UNIVERSIDADE EDUARDO MONDLANE

Faculdade de Direito

Dissertação de Mestrado

A PROBLEMÁTICA DAS ESCUTAS TELEFÓNICAS E DA PROVA DIGITAL COMO MEIOS DE OBTENÇÃO DE PROVA: UMA ANÁLISE COMPARADA (MOÇAMBIQUE, PORTUGAL E BRASIL)

Autora: Zvika Costino Maniquidzua Cossa

Maputo, Março de 2026

A problemática das escutas telefônicas e da prova digital como meios de obtenção de prova: uma análise comparada (Moçambique, Portugal e Brasil)

Dissertação apresentada em cumprimento parcial dos requisistos exigidos para a obtenção do grau de Mestre em Ciências Jurídicas na Universidade Eduardo Mondlane

Autora: Zvika Costino Maniquidzua Cossa
Orientador: Professor Doutor Manuel Castiano

Maputo, Março de 2026

Declaração de Honra

Eu, Zvika Costino Maniquidzua Cossa, declaro, por minha honra, que este trabalho de dissertação é resultado de uma investigação pessoal de carácter original, o qual nunca foi apresentado como tal nesta instituição e em nenhuma outra instituição de ensino superior, estando referenciadas no texto e nas referências bibliográficas as fontes utilizadas no trabalho.

Maputo, Março de 2026

_____

Zvika Costino Maniquidzua Cossa

Dedicatória

À minha família.

Ao meu esposo, Ercílio Carmindo Cossa e as minhas meninas, Melissa, Mirella, Lyana e Ellen, motivo das minhas lutas, dia após dia.

Agradecimentos

Em primeiro lugar agradeço a Deus pela vida, pela saúde e pela oportunidade que me proporcionou para que esta fase fosse conseguida.

Um especial agradecimento ao meu marido e as minhas meninas pelo amor, carinho, força, coragem e apoio incondicional pois foi determinante à realização do presente trabalho.

Aos meus pais pelo apoio, dedicação e ensinamentos ao longo da minha vida. Só aqui cheguei porque estiveram comigo o tempo todo. Aos meus irmãos e em particular a minha querida mãe, minha rainha por ter me ajudado a decidir optar pelo curso de Direito.

Agradecimentos também vão ao Professor Manuel Castiano pela paciência e atenção, que teve durante o processo de elaboração do trabalho. Obrigado pela forma metódica como me acompanhou, aconselhou e encorajou.

E por último, mas não menos importante, aos meus professores do curso de ciências jurídicas, sem os quais este feito não teria sido possível.

Muito obrigada. *Maita Basa*

Índice

ABREVIATURAS

Ac. –	Acórdão
Al. –	Alínea
Art. –	Artigo
CP –	Código Penal Moçambicano
CPP –	Código de Processo Penal Moçambicano
CPPB –	Código de Processo Penal Brasileiro
CPPP –	Código de Processo Penal Português
CRFB –	Constituição da República Federativa do Brasil
CRM –	Constituição da República de Moçambique
CRP –	Constituição da República Portuguesa
Dec. –	Decreto
DL –	Decreto Lei
IMEI –	Identificação Internacional de Equipamento Móvel
IMSI –	Identidade internacional do assinante de celular
JIC –	Juiz de Instrução Criminal
LC –	Lei do Cibercrime
MP –	Ministério Público
Nº –	Número
OPC –	Órgão de Polícia Criminal
PIC –	Polícia de Investigação Criminal
PJ –	Polícia Judiciária
Pág. –	Página
SERNIC –	Serviço Nacional de Investigação Criminal
UTI –	Unidade de telecomunicações e informática

RESUMO

Como consequência do crescimento da cibercriminalidade, tornou-se evidente a ineficácia dos meios tradicionais de obtenção de prova, os quais se revelaram incapazes de responder à nova dinâmica das sociedades contemporâneas. Diante disso, impôs-se aos Estados a necessidade de reformular ou criar instrumentos legais capazes de enquadrar novos meios de obtenção de prova, com destaque, no presente estudo, para as escutas telefónicas e a prova digital. Tratando-se de uma matéria emergente, complexa e ainda insuficientemente regulamentada, especialmente no ordenamento moçambicano, diversas dúvidas surgem quanto à sua aplicação prática e validade jurídica. Assim, o objetivo deste trabalho é analisar o regime jurídico desses meios de obtenção de prova sob a óptica do Direito Comparado, com ênfase nos sistemas jurídicos de Moçambique, Portugal e Brasil, identificando pontos de convergência e divergência. Constatou-se que, embora nenhum dos sistemas analisados disponha de um regime absolutamente completo, Portugal apresenta um modelo mais estruturado, consolidado e eficaz. Verificou-se também que Moçambique e Brasil carecem de reformas legislativas específicas. No caso moçambicano, o regime das escutas telefónicas, claramente inspirado no modelo português, foi transposto de forma parcial, resultando numa legislação incompleta e lacunar. Quanto à prova digital, observa-se a ausência de uma regulamentação clara e autônoma, estando esta dispersa em normas genéricas e insuficientes. Dessa forma, defende-se a revisão do Código de Processo Penal moçambicano, com a dupla finalidade de completar o regime das escutas telefónicas e de introduzir normas específicas sobre a obtenção, conservação e tratamento da prova digital. Recomenda-se, ainda, a capacitação técnica de instituições como o SERNIC, com a integração de peritos informáticos, bem como a adesão urgente de Moçambique à Convenção de Budapeste sobre o Cibercrime, como forma de alinhar-se aos padrões internacionais no combate à criminalidade digital e transnacional.

