solução apertada e de ponderação inerente ao art. 187.º, n.º 1 do CPP, visto que alarga, sem limite de moldura, a possibilidade de acesso a prova eletrónico-digital, podendo questionar-se sobre a legitimidade deste alargamento como fez alguma doutrina nacional[31]. Não estará o criminólogo forense e o investigador criminal forense digital condenado a rolar a pedra para o sopé da montanha e, uma vez aí chegado, julgando ter encontrado uma forma de compatibilizar a desordem legislativa, cair, novamente, até ao abismo da incerteza e das dificuldades operativas.

Qual a solução proposta?

[31] Nesse sentido, veja-se: RODRIGUES, *Benjamim Silva, Das Escutas Telefónicas*, Tomo II, p. 546-564.

CAPÍTULO III – AS DIFICULDADES DO ATUAL REGIME DE OBTENÇÃO DA PROVA ELETRÓNICO-DIGITAL EM TEMA DE "CORREIO ELETRÓNICO"

1. AS DIFICULDADES DO ATUAL REGIME DE OBTENÇÃO DA PROVA ELETRÓNICO-DIGITAL EM TEMA DE "CORREIO ELETRÓNICO"

Verificamos que o atual regime de obtenção da prova eletrónico-digital é uma verdadeira confusão, tal a multiplicidade de documentos legais que convergem nas zonas de aplicação e divergem quanto ao tratamento a dar a situações similares, sem orientação do legislador, de como harmonizar esta trindade jurídica. Não entendemos que existe uma interpretação dos documentos legais (arts. 179.º, 189.º, n.º 1, do CPP, e arts. 17.º e 18.º, da Lei n.º 109/2009) para cada gosto, mas sim que cada solução apontada poderá ter duas ou três perspetivas válidas fazendo sentido, portanto, ganharmos alguma densidade dogmática e doutrinária, ao nível desta matéria.

1.1. A tese da revogação tácita do art. 189.º n.º 1 do CPP, por força do art. 17.º da Lei n.º 109/2019

As divergências, ao nível das soluções legais de obtenção da prova eletrónico-digital, previstas no CPP e na LC, afiguram-se claras e evidentes. Numa fórmula esdrúxula de limitação do regime processual das escutas telefónicas, que não é limitação alguma, mas sim, uma extensão e alargamento do âmbito da

restrição, posta no art. 189.º, n.º 1 do CPP, o legislador, após as Reformas de 1998 e 2007, foi misturando realidades. Na verdade, mesclou a ingerência nas comunicações eletrónicas com as captações de conversações e comunicações em "ambiente físico", entre presentes (cara a cara), em que a veiculação do fluxo ocorre pelo meio físico e não pelas redes de comunicações eletrónicas, publicamente acessíveis.

Na opinião de JOÃO CONDE CORREIA[32], a extensão do art. 189.º deve considerar-se, desde logo, em grande parte, tacitamente revogada pelas Leis n.os 32/2008 e 109/2009, visto que, no seu entender, a sobreposição regimental, por parte das leis extravagantes, relativamente ao art. 189.º, n.º 1, do CPP, implicariam, na vertente do acesso ao correio eletrónico, a sua revogação e exclusiva sujeição ao previsto no art. 17.º, da LC.

Outra parte da doutrina defende que, a LC, por força do art. 11.º n.º 1, alínea c), atenta contra o princípio da proibição de excesso, bem como os direitos à palavra, inviolabilidade do sigilo das comunicações privadas e da correspondência, senão mesmo a chamada "privacidade eletrónico-digital" [33], que alguma doutrina

[32] CORREIA, João Conde, «*Prova digital: as leis que temos e a lei que devíamos ter*», RMP, N.º139, Julho/Setembro 2014, p. 29-59, acedida e consultada, em 2020-05-02, na URL: <http://rmp.smmp.pt/wp-content/uploads/2014/04/3_RMP_139_Joao_Correia.pdf>.

[33] SILVA RODRIGUES advoga tal compreensão, indo ao ponto de identificar um super-conceito ou direito que seria uma confluência de todos esses direitos fundamentais para lograr o «direito à autodeterminação informacional e comunicacional».

identifica a partir da confluência dos arts. 1.º, 26.º, 34.º, n.os 1 e 4, 35.º, n.os e 4, e 37.º, da CRP.

1.2. A tese moderada

Sem prejuízo do anteriormente referido, qualquer solução que, aqui se adiante, será sempre uma solução artificial e não pretendida pelo legislador que, frontalmente, no art. 189.º, n.º 1, do CPP, e no art. 17.º, da Lei n.º 109/2009, adota regimes processuais penais de obtenção da prova eletrónico-digital, inegavelmente, contraditórios.

Um dos problemas mais debatidos, em torno do n.º 1 do art. 189.º, mesmo ao nível dos nossos tribunais, é o acesso às SMS, isto é, ao conteúdo de uma mensagem que, hoje em dia, pode ser imagética, escrita ou mista.

A que regime ficam submetidas as SMS enviada por telemóveis?

Poderá a natureza das escutas telefónicas, isto é, o tipo de comunicações a que se destinou, originariamente, ajudar a deslindar e erguer uma solução que permite a convivência ou compatibilização de ambos os regimes? E, concluindo-se estarem vocacionadas para as comunicações e conversações orais, será que tal não ajudará a delimitar o campo das escutas telefónicas, face aos modernos meios de obtenção da prova digital, que, esses sim, seriam votados a outras formas de comunicação e conversação, escrita ou com imagem, senão mesmo mista?

Na verdade, SILVA RODRIGUES[34], aduz, em termos que subscrevemos, que, geneticamente, o instituto das escutas telefónicas se encontrava circunscrito às conversações e comunicações faladas. Já anteriormente, nesse sentido, ainda que sob a alçada do antigo art. 190.º do CPP (atual art. 189.º), COSTA ANDRADE referia que as escutas telefónicas seriam «um regime em princípio reservado às formas de comunicação oral, isto é, que possibilitam a emissão e receção da própria palavra falada. Dele estarão, por exemplo, excluídas formas de comunicação como o telégrafo ou o telefax»[35].

Esta posição defende que o regime das escutas telefónicas, criado e pensado para comunicações orais, por voz, não faria sentido ser estendido às comunicações por escrito e, portanto, tais tipos de comunicações eletrónicas especiais e escritas não estariam sob a alçada do regime processual penal das escutas telefónicas, que encontramos nos arts. 187.º a 190.º do CPP, mas sob o regime da apreensão de correio eletrónico do art. 17.º, da lei do cibercrime.

No contexto das comunicações eletrónicas surgem, hoje, dois tipos de comunicação, com características próprias e diferente relevância, as que fazem uso da palavra escrita e as que fazem uso da palavra falada, bem como as mensagens imagéticas (envio de

[34] RODRIGUES, Benjamin Silva, *Das escutas telefónicas*, Tomo I, p. 455 e ss.
[35] ANDRADE, Manuel da Costa, *Sobre as proibições de Prova em Processo Penal*, Reimpressão, Coimbra Editora, Coimbra, 2006, p. 274-275.

imagem) ou, mistas, em formato de vídeo ou a realização de chamada com imagem.

Sabido que a palavra falada é, desde os primórdios da humanidade, a base da comunicação, é instantânea e tendencialmente efémera, para ser ouvida apenas pelos intervenientes e para depois ser, eventualmente, esquecida e, por tudo isto, é também instintiva e irrefletida. Por sua vez, a palavra escrita surge com a invenção da escrita, limitada inicialmente às elites económicas e culturais da sociedade, a habilidade de ler e escrever ganha importância de forma gradual, com particular destaque para invenção da imprensa no século XV e, particularmente, com a literacia generalizada da população nos últimos séculos. Constitui uma comunicação mais racional, com intenção de perdurar no tempo, onde o autor ao redigir qualquer texto, fá-lo conscientemente e selecionando as palavras, sem descurar a grafia e a gramática. É, portanto, normal, e até desejável, que sejam alvo de graus de proteção diferentes, já que a gravação/interceção da palavra falada pelas características que já referimos constitui uma ofensa superior aos direitos dos cidadãos. Parece-nos que, na senda destes autores, deveria haver uma clara diferenciação entre os regimes, até face às diferenças que já referimos entre a palavra escrita e a palavra falada, aplicando-se por isso ao SMS o regime da apreensão de correio eletrónico.