Palavras chave: Escutas telefónicas, Prova digital, Processo penal, Cibercrime

ABSTRACT

As a consequence of the growth of cybercrime, the traditional means of evidence collection have proven to be ineffective and unable to respond to the new dynamics of contemporary societies. This scenario has compelled States to reform or create legal instruments capable of regulating new forms of evidence gathering, with particular emphasis in this study on telephone interceptions and digital evidence. Given the emerging and complex nature of the topic, as well as the insufficient regulation—particularly within the Mozambican legal framework—numerous uncertainties arise concerning its practical application and legal validity. Accordingly, this research aims to examine the legal regime of these means of obtaining evidence from a comparative law perspective, focusing on the legal systems of Mozambique, Portugal, and Brazil, and identifying points of convergence and divergence. The findings reveal that, although none of the systems analysed have a fully comprehensive framework, Portugal has developed a more structured and effective model. It was also observed that Mozambique and Brazil require more specific legislative reforms. In Mozambique's case, while the telephone interception regime was clearly inspired by the Portuguese model, the legal transposition was partial and resulted in an incomplete framework. Regarding digital evidence, the country still lacks clear and autonomous regulation, which remains fragmented across general and insufficient provisions. Therefore, this study advocates for a revision of the Mozambican Code of Criminal Procedure, both to complete the legal regime governing telephone interceptions and to introduce specific rules concerning the collection, preservation, and handling of digital evidence. It also recommends the technical training of institutions such as SERNIC, through the integration of qualified digital forensic experts, and urges Mozambique's accession to the Budapest Convention on Cybercrime as a means of aligning its legal system with international standards in combating cyber and transnational crime.

Keywords: telephone interceptions; digital evidence; criminal procedure; cybercrime.

INTRODUÇÃO

A internet representa um dos maiores avanços tecnológicos da era moderna, transformando profundamente a forma como interagimos, trabalhamos e acessamos informação. Contudo, ao mesmo tempo em que possibilita inúmeros benefícios, também introduz novos riscos, especialmente no campo da criminalidade informática e organizada.

O direito, naturalmente, teve de acompanhar esta evolução, adaptando-se aos desafios impostos pela era digital. Como resposta, foram incorporados novos tipos penais no Código Penal, como os crimes praticados por meio de sistemas informáticos, assim como se passaram a reconhecer novos meios de obtenção de prova, complementando os meios tradicionais.

Em 2019, Moçambique aprovou um pacote legislativo penal que inclui o Código Penal, o Código de Processo Penal e o Código de Execução de Penas, trazendo à tona questões inéditas até então pouco debatidas. Entre elas, destacam-se os regimes das escutas telefónicas e da prova digital, ambos essenciais no combate à criminalidade moderna, mas que ainda suscitam diversas incertezas e desafios interpretativos — especialmente quando comparados aos regimes jurídicos de países como Portugal e Brasil.

O presente trabalho propõe-se a realizar uma análise comparativa entre os regimes jurídicos aplicáveis às escutas telefónicas e à prova digital em Moçambique, Portugal e Brasil, procurando compreender suas semelhanças, divergências e lacunas.

Diversas questões emergem nesse contexto: Como se realiza tecnicamente a interceptação e o registo de escutas? Quais são os prazos legais e sua possibilidade de renovação? Quem são os sujeitos legitimados à escuta? O operador de telefonia está preparado para lidar com os dados interceptados? Como garantir o sigilo profissional e a correta conservação da prova? Seria adequado permitir que tais operadores lidem com provas de alta sensibilidade, considerando que as escutas representam uma grave ingerência na privacidade e na liberdade de expressão, ambos direitos constitucionalmente protegidos?

Actualmente, Moçambique possui um regime específico para a prova obtida por escutas telefónicas, mas ainda carece de uma legislação própria e clara sobre a prova digital. Na prática, os aplicadores da lei têm recorrido à Constituição da República, ao Código de Processo Penal, à Lei nº 3/2017 (Lei das transações eletrônicas), à Lei nº 34/2014, de 31 de Dezembro (Lei de proteção de dados, à Lei nº 4/2016, de 3 de Junho (Lei das telecomunicações), à Lei 15/2023, de 28 de Agosto (Lei de prevenção, repreensão e combate ao Terrorismo), ao Decreto nº

44/2019 (regulamento do consumidor de telecomunicações), entre outras. Destaca-se, ainda, que Moçambique ratificou em 2019 a Convenção da União Africana sobre Cibersegurança e Proteção de Dados Pessoais, mas ainda não aderiu à Convenção de Budapeste sobre o Cibercrime, apesar dos reiterados apelos da Procuradoria-Geral da República.

Face à escassez de normas processuais específicas, a produção e admissibilidade da prova digital e das escutas telefônicas ainda se mostram pouco claras e frágeis. Assim, este estudo pretende contribuir criticamente para o debate, oferecendo uma análise fundamentada das reformas legislativas e dos caminhos possíveis para o fortalecimento do regime probatório em contexto eletrônico-digital.

A pesquisa aqui proposta se caracteriza como sendo uma pesquisa bibliográfica-documental, por pretender encontrar compreensão na revisão bibliográfica, legislativa e documental concernente ao assunto.
O estudo a ser feito basear-se-á na revisão da Literatura a qual consistirá em consultar obras e documentos que versam sobre a prova digital e as escutas telefônicas e a consulta da legislação e que regula a matéria em referência e um olhar pela jurisprudência existente.

Esta pesquisa irá versar apenas numa abordagem qualitativa, pois, far-se-à a analise, descrição, comparações e interpretações dos dados obtidos. Quanto à coleta de dados a pesquisa se enquadra como sendo de revisão bibliográfica, cujos dados serão obtidos através da Constituição da República, das leis codificadas, da legislação ordinária, da doutrina e da jurisprudência.

Os dados depois de colhidos por meio dos instrumentos de pesquisa acima mencionados, serão submetidos à leitura analítica e posterior análise de conteúdo, com vista a permitir uma interpretação crítica dos dados colhidos.

CAPÍTULO I

1. ANÁLISE CRÍTICA DA UTILIZAÇÃO DAS ESCUTAS TELEFÔNICAS

1.1. Aspectos Introdutórios

O recurso às escutas telefónicas no ordenamento jurídico moçambicano remonta ao Código de Processo Penal de 1929, cuja redação refletia os parâmetros e a realidade jurídica da época. Era no corpo do artigo 210 do referido Código, sob a epígrafe "Buscas e apreensões nos correios, telégrafos e estações radiotelegráficas", que se encontrava o fundamento legal utilizado para legitimar as atuações relacionadas a escutas telefónicas.

Face a evolução técnica e da tecnologia, da evolução criminal, situações existiam em que havia necessidade de não só se recorrer à interceptação de comunicações, como também fazer o uso da localização de um telemóvel e o nosso código não estava apto a responder a estas novas demandas, pois, o único artigo existente não especificava vários aspectos importantes, dentre os quais as circunstâncias em que esta acção deveria ocorrer ou qual a entidade competente para executar e fiscalizar o operador.

Comprovando o acima referido, verifica-se nas anotações feitas por Maia Gonçalves[1] ao referido artigo, entre outros aspectos, que existia uma fragilidade na legitimidade dos executores da diligência, na medida em que quem executava as diligências eram os empregados telégrafo-postais, sendo que a requisição desta era dirigida à Administração Geral, o que afastava a actividade da esfera da investigação criminal propriamente dita.

De referir que, com fundamento no artigo 210 do CPP de 1929, o agente da Polícia judiciaria e depois agente da polícia de Investigação Criminal (PIC) responsável por certo processo, fazia a requisição de registos (*files)* às agências sobre o contacto que se pretende investigar, direccionando-a à Administração desta, onde consta o número do processo, o facto a que se refere, o qual era assinado pelo Inspector da PIC adstrito à Brigada onde o agente estava afecto e, por fim, com vista dada pelo Juiz de Instrução Criminal (JIC).

Nisto, o agente tinha de ficar à espera que a direcção da empresa solicitada respondesse à requisição com os dados pedidos, podendo a resposta levar meses, pondo em causa a eficácia daquele acto. O mesmo acontecia em relação às gravações de conversações, em que os agentes

[1] GONÇALVES, Maia, LOPES, Manuel. (2007) *Código de Processo Penal*, 2ª Edição (anotado e Comentado). Coimbra: Almedina, pág. 316.

entregavam os números a investigar e depois de um certo período, os agentes deslocavam-se à agência para fazer a selecção do material necessário.

Não é difícil observar e concluir que estas diligências eram questionáveis pelo facto de serem executadas por funcionários não ligados à área de investigação, sobre as quais recaia a obrigatoriedade do sigilo das informações que teve acesso durante a interceptação, violando de forma grave o estabelecido no nº 1, art. 68 da CRM, relativo à inviolabilidade do domicílio e da correspondência ou outro meio de comunicação privada, salvo nos casos especialmente previstos na lei.