2. A LEI N.º 109/2009 E A LEI 32/2008: CASAMENTO OU DIVÓRCIO?

No que respeita ao relacionamento, entre as Leis n.º 109/2009 e a Lei n.º 32/2008, poderíamos equacionar se estamos perante o casamento de dois regimes processuais penais de obtenção da prova eletrónico-digital ou, pelo contrário, se assistimos a um violento divórcio.

A questão da harmonização de tais regimes suscita algumas divergências na doutrina nacional.

Para PAULO DÁ MESQUITA, a LC teria vindo revogar o art. 9.º, da Lei n.º 32/2008, uma vez que a panóplia de dados abrangido pela LC é mais abrangente que os contidos na Lei n.º 32/2008. Subscrevendo, igualmente, tal compreensão, DUARTE RODRIGUES NUNES defende uma "interpretação hábil"[36] do art. 11.º, n.º 2 da LC[37]. Importa, todavia, sublinhar que, na doutrina maioritária, vigora o entendimento de que os diplomas se encontram numa relação de "pura complementaridade"[38]. Em abono de tal compreensão está o elemento gramatical[39], atento o

---

[36] NUNES, Duarte Rodrigues, *Os meios de obtenção de prova previstos na lei do cibercrime*, GESTLEGAL, Coimbra, 2018, p.25

[37] Relativo a esta temática, Acórdão do TRL a de 22/01/2013, relatado pela Juíza-Desembargadora ALDA TOMÉ CASIMIRO; e, ainda, o Acórdão TRC de 26/02/2014, relatado pelo Juiz-Desembargador FERNANDO CHAVES, disponíveis em www.dsgi.pt

[38] CORREIA, João Conde, «*Prova digital: as leis que temos e a lei que devíamos ter*», RMP, N.º139, julho/setembro 2014,p.37

[39] Que, consabidamente, desempenha uma função negativa (proibição de uma interpretação que não tenha um mínimo de expressão na letra da lei) e positiva (entre duas opções, escolher a mais *performante*).

que se refere no art. 11.º, n.º 2 da LC, ao referir que: «*As disposições processuais previstas no presente capítulo não prejudicam o regime da lei 32/2008 de 17 de julho*». Tal dispositivo demonstra a intenção do legislador em proceder à articulação e compatibilização entre os diplomas.

3. DA CORRESPONDÊNCIA CLÁSSICA À CORRESPONDÊNCIA ELETRÓNICA: UM CASAMENTO (IM)POSSÍVEL (?!)

Os problemas que abordamos, nos pontos anteriores, também se colocam no relacionamento e compreensão entre a solução legislativa vertida no art. 179.º do CPP, e o disposto no art. 17.º da LC. Urge verificar em que termos deve ser compreendida a remissão para o CPP, posta no art. 17.º, da Lei n.º 109/2009, quando refere: «(…) *aplicando-se correspondentemente o regime da apreensão de correspondência previsto no Código de Processo Penal*». Importa relembrar que a correspondência, enquanto forma de comunicação dotada de uma particular importância, encontra-se constitucionalmente protegida, ao nível dos arts. 1.º, 26.º, n.os 1 e 2, 32.º, n.º 8, 34.º, n.os 1 e 4, e 35.º, n.os 1 e 4 da CRP. Verifica-se, mesmo, ao nível dos arts. 126.º, n. os 3 e 4, e 167.º, do CPP, a proibição de prova, exceto quando tal ingerência for imprescindível para imputar, por exemplo, um crime a um agente da PJ, que realizou escutas telefónicas não autorizadas.

Consideram-se correspondência, «as missivas, encomendas, valores, telegramas e qualquer forma estereotipada de correio, desde que enviada para um destinatário determinado»[40]. Este regime estender-se-á a toda a correspondência que «vai a caminho ou já atingiu a caixa postal do destinatário, o seu destino, mas, sublinhe-se, desde que ainda não tenha sido aberta pelo seu destinatário, já que, segundo COSTA ANDRADE, é «(…) precisamente este facto, de estar fechada, que define a fronteira da tutela penal do sigilo de correspondência e dos escritos, em geral»[41].

A correspondência terá, assim, dois níveis de tutela. Por um lado, teremos a correspondência em trânsito ou que já atingiu o seu destino, mas que ainda não foi aberta e, por outro, a correspondência já aberta, que se assume como lida e guardada pelo seu destinatário. O primeiro nível de tutela, e o mais relevante para o caso em estudo, estando a carta em trânsito ou, tendo atingido já o seu destino, não foi aberta, será direcionado para o regime de apreensão de correspondência do art. 179.º do CPP. Já no segundo caso, com a quebra da barreira física que impede o conhecimento do conteúdo da correspondência, o

[40] ALBUQUERQUE, Paulo Pinto de, *Comentário do Código de Processo Penal À Luz da Constituição da república e da Convenção Europeia dos Direitos do Homem*, 4.ª Edição Atualizada, Universidade Católica Editora, 2011, 509-510.

[41] ANDRADE, Manuel da Costa, «*Anotação ao art. 194.º (Violação de correspondência ou de telecomunicações)*», *in*: DIAS, Jorge de Figueiredo (Dir.), *Comentário Conimbricense do Código Penal*, *Parte Especial*, Tomo I – Arts. 131.º a 201.º, Coimbra Editora, 1080-1115.

"envelope" da missiva, quebra também a qualificação dessa comunicação como correspondência para o art. 179.º do CPP, sendo, portanto, equiparada a um vulgar documento e remetida para o art. 178.º, do mesmo diploma. Tal "correspondência" já não está no circuito postal, daí que outro paradigma de proteção deverá entrar em liça, no caso, será, sobretudo, a privacidade, ainda que pela mão do regime processual penal da apreensão de documentos.

O regime da correspondência, consagrado no art. 179.º do CPP, apresenta características particulares justificadas pela especificidade e importância que o serviço postal universal teve e continua, em parte, a ter, não só como meio de comunicação entre pessoas, mas também entre pessoas e entidades oficiais do Estado.

A apreensão de correspondência ocorre, nos termos do art. 179.º, n.º 1 do CPP, apenas por ordem ou autorização do juiz de instrução, «o juiz pode autorizar ou ordenar», ao invés do que sucede no regime geral das apreensões do art. 178.º do CPP, em que essa competência é responsabilidade da autoridade judiciária. Após a apreensão, «*o juiz que tiver autorizado ou ordenado a diligência é a primeira pessoa a tomar conhecimento do conteúdo da correspondência apreendida*». A apreensão da correspondência ocorre na estação de correios, devendo o Chefe de tal estação de CTT, após indicação judicial, remetê-la selada, ao juiz, que vai, depois, avaliar a relevância da comunicação, para o caso em apreço, e, caso a mesma seja efetivamente relevante,

juntá-la-á ao processo; caso contrário, a prova será restituída a quem de direito, ficando impedida de ser utilizada como meio de prova e ficando o juiz sujeito ao dever de segredo sobre o seu conteúdo.

Em casos excecionais, em que a demora na abertura da correspondência pode levar à perda de informações úteis à investigação de um crime ou não mais permitir a descoberta dos seus autores, o juiz, pode autorizar a sua abertura imediata, pelos OPC, em contexto de medidas cautelares e de polícia, nos termos do art. 252.º, n.º 2 do CPP, devendo o juiz convalidar a ordem por despacho fundamentado no prazo de 48 horas. Solução que se afigura problemática, sempre que ocorrer fora de um concreto processo penal, cujo inquérito já está em curso, por força do limite constitucional, referido no art. 34.º, n.º 4 da CRP.

Verifica-se ainda que no regime geral da apreensão, não havendo necessidade de autorização ou ordem por parte do juiz, este não tem envolvimento nesta fase do processo e cabe apenas aos OPC e ao MP o conhecimento primário do conteúdo das apreensões e a decisão sobre o que será ou não relevante para o processo em causa.

O CPP, no capítulo dos meios de obtenção da prova, encontra-se sistematizado de forma crescente, iniciando nos meios menos intrusivos dos direitos e liberdades dos cidadãos e terminando com aquele que é o mais intrusivo, as escutas telefónicas. Deparamos-mos agora com alguma incoerência sistemática, ora vejamos:

Quando é realizado uma apreensão de correspondência, e por forma a garantir a privacidade da mesma, é o juiz que toma em primeiro lugar, conhecimento do conteúdo da mesma. Quando é realizada uma escuta telefónica, esta é intercetada pelo OPC, que elabora um auto e um relatório que apresenta ao MP que por sua vez o vai apresentar ao juiz. Temos, portanto, um regime mais gravoso e mais intrusivo (as escutas telefónicas), que põe em causa a privacidade não só do visado, mas também de todos aqueles que por uma ou outra razão, entram em contacto com ele. No entanto, face ao conhecimento do conteúdo das comunicações este regime é menos restrito que o regime da apreensão de correspondência. Fará sentido? Numa perspetiva de coerência dogmática e sistemática talvez o não faça, mas parece-nos evidente que, por razões pragmáticas, não será possível ao juiz avaliar várias horas de gravações de chamadas telefónicas para determinar a sua relevância.

O conceito de mensagens de correio eletrónico apesar de comumente ligado aos serviços de webmail através do protocolo SMTP (Simple Mail Transfer Protocol) como o Google Mail ou o Outlook, que consistem na transferência, via internet, entre um sujeito emissor e um sujeito recetor, não se restringe necessariamente a estes, sendo difícil uma definição clara do que constitui exatamente uma mensagem de correio eletrónico.

O correio eletrónico, enquanto meio de comunicação, acaba por não ter uma definição consensual. Para ARMANDO VEIGA e SILVA RODRIGUES, trata-se de «um fluxo informacional e

comunicacional digital, sob o formato de texto, voz, som, informacional e comunicacional (tendencialmente) fechado, através de um ponto terminal da rede, na rede pública de comunicações eletrónicas, conduzida até ao servidor de mail ou ao terminal do destinatário de fluxo até que o mesmo proceda à sua recolha, leitura e/ou posterior eliminação»[42].

Constata-se que, o legislador nacional na Lei n.º 41/2004, de 18 de agosto – Proteção de Dados Pessoais e Privacidade nas Telecomunicações –, alterada pela Lei n.º 46/2012, de 29 de Agosto, no art. 2.º, alínea *b*), definiu o correio eletrónico como «*qualquer mensagem textual, vocal, sonora ou gráfica enviada através de uma rede pública de comunicações que possa ser armazenada na rede ou no equipamento terminal do destinatário até que este a recolha*».

Como já vimos, quer o art. 189.º, n.º 1 do CPP, quer o art. 17.º da LC, fazem alusão ao correio eletrónico. De facto, o último dos citados preceitos refere «correio eletrónico ou registos de comunicações de natureza semelhante». Vimos já, anteriormente, a dificuldade e as divergências doutrinais do que configura efetivamente o correio eletrónico, então o que será um registo de comunicação de natureza semelhante? Ora, não sendo possível sequer uma definição clara do que é o correio eletrónico como se

[42] VEIGA, Armando e RODRIGUES, Benjamim Silva, *Escutas Telefónicas. Rumo à Monitorização dos Fluxos Informacionais e Comunicacionais Digitais*, Edição de Autor (distribuída pela Coimbra Editora), 2007,p. 374

pode definir o núcleo sobre o qual iremos construir a característica de semelhança, ao nível das comunicações?

Parece claro que desta expressão só pode resultar uma compreensão abrangente do conceito de comunicações semelhantes, incluindo não só os serviços de telemóvel como SMS ou MMS, como os tão em voga, serviços de mensagens instantâneas via internet como o *Facebook Messenger* e *WhatsApp* entre outros, incluindo nesta definição de comunicações semelhantes em *lato sensu*, todas as comunicações de caráter instantâneo ou quase instantâneo que ocorrem no ciberespaço, podendo estas ser em formato de texto, imagem ou voz.

Depois de termos analisado os regimes processuais penais, relativos à obtenção da prova digital, qual será, então, o regime aplicável ao correio eletrónico e às comunicações semelhantes? A resposta, dada o pouco cuidado do legislador, afigura-se espinhosa. Na doutrina, alguns autores defendem um regime trifásico, consubstanciado nos seguintes momentos:

i) Enquanto a comunicação eletrónica está em trânsito, entre o emissor e o recetor, esta é suscetível de interceção em tempo real, podendo ser sujeita ao regime processual penal consagrado no art. 18.º, da Lei n.º 109/2009 relativo à interceção de comunicações.

ii) Quando a comunicação já atingiu o seu destinatário, mas este ainda não a abriu ou tomou conhecimento do seu conteúdo, configura uma comunicação semelhante à apreensão de

correspondência e, portanto, sujeita ao regime do art. 17.º, da Lei n.º 109/2009, relativa à apreensão de correio eletrónico e comunicações de natureza semelhante.

iii) Por fim, estando já na posse do seu destinatário e tendo sido já aberto/lido, a comunicação eletrónica perde a especialidade que o estatuto da correspondência lhe confere e, portanto, funciona como um simples dado informático suscetível de ser apreendido nos termos do art. 16.º, da Lei n.º 109/2009.

Vejamos, então, detalhadamente, os argumentos doutrinários convocados em abono de cada uma dessas visões.

4. QUAL É O REGIME APLICÁVEL AO CORREIO ELETRÓNICO E ÀS COMUNICAÇÕES SEMELHANTES?

Iremos procurar responder à pergunta *supra* formulada, expondo, de modo crítico, os posicionamentos doutrinários e jurisprudenciais que suportam cada uma das interpretações possíveis.

4.1. O problema relativamente interceção do correio eletrónico

Num primeiro momento, a comunicação eletrónica é suscetível de interceção, em tempo real, e, por isso, atento o disposto no art. 18.º, da LC, pode ser utilizada relativamente aos crimes previstos nos arts. 3.º a 8.º, do citado diploma, bem como

aos cometidos *por meio* de um sistema informático ou em relação aos quais *seja necessário* proceder à recolha de prova em suporte eletrónico, nos crimes previstos no art.187.º, do CPP. Este normativo, configura, pois, à semelhança das escutas telefónicas no CPP, o meio de obtenção da prova mais gravoso e intrusivo da esfera privada dos cidadãos. É normal portanto que o seu âmbito de aplicação se encontre reduzido, face aos restantes meios de prova da Lei n.º 109/2009, sendo apenas aplicável aos crimes elencados nas várias alíneas do n.º 1, do art.187.º do CPP, acrescendo-lhe, ainda, os crimes previstos na LC e aqueles em que tal tipo de prova digital se afigure necessária, sobretudo quando seja de outra forma impossível ou de muito difícil obtenção.

Importa, ainda, notar que o art.18.º, n.º 4, da LC, refere que é aplicável, à interceção de comunicações, o regime das escutas telefónicas, em tudo o que não contrarie o primeiro. Parece claro que este meio de obtenção da prova, por permitir aos OPC conhecer o conteúdo das comunicações eletrónicas, sem o conhecimento dos intervenientes, constitui um meio essencial e eficaz de recolha de prova digital, particularmente pelo facto de o intercetado não saber que o está a ser, funcionando como um meio oculto de investigação.