Um aspecto que importa fazer menção ainda neste regime é o § 2º do art. 210 do CPP de 1929 que exigia a fundamentação da necessidade do recurso a esses meios. Sucede que, o que se verificava é que se recorria a este meio de obtenção de prova para a localização de um telemóvel subtraído quando se sabe que este meio é usado em última instância, quando não é possível o uso dos tradicionais meios de prova, pois esta actuação viola o princípio da proporcionalidade, na medida em que sobrepesava o direito à propriedade em detrimento dos direitos a liberdade, dignidade e confidencialidade.

Outro aspecto que importa fazer referência é a última parte do corpo de texto do art. 210, do CPP de 1929, ao remeter a regulamentação do que não consta neste para uma lei especial deste meio, facto que até a data de aprovação do novo CPP, não se verificou. Nesta medida, ocorria que não havendo uma norma que determinava e limitava a actuação dos agentes, abria-se espaço para que ocorressem arbitrariedades no uso deste exclusivo meio de obtenção de prova.

Focando ainda na análise ao art. 210 do CPP, pode-se constatar que a redacção sobre a questão da interceptação e gravação de comunicações encontra-se incorporada no seio de outras formas de obtenção de prova, como é o caso de buscas e apreensões, que apesar de serem meios distintos, não clarificava em que circunstâncias cada uma delas deve ocorrer e os critérios a serem tomados em consideração para tal.

Por forma a tentar suprir as lacunas existentes no CPP de 1929, os aplicadores da lei socorriam-se das normas dispersas como as previstas na Lei nº 4/2016 de 3 de Junho[2], no seu artigo 64 que prevê a derrogação do sigilo das telecomunicações nos casos previstos na lei em matéria criminal ou que interessem à segurança nacional e à prevenção do terrorismo, criminalidade e

[2] Lei das telecomunicações.

delinquência organizadas e no nº 1 do artigo 66 que impõe que todo o operador de telecomunicações deva ter um sistema devidamente operacional e eficiente de interceptação legal de comunicação para efeitos de investigação criminal.

Também eram invocadas a Lei nº 3/2017 de 9 de Janeiro[3], no art. 68, que determina a garantia de "sigilo das comunicações transmitidas através das redes de telecomunicações de uso público, salvo nos casos previstos na lei em matéria de processo criminal ou que interesse à segurança nacional e à prevenção do terrorismo, criminalidade e delinquência organizada".

Igualmente, a Lei nº 15/2023[4] que prevê a intercepção do fluxo de comunicações em sistema de informática ou telemática, bem como a ordem a um provedor de serviço de comunicações para interceptar e reter comunicação específica, de uma descrição especificada recebida ou transmitida, ou prestes a ser recebida ou transmitida por um prestador de serviços de comunicação e por fim o decreto nº 44/2019 de 22 de Maio[5].

Apesar do esforço legislativo, nenhuma dessas normas fornece regras processuais claras quanto à execução das escutas, como: quem as deve realizar, o procedimento técnico de interceptação, ou quando essa pode ser realizada.

Outra lei usada para colmatar as lacunas do CPP de 1929, é a Lei Orgânica da Polícia da República de Moçambique, Lei nº 16/2013, de 12 de Agosto[6], que na Subsecção II, art. 19, nº 1, al. *a*), determinava que as escutas telefónicas constituíam tarefa específica da então PIC e, mesmo assim, apesar do esforço do legislador em determinar a competência para a execução da diligência, ainda não estava resolvida a questão de quais casos serão submetidos a esse meio de obtenção de prova, local para sua execução (se nas instalações dos serviços de telecomunicações, ou em sede própria- nas instalações onde funcionava a então PIC), os prazos de execução, fiscalização, a competência para autorização da realização destas, entre outras.

Por fim, não se pode esquecer que para fazer face aos desafios da nova era criminal, também recorria-se/recorre-se ao apoio dos países da região com os quais há cooperação, que o tenham regulado em sua legislação e tenham recursos materiais para sua realização, com vista a obter os resultados esperados.

[3] Lei das transações eletrônicas.
[4] Lei de prevenção, repreensão e combate ao Terrorismo.
[5] Regulamento de proteção do consumidor do serviço de telecomunicações.
[6] Revoga a lei que cria a Polícia da República de Moçambique (PRM), Lei nº 19/92, de 31 de Dezembro.

No ordenamento jurídico português, o regime actual está consagrado no CPP de 1987 (DL nº 78/87, de 17 de Fevereiro, com alterações da Lei nº 48/2007, de 29 de Agosto). Assim como em Moçambique, a previsão de gravações de comunicações já existia no CPP de 1929 (Dec. nº 16 489, de 15 de Fevereiro), alterado pelo DL nº 377/77, de 6 de Setembro, no qual o artigo 210 autorizava, por ordem judicial, a intercepção e gravação de comunicações.

Já no ordenamento jurídico brasileiro, convém destacar que antes da Constituição Federal de 1988, não havia, um diploma legal específico que disciplinasse a respeito das interceptações telefônicas de forma clara e eficiente[7].

Todavia, era o Código Brasileiro de Telecomunicações, aprovado pela Lei nº 4.117/1962, que regia a matéria, em seu artigo 57, inciso II, que estabelecia não constituir violação de comunicações *"o conhecimento dado ao juiz competente, mediante requisição ou intimação deste",* apresentava a relativização do direito ao sigilo, assim como alguns doutrinários demonstraram ser um direito sujeito a excepções, desde que a interceptação fosse precedida de ordem judicial.

Porém, devido ao desenvolvimento tecnológico e a utilização de comunicações telefônicas em larga escala, o legislador constituinte brasileiro verificou a necessidade de regulamentar as interceptações telefônicas, trazendo tal instituto expressamente no inciso XII, do art. 5º da Constituição Federal de 1988.

Todavia, após a nova Constituição houve controvérsias se havia necessidade de ser elaborada uma nova lei para permitir a interceptação ou se o código de telecomunicações continuava a permitir tal procedimento. Desta forma, em 1996 com o advento da Lei 9.296[8], ocorreu a devida regulamentação das interceptações telefônicas, apresentando as hipóteses de cabimento, formas e limites. Por ser composta de normas eminentemente processuais, sua aplicação é imediata, conforme o estabelecido no artigo 2º do CPP do Brasil.

É pacífico que em todos os ordenamentos jurídicos em estudo, o advento tecnológico e a crescente criminalidade organizada, foram os pressupostos para a criação de novos meios de

[7] GOMES, Luiz Flávio. MACIEL, Silvio. (2011). *Interceptação Telefônica: comentários à Lei 9.296, de 24.07.1996*. São Paulo: Editora: Revista dos Tribunais, pág. 15.
[8] BRASIL. Lei 9296 de 24 de julho de 1996. Regulamento o inciso XII, parte final, do art. 5º da Constituição Federal.

obtenção de prova, no caso as escutas telefónicas. Vale lembrar que o Brasil foi pioneiro na legislação especifica para disciplinar a matéria em estudo e até a presente data a referida legislação ainda está em vigor, apesar de já existir na mesa várias propostas de revisão legislativa.

1.2. Conceito

Não existe, até o momento, uma definição legal clara e precisa para o termo escutas telefónicas, apesar dos avanços legislativos que vêm sendo introduzidos. Porém, estas encontram-se tuteladas no nosso ordenamento jurídico no capítulo IV, secção I do CPP, enquanto meio de obtenção de prova suscetível de ser utilizado na investigação criminal, traduzindo-se na "intercepção" e gravação de conversações ou comunicações telefónicas.[9]

Do ponto de vista linguístico, a palavra escuta é um substantivo derivado do verbo escutar, e pode significar: "Acto de escutar; pessoa que escuta; lugar em que se escuta; (do antigo) esculca […]"[10]. Escutar pode ter os seguintes significados: "[…] prestar o ouvido a; dar ouvidos a; dar atenção a; tornar-se atento para ouvir; espiar; pôr-se a ouvir; deixar-se guiar por […]"[11]. Já a palavra intercepção está ligada ao verbo interceptar, que significa: "[…]deter ou interromper no seu curso; não deixar chegar ao seu destino; cortar; e pôr obstáculos no meio de […]".[12]

O conceito técnico de escuta telefónica é definido por Nuno Maurício e Catarina Iria da seguinte forma: "[…] a escuta telefónica consubstancia-se na captação, por meio técnico, das comunicações estabelecidas entre uma pessoa (o escutado) e todos os demais, por princípio sem conhecimento de qualquer um dos interlocutores"[13]. O conceito em análise abarca não só as conversações transmitidas por telefone, como também, o correio electrónico, outras formas de transmissão de dados por via telemática, bem como a intercepção das comunicações entre presentes.

[9] Cfr. Nº 1 do artigo 222 do CPP e nº 1 do artigo 187º do CPP de Portugal.
[10] Dicionário Priberam da Língua Portuguesa.
[11] Idem.
[12] Idem.
[13] MAURÍCIO, Nuno; IRIA, Catarina. (Janeiro-Junho 2006). *As escutas telefónicas como meio de obtenção de prova - Necessidade de uma reforma legislativa ou suficiência de uma interpretação conforme?: Ponto de situação numa já vaexata quaestio,* Polícia e Justiça. Instituto Superior de Polícia Judiciária e Ciências Criminais. Loures: III Série, N. º 7. pág. 93.