4.2. O problema do correio eletrónico recebido na "*inbox*" mas não aberto ou lido

Num segundo momento, encontramos aqueles casos em que a comunicação já atingiu a esfera de domínio do seu destinatário sem que, contudo, a mesma haja sido aberta ou lida. Como vimos, na teoria tripartida, aqui aplicar-se-ia o art. 17.º da LC, que manda aplicar, ao correio eletrónico e os registos de comunicações de natureza semelhante, o regime da correspondência do CPP que já referimos anteriormente, consagrado no art. 179.º.

Tendo em conta o que previamente vimos, relativamente à correspondência aberta, poder-se-á restringir a aplicação do art. 17.º, da Lei n.º 109/2009, às mensagens de correio eletrónico e aos registos de comunicação semelhante não abertos/lidos pelos seus destinatários? Em abstrato afigura-se possível, mas será mesmo assim?

A característica essencial do conceito de correspondência tradicional, no qual se baseia o CPP, é o facto de ser uma comunicação fechada. É o ato de colocar uma comunicação num recipiente (envelope) fechado e selado que lhe confere o estatuto de correspondência. Ora, existem dúvidas se este elemento pode ser transferido para ao âmbito das comunicações eletrónicas. Não sendo uma coisa física, palpável, não será suscetível de ser colocada num envelope nem tão pouco se pode considerar a limitação ao acesso do conteúdo por uma *password* ou código de acesso como um "envelope" da mesma.

4.3. O correio eletrónico já aberto

Chegamos, agora, a um terceiro momento, reportando-nos aos casos em que a comunicação eletrónica já atingiu a esfera de controlo do seu destinatário e já foi aberta/lida.

SANTOS CABRAL defende que «a mensagem eletrónica mantida em suporte digital depois de recebida, e lida, terá a mesma proteção da carta da carta em papel que tenha sido recebida pelo correio e que foi aberta e guardada em arquivo pessoal (…) São um mero documento escrito pelo que tais mensagens não gozam da aplicação do regime de proteção da reserva da correspondência e telecomunicações» [43]. No mesmo sentido, COSTA ANDRADE e RITA CASTANHEIRA NEVES, defendem que, após a receção e leitura da comunicação eletrónica pelo seu destinatário cessa a comunicação, sendo agora, em semelhança com o regime da apreensão de correspondência do CPP, um simples dado informático e, portanto, suscetível de ser apreendido nos termos do art. 16.º, da Lei do Cibercrime.

Importa sublinhar que, já antes da promulgação da lei, PEDRO VERDELHO, referindo-se às mensagens não lidas/não recebidas e às recebidas e abertas, «às primeiras parece fácil dar, analogicamente o mesmo tratamento físico, dito tradicional, contido em envelopes ainda não abertas. Quanto às segundas, é de admitir a possibilidade de se considerarem como meros

[43] CABRAL, SANTOS, José António Henriques dos *et al.*, in *Código de Processo Penal Comentado*, 2.ª Edição Revista, Livraria Almedina, 2016: 707

documentos armazenados num computador, com o mesmo estatuto de uma carta recebida e guardada num arquivo pessoal ou de texto escrito e guardado em suporte digital»[44].

4.4. Quantos momentos e quantos regimes para o correio eletrónico?

Parece-nos que o primeiro momento configurará sempre a interceção em tempo real, suscetível de ser intercetada nos termos do art. 18.º, da Lei do Cibercrime e nas condições anteriormente descritas.

Quanto ao segundo momento, surgem-nos algumas dúvidas. Todas estas características que referimos anteriormente, colocam problemas quando chega a altura de avaliar se o recetor da comunicação já tomou conhecimento real do conteúdo da mesma, não havendo o ato material de rasgar ou abrir o envelope não há qualquer prova clara se o conteúdo da mesma foi acedido ou não, a não ser nos casos em que é enviado um pedido de receção e este não é descartado, pelo recetor. Veja-se, por exemplo, os casos dos correios eletrónicos por *webmail*, como o "*Google Mail*" ou o "*Outlook*", em que se afigura possível, abrir e tomar conhecimento do conteúdo da mensagem e, através de uma função do próprio serviço, continuar a assinalar a mensagem como não lida.

[44] VERDELHO, Pedro, «*A obtenção de prova no ambiente digital*», p.124

O sentido de aplicação do art. 179.º, do CPP, não é, certamente, o de considerar esta mensagem como correspondência em detrimento de outras. Um outro caso relevante, é o que ocorre com os *smartphones*, quando é recebida uma mensagem instantânea ou um *e-mail*, pode surgir uma notificação onde se pode ler o conteúdo da mensagem sem, no entanto, o dispositivo considerar a mensagem como lida, ou até serviços que permitem considerar mensagens como lidas sem sequer serem abertas pelo seu destinatário. Além disso, enquanto a carta é apenas uma coisa física e única, com as comunicações eletrónicas existe a possibilidade de a mensagem estar presente, simultaneamente, em vários sistemas informáticos.

A questão não se colocará se o recetor, após a leitura da comunicação eletrónica, a guardar no dispositivo ou de outra forma, disponha dela, criando um novo documento, não sendo estes ficheiros merecedores de uma tutela especial pela sua proveniência, sendo por isso equiparado, nos termos do art. 16.º, da LC, à apreensão de dados informáticos.

Apesar de nos parecer que a distinção entre correio eletrónico, fechado e aberto, se afigura a solução que mais vai ao encontro do espírito do legislador, parece-nos, contudo, desadequada, tendo em conta o tipo de comunicação que pretende abarcar, não sendo possível determinar, com certeza, se a mensagem já foi ou não aberta pelo seu destinatário. O legislador, mesmo em 2009 e antes da chegada da era dos "smartphones", deveria ter previsto que um regime tão específico como o regime da apreensão de

correspondência não teria capacidade para acompanhar a curto prazo, a evolução da tecnologia e da comunicação.

Uma distinção entre comunicação eletrónica aberta e fechada não poderá, por tudo o que foi dito até aqui, ser transposta para a problemática das comunicações eletrónicas, por força das lacunas, arbitrariedade e possibilidade de manipulação que dela podem advir.

Não sendo possível uma distinção entre comunicação aberta e fechada ou lida e não lida, deverá existir outra solução para diferenciar entre tipos de comunicação?

Uma questão a considerar, será saber se, tendo em conta a instantaneidade, acesso fácil e imediato a sistemas como os telemóveis, os computadores e os "*smartphones*", se poderá defender o entendimento segundo o qual, pelo simples facto de já estarem à disposição do recetor, se pode considerar que, a partir desse momento, o seu conteúdo já foi acedido pelo utilizador?

SANTOS CABRAL defende que «a mensagem recebida em telemóvel, atenta à natureza e finalidade do aparelho e o seu porte pelo arguido no momento da revista, é de presumir que, uma vez recebida, foi lida pelo seu destinatário» [45]. A questão que se coloca é a de saber se tal entendimento pode ter um mínimo de expressão no âmbito de proteção da norma.

Não existindo qualquer obrigação legal de tomar conhecimento do conteúdo das comunicações, não nos parece que

[45] GASPAR, António Henriques *et al. In Código de Processo Penal Comentado*, 2.ª Edição Revista, Livraria Almedina, 2016: 707.

o simples facto de o conteúdo estar acessível ao sujeito se possa considerar como uma "abertura do envelope", não se protegendo realmente a inviolabilidade e privacidade das comunicações que apesar de recebidas ainda não foram lidas pelos seus destinatários. Além disso, uma adaptação do regime da apreensão da correspondência, provocaria uma total ou quase total, irrelevância do regime, permitindo que todas as comunicações que atingiram o seu destino, se transformassem em simples dados informáticos, razão pela qual esta interpretação, não colhe razoabilidade, criticando-se o entendimento de SANTOS CABRAL, relativamente à sua exposição sobre o regime de obtenção da prova digital, no contexto da mensagem recebida em telemóvel.