No que concerne as escutas telefônicas, o legislador nacional, estatuiu os pressupostos de admissibilidade das escutas, as formalidades a que devem respeitar e as consequências da inobservância dos pressupostos estabelecidos.

No que tange às intervenções em comunicações, é importante considerar dois tipos penais que são diretamente relacionados ao tema: o crime de devassa da vida privada e o crime de violação de correspondência ou de comunicação, previstos e punidos no artigo 252 e 253, ambos do CP.

Em primeiro lugar, encontramos na al. a) do nº 1 do artigo 252 do CP, que pune quem "interceptar, gravar, registar, utilizar, transmitir ou divulgar conversa, comunicação telefónica…"; e em segundo lugar, no nº 2 do artigo 253 do CP, que pune quem "sem consentimento, se intrometer no conteúdo de telecomunicações ou dele tomar conhecimento. "

Assim, entendemos nós ser relevante, para o entendimento dos artigos 222 do CPP, a destrinça entre os dois ilícitos e, mais precisamente, os conceitos de "intercepção" e "intromissão".
Deste modo, fala-se de "intromissão" quando se entra em algo que, como se costuma dizer na gíria, "não é da sua conta"[14]. Aqui, o tipo objetivo não exige que exista consciência da informação tida na conversa, sendo suficiente, para que se preencha o tipo penal deste artigo, que se impeça a recepção do destinatário do conteúdo da conversação. Já a "intercepção" implica que alguém se apodere do conteúdo de qualquer telecomunicação que não lhe está adstrito.

A palavra "intercepção" inclui a "intromissão" na conversa, sendo esta condição necessária para que alguém consiga obter o seu conteúdo (através de gravações ou registos)[15]. Nestes ilícitos, é elemento do tipo a intenção de devassa da vida privada. Quer isto dizer que, toda a intercepção implica uma intromissão, mas nem toda a intromissão implica uma intercepção.

Realizada esta distinção, depreende-se também a existência de concurso aparente de normas, por consumpção, na medida em que o crime de violação de correspondência ou de Telecomunicações é consumido pelo crime de devassa da vida privada.[16]

[14] CONCEIÇÃO, Ana Raquel, (2009). *Escutas Telefónicas: Regime Processual Penal*, Lisboa, Quid Juris, pág. 17.
[15] *Idem*, pág. 17.
[16] Sob pena de violação do princípio *ne bis in idem*, "segundo o qual o Estado não pode submeter a um processo um acusado duas vezes pelo mesmo facto, seja em forma simultânea ou sucessiva", cfr. Ac. do Tribunal da Relação de Guimarães, de 26/02/2020, proc. 105/17.9 GAMGD.G1, disponível em http://www.dgsi.pt.

Qualquer um destes conceitos exige que se utilizem meios técnicos de captação, audição e registos, uma vez que o conhecimento através de outra forma não preenche os conceitos tipos.[17]

As escutas telefónicas constituem uma categoria de métodos ocultos de investigação, em virtude de serem realizadas sem o conhecimento do visado, "o que faz com que continuem a agir, interagir, a expressar-se e a comunicar de forma inocente, fazendo ou dizendo coisas de sentido auto-incriminatório ou incriminatório daqueles que com ela interagem ou comunicam, ou seja, levam as pessoas atingidas a ditar de forma inconsciente confissões não livres"[18].

As escutas telefônicas têm em vista a investigação e a recolha de provas que permitam a descoberta da verdade material[19], mas possuem o compromisso de garantir a conjugação de duas vertentes: em que, de um lado, se exige a segurança da sociedade em geral e o (re)estabelecimento da paz jurídica, fruto dos novos fenómenos da criminalidade, nomeadamente a criminalidade violenta e organizada, o terrorismo e o cibercrime; e, de outro lado, o respeito pelos direitos fundamentais dos cidadãos, face à necessidade de utilização de meios de obtenção de prova mais sofisticados que, apesar de se revelarem mais eficazes perante a criminalidade que se vem enfrentado, demonstram-se, também, mais invasivos e intrusivos na esfera da vida privada.

Muitas vezes, é neste domínio que se suscitam os essenciais problemas jurídicos, uma vez que, tem-se tornado vulgar o recurso ao excepcional, mesmo sabendo que as escutas telefónicas só devem ser determinadas em última instância face à lesão que causa a direitos constitucionalmente consagrados.[20]

Assim sendo, afirma-se que as escutas telefónicas operam "de forma endémica e epidémica, sem adequados controles formais e substantivos e são feitas a quem entenda que é útil escutar em segredo (…) onde o melhor seria que a confissão fosse extorquida à bruta para se não perder tempo, tal como acontecia em épocas pretéritas"[21].

---

[17] CONCEIÇÃO, Ana Raquel. (2009). *Escutas Telefónicas: Regime Processual Penal*, Lisboa, Quid Juris, pág. 18.
[18] ANDRADE, Manuel da Costa, (2009). *"Bruscamente no Verão Passado" a Reforma do Código de Processo Penal: As observações críticas sobre uma lei que podia e devia ter sido diferente*, Coimbra, Coimbra Editora, pág. 105.
[19] SILVA, Germano Marques da, (2008). *Curso de Processo Penal, Vol. II*, 4.ª Ed., Lisboa: Verbo, pág. 233.
[20] VALENTE, Manuel Guedes, (2008). *Escutas Telefónicas: Da Excecionalidade à Vulgaridade*, 2.ª Ed., Lisboa, Almedina, pág. 59.
[21] CORREIA, João, (2004). *Afirmar a Advocacia: Reflexões sobre a Cidadania e a Justiça*, Coimbra: Almedina, pág. 72.

No ordenamento jurídico português a semelhança do nosso, as escutas telefônicas também são consideradas meios de obtenção de prova, encontrados no livro III, título III, capítulo IV do CPP português. Também naquele ordenamento não encontramos uma definição legal clara e concreta sobre as escutas telefônicas, apenas os pressupostos de admissibilidade das escutas, as formalidades a que devem respeitar e as consequências da inobservância dos pressupostos estabelecidos.

No Brasil, importa referir que, o regime das escutas telefônicas é ditado pela Lei nº 9.296/96 de 24 de Julho e não pelo CPP brasileiro, como acontece no nosso caso e em Portugal. Relativamente ao conceito de escutas telefônicas, a supracitada lei também não apresenta o conceito desta, sendo a doutrina quem traz o conceito.

A lei brasileira destaca ser diferente o conceito de interceptação telefônica, da escuta telefônica, da gravação telefônica, da interceptação ambiental, da escuta ambiental e por fim da gravação ambiental[22].

A doutrina brasileira[23] entende ser interceptação telefônica (ou interceptação em sentido estrito) a captação da conversa telefônica realizada por terceiro sem o conhecimento dos comunicadores; já a escuta telefônica: é a captação da conversa telefônica realizada por terceiro com o conhecimento e assentimento de um dos comunicadores e desconhecimento do outro; a gravação telefônica ou gravação clandestina vai ser a captação da conversa telefônica realizada por um dos comunicadores, sem o conhecimento do outro. Inexiste a figura do terceiro interceptador, trata-se de uma autogravação;

Interceptação ambiental: é a captação da conversa ambiente realizada por terceiro sem o conhecimento dos interlocutores. Inexiste comunicação telefônica e também ocorre com violação do direito à intimidade; a escuta ambiental é definida como sendo a captação de uma comunicação, no ambiente dela, realizada por terceiro com o conhecimento e assentimento de apenas um dos interlocutores. Não há comunicação telefônica; e por fim a gravação ambiental

[22] A escuta ambiental e a gravação ambiental são conceitos inexistentes na nossa legislação assim como na legislação portuguesa.
[23] GRINOVER, Ada Pellegrini, GOMES FILHO, Antônio Magalhães; FERNANDES, António Scarance. (2009). *As nulidades no processo penal.* 11ª edição, rev., atual. e ampl. São Paulo: Revista dos Tribunais, pág. 160 seguintes.

é a captação da conversa ambiente realizada por um dos interlocutores, sem o conhecimento do outro. Inexiste a figura do terceiro interceptador. Não há comunicação telefônica.[24]

No entanto, imperioso é observar que a Lei 9.296 menciona em seu artigo 1º o seguinte: *"interceptação de comunicações telefônicas de qualquer natureza"* o que imporia ser necessária a autorização em qualquer forma de captação. No entanto, mesmo a legislação transmitindo a ideia de amplidão em seu conceito, ele permanece limitado, Grinover[25] sustenta que o conceito somente engloba a escuta e eventual gravação de conversa telefônica, quando praticada por terceira pessoa, esta, devendo ser diversa dos interlocutores, podendo ter conhecimento ou não. Portanto, restam excluídas do previsto em lei, as gravações clandestinas de telefonemas próprios, bem como as gravações entre presentes "escuta ambiental".

1.3. A tutela constitucional e processual penal das escutas telefónicas

As escutas telefónicas, por se tratarem de métodos ocultos de obtenção de prova, são consideradas extremamente intrusivas, uma vez que afetam diretamente direitos fundamentais dos cidadãos. Sua utilização implica inevitavelmente a derrogação de garantias constitucionais, tais como o direito à palavra, à privacidade da vida pessoal e familiar, e ao bom nome e reputação, consagrados no artigo 41 da Constituição da República de Moçambique (CRM). Ressalte-se que, no caso do direito à reputação, a violação ocorre não no momento da escuta, mas sim na divulgação do conteúdo interceptado.

É, ainda, restringido ao sujeito, o direito à liberdade de expressão, tutelado no artigo 48 da CRM, enquanto direito fundamental negativo de não ser impedido, pelas autoridades públicas, de se exprimir livremente.