Desta teoria poderia ainda surgir a questão de saber em que momento exato se pode considerar que as comunicações se encontram à disposição do recetor. Todavia, tendo em conta a excessiva tecnicidade da discussão e a pouca relevância prática do assunto, abster-nos-emos de considerações a esse respeito.

Um outro entendimento possível será uma aplicação total do regime da correspondência, a todas as comunicações de correio eletrónico e registos de comunicação semelhante. Este entendimento confere uma proteção superior a todas as comunicações eletrónicas, mas fere quando comparado com o regime tradicional da apreensão da correspondência. Faz sentido que uma carta aberta, à qual não se aplica o regime da apreensão de correspondência, tenha menor proteção que uma qualquer mensagem instantânea?

Não é claro se a intenção do legislador foi a de conferir, a todas as comunicações, no ciberespaço, uma proteção superior, fazendo uso do regime da correspondência; ou, se pelo contrário, a sua intenção era continuar a fazer uma distinção entre comunicações abertas e fechadas, tendo com leviandade ignorado as especificidades das comunicações eletrónicas.

Desde logo, afigura-se-nos que o legislador cometeu um erro, *ad initium*, ao aplicar nas comunicações eletrónicas o regime da correspondência. Como vimos anteriormente as mensagens de correio eletrónico, e registos de natureza semelhante, ocorrem num muito curto espaço de tempo e sem intermediários além da plataforma utilizada, em clara e manifesta diferença da correspondência tradicional onde o espaço temporal é bastante mais longo e podendo passar por largo número de intermediários entre o emissor e o destinatário. Além disso, as comunicações eletrónicas não são passíveis de ser fechadas, pelo menos no sentido tradicional, e, portanto, muito dificilmente poderemos ter situações análogas à correspondência recebida e não lida.

Tendo em conta o regime atual, na nossa modesta opinião a aplicação do regime de correspondência, terá que ser feito, de maneira geral, a toda a comunicação eletrónica, reduzindo assim o correio eletrónico a apenas dois regimes. Não encontrando uma circunscrição tecnicamente prática e que proteja a *ratio legis* da norma, a opção será recorrer à solução que mais protege o sujeito individual. A aplicação do regime da correspondência de forma indiscriminada a toda a comunicação eletrónica que tenha

atingido a esfera de domínio do recetor, não diferenciando a comunicação lida da comunicação não lidas.

Segundo DAVID SILVA RAMALHO[46] «com a criação do art. 17º da Lei do Cibercrime, o legislador tornou clara a sua intenção de submeter toda a apreensão do correio eletrónico e registos de comunicações de natureza semelhante ao regime de apreensão de correspondência, independentemente de as mensagens se encontrarem lidas ou não lidas». Resultando, portanto, nas palavras das Juízas-Desembargadoras da 3.ª Secção Criminal do TRL[47] «a atribuição de uma tutela acrescida à mensagem em formato digital, submetendo a sua apreensão sempre aos requisitos da apreensão da correspondência, em nome, desde logo da privacidade e da autodeterminação informacional».

Na jurisprudência, encontra-se ainda outro critério que defende a ideia de que o legislador não pretendeu fazer distinção entre as comunicações abertas/lidas ou fechadas, defendendo que a expressão «armazenados nesse sistema informático», do art. 17.º da LC, pressupõe, desde logo, um ato proativo do recipiente da comunicação que a armazena, pelo que «recorrendo ao argumento literal somos levados a concluir que o legislador não quis fazer distinção entre correio armazenado e correio não armazenado»[48].

---

[46] RAMALHO, David Silva, *Métodos Ocultos de investigação Criminal em Ambiente Digital*, Livraria Almedina, Coimbra, 2017, p.278

[47] Acórdão do TRL de 11/07/2019 da relatora Juíza-Desembargadora CONCEIÇÃO GONÇALVES.

[48] Acórdão do TRL de 11/07/2019 da relatora Juíza-Desembargadora CONCEIÇÃO GONÇALVES.

4.5. A questão do conhecimento

Decorre, diretamente, do art. 179.º, n.º 3 do CPP, que o juiz será a primeira pessoa a tomar conhecimento do conteúdo da correspondência. Verifica-se que tal regime se aplica às comunicações eletrónicas, nos termos do art. 17.º, da Lei do cibercrime.

No caso de uma busca a um sistema informático será legítimo dizer que os OPC não poderiam ter qualquer tipo de acesso ao conteúdo das comunicações? Não parecerá tal um pouco irrealista e não consentâneo com as concretas necessidades da investigação criminal?

Identificando algum tipo de comunicação eletrónica, os OPC deveriam remeter todas as comunicações, em bloco, para o juiz de instrução a quem competiria decidir individualmente sobre a relevância de cada comunicação para a investigação em causa.

DUARTE RODRIGUES NUNES defende que a extensão do art. 252.º, n.º 2 do CPP, que permite ao MP abrir encomendas ou valores fechados em casos excecionais, não está prevista para qualquer forma de correspondência, «mas apenas para encomendas e valores fechados, sendo que, no âmbito correio eletrónico e dos registos de comunicação semelhantes, inexiste qualquer modalidade que possa ser equiparada a tais realidades, mas tão-só a cartas, telegramas ou realidades análogas»[49]. Parece

[49] NUNES, Duarte Rodrigues, «*Algumas reflexões em matéria apreensão de correio eletrónico e registos de comunicação de natureza semelhante*», CYBERLAW *by* CIJIC, Edição N.º VI – setembro/outubro 2018: 35-36

claro que a expressão «*tratando-se de encomendas ou valores fechados suscetíveis de serem apreendidos*», pretende fazer uma distinção e restringir a possibilidade de abertura das mesmas pelo MP, no entanto por razões análogas esta é estendida a cartas e outras formas de comunicação tradicional.

Não nos parece que a intenção do legislador, ao aplicar o regime da correspondência, fosse negar o acesso a este instituto excecional nas comunicações eletrónicas, mas tendo em conta a letra da lei e a distinção criada pelo vocábulo «tratando-se», este regime não nos parece aplicável às comunicações eletrónicas. O que significa que estamos perante mais uma das várias incoerências da aplicação da apreensão de correspondência às comunicações eletrónicas.

Não sendo, portanto, aplicável às comunicações eletrónicas as exceções, que permitem aos OPC ser os primeiros a conhecer do conteúdo da correspondência, sendo imperativamente o juiz o primeiro a conhecer o conteúdo das comunicações eletrónicas.

Outra posição, sufragada em grande parte por magistrados do MP, defende que os OPC devem fazer uma primeira leitura do conteúdo das comunicações selecionando as comunicações que seriam de interesse para o caso em apreço, remetendo depois apenas essas comunicações para o JIC, que decidiria pela sua apreensão ou não. Neste sentido, transcrevemos aqui o essencial da posição defendida por RUI CARDOSO, Procurador da República, que refere o seguinte:

«A interpretação conjugada do art. 17.º da LCC e do art. 179.º do CPP no sentido de aí fundar uma norma com o sentido de que é o juiz de instrução que, no inquérito, em primeiro lugar toma conhecimento das mensagens de correio eletrónico ou semelhantes e que é ele que, oficiosamente, procede à seleção daquelas que são de grande interesse para a descoberta da verdade ou para a prova, para além de não se traduzir em qualquer real garantia, viola a estrutura acusatória do processo, pois essa é matéria essencial à direção do inquérito e à definição do seu objeto, assim comprometendo a posição de imparcial juiz das liberdades. O juiz de instrução não pode ter qualquer "influência" ou "manipulação" sobre a definição do objeto do inquérito; deve ser alheio à definição da estratégia de investigação do MP e OPC (...). Exigir que seja o juiz, oficiosamente a selecionar as mensagens relevantes é tão fundamentado como seria exigir que o MP apresentasse ao juiz de instrução uma lista de casas onde, em abstrato, pudessem existir objetos relacionados com um crime ou que pudessem servir de prova, ou uma lista de pessoas que, em abstrato, pudessem ter conhecimento dos factos, e ser o juiz de instrução a ordenar em quais dessas casas se fariam buscas e quais dessas pessoas seriam inquiridas como testemunhas, a realizar tais diligências e a apresentar depois ao MP os resultados que considerasse relevantes para a prova».

Destaca-se do excerto transcrito, a crítica ao facto de dever ser o juiz o primeiro tomar conhecimento do conteúdo das comunicações eletrónicas apreendidas, visto que, na sua opinião,

ao ser o Juiz a definir o que é relevante para o processo, põe-se em causa a estrutura acusatória do processo e a idoneidade do Juiz.

No mesmo sentido, já se escreveu, no acórdão do TRG, que «não poderá nunca haver mensagens de correio eletrónico apreendidas para serem utilizadas como prova num determinando processo sem que haja um despacho de um juiz nesse sentido»[50], defendendo, contudo, nem sempre ser exigível a existência de uma prévia decisão judicial para a respetiva apreensão, que pode revestir a natureza provisória, quando surgida no decurso de uma pesquisa realizada com a autorização do MP.

Além das críticas formuladas por RUI CARDOSO, poderíamos aduzir uma outra de cariz prático, visto que, se o juiz é o primeiro a tomar conhecimento do conteúdo das comunicações eletrónicas, caber-lhe-á abrir e analisar todas as comunicações apreendidas.

É manifesta, a inadequação da aplicação do regime da correspondência às comunicações eletrónicas. A correspondência tradicional pelas suas características, pelo seu custo e por ser possível determinar a sua abertura pela quebra do recetáculo, faria com que o número de correspondências que o juiz teria de analisar seria relativamente reduzido. As comunicações eletrónicas pela sua facilidade de emissão e receção instantânea, pelo seu custo

[50] Acórdão do TRG de 29/03/2011 da relatora Juíza-Desembargadora MARIA JOSÉ NOGUEIRA.

nulo e pelas suas características intrínsecas, resultam num número mais elevado de comunicações a serem analisadas individualmente.

Uma outra questão ou dificuldade, resultará de saber se o juiz, sobrecarregado por um elevado número de comunicações eletrónicas, não acabará por, de forma ligeira, ao avaliar a relevância das comunicações, optar por uma excessiva restrição ou uma excessiva abertura das comunicações. No entanto, parece-nos que a chamada "pré-apreensão" não vai de encontro ao postulado no art. 179.º, n.º 3, devendo «*O juiz que tiver autorizado ou ordenado a diligência é a primeira pessoa a tomar conhecimento do conteúdo da correspondência apreendida*» e, além disso, ao permitir aos OPC aceder de forma indiscriminada às comunicações, acaba-se por se cair na violação do princípio da proibição de excesso e afrontar o paradigma legal e constitucional, ponderado e codificado, de proibição de ingerência na correspondência e nas comunicações privadas.

Coloca-se a questão de saber, se o regime das escutas telefónicas (regime de *última ratio*, dada a alta danosidade social que envolve a vida dos cidadãos) permite o conhecimento do conteúdo das mesmas pelos OPC e do MP, não faria sentido aplicar um sistema semelhante às comunicações eletrónicas? A questão não é clara, pois se o regime das escutas telefónicas é menos restritivo face ao conhecimento do conteúdo, os seus pressupostos de aplicação são também mais restritos, ou seja, os OPC e os MP vão ter conhecimento do conteúdo, mas será sempre

nos crimes de catálogo do art. 187.º ou, nos casos de interceção de comunicações eletrónicas, nos crimes previstos no art. 18.º, da Lei n.º 109/2009.

4.6. Perspetivas "de iure condendo"

Parece-nos claro que o estado atual da prova digital em Portugal e, particularmente, da apreensão de correio eletrónico e comunicações de natureza semelhante não é o mais coerente.

Quanto aos OPC, o seu trabalho afigura-se complexo, atento o regime restritivo de acesso ao correio eletrónico, mediatizado pelo JIC. Podem fazer uma pré-apreensão e remeter aos juízes apenas as comunicações relevantes para o caso, como é a posição defendida pelo MP, apesar de ser contra o postulado no regime da apreensão de correspondência? Ou devem seguir a lei de forma clara e, detetando algum tipo de comunicação, remeter todas estas seladas e invioladas para apreciação do JIC? A resposta parece clara, sob pena de entrarmos em proibição de prova, a cair sob a alçada do art. 32.º, n.º 8, da CRP, e arts. 126.º, nº 3, e 167.º, do CPP.

Quanto aos Tribunais e particularmente, os JIC veem-se numa situação frágil. A lei é clara, o JIC é o primeiro a tomar conhecimento do conteúdo das comunicações eletrónicas apreendidas. No entanto, em casos de grande volume e complexidade em que sejam apreendidos grandes sistemas informáticos, o número de comunicações pode ascender facilmente às milhares e às centenas de milhares, resultando numa

decisão excessivamente demorada que poderá pôr em causa uma decisão célere e em tempo útil.

Por fim, os cidadãos, que podem ser alvo de uma ação de apreensão de comunicações eletrónicas, veem a sua situação envolvida numa névoa de incerteza, não sendo possível a um leigo descortinar facilmente qual a lei aplicável e quais as suas condições resultando numa incerteza jurídica que em nada contribui para o bom funcionamento do estado de direito.

Parece-nos, portanto, que o futuro dos meios de prova digital poderá passar em primeiro lugar pela clarificação do regime a aplicar. E em que consistirá esta clarificação?

Em primeiro lugar parece-nos que o art. 189.º, nos termos em que existe hoje, já não faz qualquer sentido. No nosso entendimento, o art. 189.º, do CPP, esgota o seu sentido quanto às comunicações por meio diferente do telemóvel e guardadas em suporte digital, pois esse tipo de comunicações já se encontram reguladas num regime autónomo, sendo portanto no nosso entendimento essencial para a clarificação dos regimes, a redução do art. 189.º, apenas à interceção de comunicação entre presentes, devendo o previsto no art. 2.º ser também remetido para um regime especial.

Quanto aos meios de obtenção da prova em si, previstos atualmente na Lei n.º 109/2009, reconhecemos a sua importância, principalmente face às pressões comunitárias para as adotar, sem, no entanto, esta se encontrar imune às nossas críticas.

A previsão de vários meios de prova numa lei especial faz sentido, quando aquelas medidas se aplicarem exclusivamente ou quase exclusivamente à temática em causa.

Ora, como foi referido anteriormente, este não é o caso das medidas processuais da lei 109/2009, com o âmbito quase universal que estas possuem. Por razões orgânicas, faria todo o sentido que estas fossem inseridas no capítulo que respeita aos meios de prova no processo penal português.

Já quanto à apreensão de correio eletrónico e de comunicações de natureza semelhante, por tudo o que foi exposto anteriormente, não faz sentido a sua remissão para o regime da apreensão da correspondência sendo, por isso, essencial, no nosso entendimento, a previsão de um regime integral e com as devidas especificidades técnicas para a apreensão de correio eletrónico e comunicações semelhantes, dotando os OPC dos meios necessários para combater a criminalidade, garantindo no entanto o mínimo de agressão aos direitos essenciais dos cidadãos.

A luta entre o direito à privacidade e a necessidade de uma Estado capaz de responder à criminalidade, mais não constitui do que, uma representação da dicotomia, privacidade versus segurança.

Entendemos que o futuro, e como sugerido por RUI CARDOSO[51] ou SILVA RODRIGUES[52], passará pela criação de

[51] RMP, n.º 153, janeiro-março, 2018.

[52] Este autor defende a criação uniforme de obtenção de prova eletrónico-digital. RODRIGUES, Benjamin Silva, "*Das Escutas Telefónicas*», Tomo II, em 2008 (1.ª Edição), 543-564

um regime autónomo e autossuficiente com competências partilhadas entre o MP e o Juiz de Instrução adequado ás especificidades técnicas das comunicações eletrónicas, de forma a garantir por um lado a capacidade aos OPC e ao MP de fazer face a uma criminalidade cada vez mais técnica e complexa sem no entanto por em causa um valor fundamental de uma estado democrático e de direito no que concerne à privacidade.

4.7. Síntese conclusiva

Sucessivamente, desde a Lei n.º 109/91 (Criminalidade Informática), às várias alterações do CPP (Reformas de 1998 e 2007) e ao surgimento da Lei n.º 109/2009, o legislador coibiu-se de criar um regime autónomo e que, respeitando simultaneamente as necessidades técnicas e sociais de investigação criminal garantisse a preservação e proteção dos direitos fundamentais dos cidadãos.

A conservação de três regimes relativos à prova digital – no CPP, nas Leis n. os 32/2008 e 109/2009, provocou o caos e desordem no ordenamento jurídico.

A manutenção da extensão do art. 189.º, relativamente às conversações ou comunicações transmitidas por qualquer meio técnico diferente do telefone, que foi criticado mesmo na sua génese em 1987, mantêm-se ainda hoje em vigor criando uma confusão desnecessária aos OPC, ao sistema judicial e aos próprios cidadãos.

A Lei n.º 109/2009 surge, atualmente, como o principal normativo na temática da prova digital e particularmente, ao nível da comunicação eletrónica, seja ela através de correio eletrónico ou outro tipo de comunicação seja ela, escrita, por voz, por imagem o vídeo.

Ao nível das comunicações, apresenta especial relevância o art. 17.º, que visa a apreensão de correio eletrónico e registos de comunicações de natureza semelhante. Este artigo, que nos remete para o regime da apreensão de correspondência, previsto no art. 179.º, do CPP, acaba por transferir a temática da apreensão de comunicações eletrónicas para o âmbito tradicional da correspondência com tudo o que isso acarreta.

A aplicação de conceitos da correspondência tradicional à correspondência eletrónica vai colidir diretamente com as próprias características do correio eletrónico e das comunicações eletrónicas, particularmente na questão de determinar se o recetor já tomou conhecimento da comunicação e provocando o caos ao exigir ao JIC, a análise de toda e qualquer comunicação apreendida, sob pena de nulidade.

Por tudo quanto expressamos, afigura-se-nos que o regime da correspondência é manifestamente inadequado às exigências e características das comunicações eletrónicas. O futuro da prova digital não poderá deixar de passar, na nossa humilde opinião, pela criação de um regime específico que respeite os direitos fundamentais dos cidadãos, mas garantindo aos OPC, às autoridades judiciárias e aos tribunais a capacidade para combater

o cibercrime e a garantia dos meios adequados para a recolha de prova eletrónico-digital.

BIBLIOGRAFIA

– ALBUQUERQUE, Paulo Pinto de, *Comentário do Código de Processo Penal À Luz da Constituição da república e da Convenção Europeia dos Direitos do Homem*, 4.ª Edição Atualizada, Universidade Católica Editora, Lisboa, 2011: (1-1712).

– AMADOR, Nelson José Roque, "Cibercrime em Portugal: Trajetórias e Perspetivas de Futuro" disponível em https://comum.rcaap.pt/, consultado a 1 de abril de 2020;

– AGUIAR, Tiago Leonel Dos Santos, "O correio eletrónico, a apreensão e interceção no processo penal português, Dissertação apresentada à Faculdade de Direito da Universidade de Coimbra no âmbito do 2.º Ciclo de Estudos em Direito (, na Área de Especialização em Ciências Jurídico – Criminais sob orientação do Dr. Nuno Brandão;

– ALMEIDA, Ivo Filipe De *"a prova digital*", Dissertação de mestrado em ciências jurídicas sob orientação do Dr. Rui Manuel de Freitas Rangel;

–ANDRADE, Manuel da Costa, «*Anotação ao art. 194.º (Violação de correspondência ou de telecomunicações)*», *in*: DIAS, Jorge de Figueiredo (Direção), *Comentário Conimbricense do Código Penal*, *Parte Especial*, Tomo I – Arts. 131.º a 201.º, Coimbra Editora, Coimbra, (1-1272): [1080-1115].

– ANDRADE, Manuel Da Costa, *Bruscamente no verão passado, a Reforma do Código de Processo Penal-Observação*

críticas sobre uma lei que podia e devia ter sido diferente, Coimbra Editora, 2009.

– ANDRADE, Manuel da Costa, *Sobre as proibições de Prova em Processo Penal*, Reimpressão, Coimbra Editora, Coimbra, 2006: (1-344).

– BRAVO, Jorge dos Reis/LEAL, Celso, *Prova Genética: Implicações em Processo Penal*, Universidade Católica Editora, Lisboa, 2018: (1-451).

– CANCELA, Alberto Gil Lima, "*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 sob orientação da Professora Doutora Sónia Mariza Florêncio Fidalgo;

– CARDOSO, Rui*," apreensão de correio eletrónico e registos de comunicações de natureza semelhante – artigo 17.º da lei n.º 109/2009 de 15 de setembro"*, publicado na Revista do Ministério Público n.º 153 (janeiro-março de 2018);

– CORREIA, João Conde, «*Prova digital: as leis que temos e a lei que devíamos ter*», RMP, N.º139, julho/setembro 2014: [29-59], acedida e consultada, em 2020-05-02, na URL: <http://rmp.smmp.pt/wp-content/uploads/2014/04/3_RMP_139_Joao_Correia.pdf>.

– COSTA, José de Faria, «*As telecomunicações e a privacidade: o olhar (in)discreto de um penalista*», *in*: As

telecomunicações e o direito na sociedade da informação, Actas do Colóquio organizado pelo IJC em 23 e 24 de Abril de 1998, IJC, Coimbra, 1999: [49 e segs.]: 76-77.

– COSTA, José Francisco de Faria, «*As telecomunicações e a privacidade: o olhar (in)discreto de um penalista*», *in*: *Direito Penal da Comunicação, Alguns Escritos*, Coimbra Editora, Coimbra, 1998: (1-182): [143-177].

– COSTA, José Francisco de Faria, *Direito Penal da Comunicação, Alguns Escritos*, Coimbra Editora, Coimbra, 1998: (1-182).

– FREITAS, José Pedro Coutinho Barreiros De*," Os Meios de Obtenção de Prova Digital na Investigação Criminal: o Regime Jurídico dos Serviços de Correio Eletrónico e de Mensagens Curtas*", Dissertação de Mestrado em Direito e Informática, sob a orientação do Dr. Alexandre Júlio Teixeira Santos Dr. Pedro Miguel Fernandes Freitas.

– GASPAR, António Henriques/CABRAL, SANTOS, José António Henriques dos/COSTA, Eduardo Maia/MENDES, António Jorge de Oliveira/MADEIRA, António Pereira/GRAÇA, António Pires Henriques da, *Código de Processo Penal Comentado*, 2.ª Edição Revista, Livraria Almedina, Coimbra, 2016: (1-1704).

– GASPAR, António Henriques; CABRAL, José António Henriques Dos Santos; COSTA, Eduardo Maia; MENDES, António Jorge De Oliveira; MADEIRA, António Pereira;

GRAÇA, António Pires Henrique da "Código *de Processo Penal Comentado"* 2º edição revista;

– GONÇALVES, João Gama, "*a prova digital em 2017 – reflexões sobre algumas insuficiências processuais e dificuldades da investigação*";

– 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 de Mestrado apresentada à Universidade Católica Portuguesa para obtenção de grau de Mestre, sob orientação do Professor Doutor Henrique Salinas;

– MESQUITA, Paulo Dá, *"Processo Penal, Prova e Sistema Judiciário*", Coimbra Editora, 2010;

– MONTEIRO, Vera L. Azevedo, "*os meios de obtenção de prova no ambiente digital: o correio eletrónico*", Dissertação de Mestrado na área de Direito Criminal apresentada à Universidade Católica Portuguesa, sob orientação do Professor Doutor José Manuel Damião da Cunha – NEVES, Rita Castanheira, *"As Ingerências nas Comunicações Eletrónicas em Processo Penal – Natureza e respetivo regime jurídico do correio eletrónico enquanto meio de obtenção de prova"*, Coimbra; Coimbra Editora, 2011;

– NUNES, Duarte Rodrigues, «*Algumas reflexões em matéria apreensão de correio eletrónico e registos de comunicação de natureza semelhante*», CYBERLAW *by* CIJIC, Edição N.º VI – setembro/outubro 2018.

– PRATAS, Rita Maria Coelho Salvado, "*O correio eletrónico como meio de prova em processo penal*", Dissertação de Mestrado orientada pelo Senhor Professor Doutor Germano Marques da Silva;

– RAMALHO, David Silva, *Métodos Ocultos de investigação Criminal em Ambiente Digital*, Livraria Almedina, Coimbra, 2017: (1-378).

– RODRIGUES, Benjamim Silva Rodrigues, *Da Prova Penal*, Tomo IV – *Da Prova Eletrónico-Digital e da Criminalidade Informático-Digital (Contributo para a Fundamentação de um Modelo Dinâmico-Reversivo de Ciência Forense Digital em sede de Investigação da Cyber-Criminalidade Informático-Digital e à Luz do Novíssimo Regime da Lei do Cibercrime Portuguesa)*, 1.ª Edição, Prefácio de D.ra CATARINA DOS SANTOS GOMES, Rei dos Livros, Lisboa, 2011: (1-616).

– RODRIGUES, Benjamim Silva, 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*, Prefácio da D.ra SARA ANTUNES, Edição de Autor, Distribuição: Coimbra Editora, Coimbra, 2009: (1-839).

– RODRIGUES, Benjamim Silva, *Das Escutas Telefónicas à Obtenção da Prova [Em Ambiente] Digital, Tomo II, A Monitorização dos Fluxos Informacionais e Comunicacionais*, Prefácio da D.ra CATARINA DOS SANTOS GOMES, 2.ª Edição

Revista, Atualizada e Aumentada, Edição de Autor, Distribuição: Coimbra Editora, Coimbra, 2009: (1-650).

– RODRIGUES, Benjamim Silva, *Criminologia Forense (Forensic Criminology),* Tomo I – *O nascimento e a autonomia dogmático-científica da Criminologia Forense face à "Enciclopédia das Ciências Criminais" e à "Ciência Conjunta do Direito Penal*", *O Criminólogo Forense e o Método ideográfico-nomotético, semiótico, dinâmico-reversivo e teleológico-funcional e racionalmente orientado de investigação Criminal*, Rei dos Livros/Empório do Direito, São Paulo/Lisboa, 2015: (1-325).

– RODRIGUES, Benjamim Silva, *Da Prova Penal*, Tomo VI, *Novos Métodos "Científicos" de Investigação Criminal nas Fronteiras das nossas Crenças (A "Psicografia", a "Grafologia" e a "Ergonomia" Forense, a "Perícia à Voz Humana", em Contexto de Escutas Telefónicas e "Captações e Gravações Áudio em Voz-Off, e o "Testing"...) [Contributo Para a Identificação do Paradigma Constitucional e Legalmente Poderado e Codificado em Matéria de Entrada, Ex vi "Cláusula Aberta" do Art. 125.º, do CPP, de Novos Métodos "Científicos" de Investigação Criminal)], Nos Vinte Anotes do Desaparecimento do Professor Doutor EDUARDO CORREIA, In Memoriam*, Com Prefácio da D.ra CAROLINA ANDRADE DA SILVA RODRIGUES CORREIA, Rei dos Livros, Lisboa, 2011: (1-604).

– VEIGA, Armando e RODRIGUES, Benjamim Silva, *Escutas Telefónicas. Rumo à Monitorização dos Fluxos Informacionais e Comunicacionais Digitais*, Edição de Autor (distribuída pela Coimbra Editora), Coimbra, 2007.

– VENÂNCIO, Pedro Dias, «*Breve introdução da questão da investigação e meios de prova na criminalidade informática*», Verbojurídico, Dezembro de 2006: (1-34), acedido e consultado, em 205-05-05, na URL: <https://www.verbojuridico.net/doutrina/tecnologia/meiosprovacriminalidadeinformatica.pdf>.

– Centro de Estudos Judiciários (CEJ), "Cibercriminalidade e Prova Digital", Coleção Formação Continua, julho 2018, disponível em http://www.cej.mj.pt/cej/recursos/ebooks/penal/eb_Ciber_PDigital2018.pdf , consultado a 27 de Abril de 2020;

– Relatório de atividade do Gabinete do Cibercrime, Set.2015 a Dez.2016, disponível em http://www.ministeriopublico.pt/sites/default/files/documentos/pdf/relatorio_anual_gabinete_cibercrime2015_02-03-2017.pdf, consultado a 15 de Fevereiro de 2020;

– Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, disponível em https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf, consultado a 27 de Abril de 2020;

– MILITÃO, Renato Lopes, "A propósito da prova digital no processo penal", disponível em https://www.oa.pt/upl/%7B53f46e96-536f-47bc-919d-525a494e9618%7D.pdf, consultado a 15 de Janeiro de 2020;

– NUNES, Duarte Rodrigues, in "algumas reflexões em matéria apreensão de correio eletrónico e registos de comunicação de natureza semelhante", CYBERLAW by CIJIC, Edição nºVI – setembro/outubro 2018, disponível em http://www.cijic.org/publicacao/ , consultado a 20 de Abril de 2020;

JURISPRUDÊNCIA CONSULTADA

– Acórdão do Tribunal da Relação de Lisboa, processo nº 1286/14.9IDLSB-A. l1-5 de 04/02/2020 do relator, Juiz-Desembargador LUÍS GOMINHO;

– Acórdão do Tribunal da Relação de Guimarães, processo nº 735/10.0GAPTL – A.G1 de 29/03/2011 da relatora, Juíza-Desembargadora MARIA JOSÉ NOGUEIRA;

– Acórdão do Tribunal da Relação de Lisboa, processo nº 744/09-1S5LSB-A. L1-9 de 29/03/2012 do relator, Juiz-Desembargador JOÃO CARROLA;

– Acórdão do Tribunal da Relação do Porto, processo nº 896/07.5JAPRT.P1 de 27/01/2010 do relator, Juiz-Desembargador ARTUR VARGUES;

– Acórdão do Tribunal da Relação de Guimarães, processo nº 639/08.6GBFLG.G1 de 15/10/2012 do relator, Juiz-Desembargador FERNANDO MONTERROSO;

– Acórdão do Tribunal da Relação de Évora, processo nº 133/13.3YREVR de 18/10/2011 do relator, Juiz-Desembargador FERNANDO RIBEIRO CARDOSO;

– Acórdão do Tribunal da Relação de Lisboa, processo nº 1246/08.9TASNT.L1-5 de 20/12/2011 do relator, Juiz-Desembargador AGOSTINHO TORRES