Para além dos direitos fundamentais, constitucionalmente garantidos, há direitos fundamentais de natureza processual que também são afetados. É caso disso, o direito ao silêncio do arguido enquanto núcleo fundamental do direito à não autoincriminação[26], e a presunção de inocência do arguido (nº 2 do artigo 59 da CRM). O arguido tem, segundo os artigos referidos, o direito de não produzir prova contra si mesmo, isto é, o direito de não ter de contribuir positivamente para a sua condenação.

---

[24] *Idem*, pág. 160 e seguintes.
[25] GRINOVER, Ada Pellegrini, GOMES FILHO, Antônio Magalhães; FERNANDES, António Scarance. *As nulidades no processo penal.* 11ª edição, rev., atual. e ampl. São Paulo: Revista dos Tribunais, 2009. pág. 170/171.
[26] ANDRADE, Manuel da Costa, *"Bruscamente no Verão Passado"...,* op. cit., pág. 186.

A restrição destes direitos é em razão da sua lesão irreparável, resultando assim, do nº 2 do artigo 68 da CRM, referente ao direito à inviolabilidade do sigilo da correspondência e dos outros meios de comunicação privada, a proibição de ingerência das autoridades públicas nas telecomunicações, excepto com autorização da lei processual penal.

Conforme se pode depreender da parte final deste preceito, esta proibição não é absoluta, deixando o legislador espaço para situações em que fosse imprescindível usar certo meio de obtenção de prova, em razão da ineficácia de outro meio de obtenção de prova.

Esta excepção justifica-se em proveito do princípio da descoberta da verdade material[27], e só é permitido se cumpridos determinados requisitos, que analisaremos no decorrer deste trabalho. Portanto, estabelecem-se nulas as provas adquiridas sem a observância das formalidades legais, fazendo parte do catálogo das proibições de prova[28].

Os danos sociais intrinsecamente ligados às escutas telefónicas são definidos por Manuel da Costa Andrade como "polimórfica", uma vez que "quem aplicar as escutas telefónicas nunca consegue limitar os danos. Os estragos têm uma dimensão subjetiva (apanhamos sempre mais pessoas do que queríamos apanhar) e lesam sempre muitos mais bens jurídicos, muitos mais interesses do que aqueles que se queria lesar"[29].

Estes danos, no contexto do Estado de Direito e com base no princípio da liberdade, legalidade e respeito pela dignidade da pessoa humana, leva à determinação deste meio de obtenção de prova como excecional, sendo este admitido apenas quando se chegue à conclusão de que a prova seria impossível ou muito difícil de obter através de outro meio.

No ordenamento jurídico português, adota-se abordagem semelhante, o legislador a par das escutas telefônicas procurou sempre a salvaguarda dos direitos constitucionalmente consagrados, tais como o direito à palavra, o direito à reserva da vida privada, familiar e o direito ao bom nome e reputação (artigo 26º da CRP). Os direitos fundamentais de natureza processual (direito ao silêncio do arguido enquanto núcleo fundamental do direito à não autoincriminação[30], e a presunção de inocência do arguido previsto no artigo 32.º, n.º 2 da

[27] CONCEIÇÃO, Ana Raquel, op. cit., pág. 68.
[28] Cfr. Nº 3 do art. 65 da CRM, nº 2 do art. 156 e art. 224, ambos do CPP e nº 8 do art. 32º da CRP, nº 3 do art. 126º e art. 190º ambos do CPP de Portugal.
[29] ANDRADE, Manuel da Costa, *op.* cit., pág. 187.
[30] ANDRADE, Manuel da Costa, op. cit., pág. 186.

CRP), também foram alvo de salvaguarda. Portanto, a violação destes direitos só será possível com autorização da lei processual penal.

Já no Brasil, o artigo 5º da CRFB, garante o sigilo de correspondência e de comunicação telegráfica, de dados bancários e fiscal e de comunicação telefônica. A CRFB declara invioláveis, a intimidade, a vida privada, a honra e a imagem das pessoas. Sendo assim, estamos em face de garantias constitucionais, não podendo e não devendo ser violadas, salvo nos termos da própria constituição. Portanto, nos termos dela a inviolabilidade destes direitos é admitida por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal.

Em todos os três ordenamentos jurídicos analisados, é pacífico o entendimento de que a escuta telefónica representa uma exceção constitucional, só admitida quando expressamente autorizada e quando os requisitos legais forem rigorosamente observados. Trata-se de uma medida de última instância, cuja aplicação exige uma rigorosa ponderação entre o interesse público da investigação e os direitos individuais do cidadão.

1.4. Requisitos de admissibilidade materiais/substanciais[31]

No contexto moçambicano, as escutas telefónicas são admitidas no âmbito de um processo penal e encontram fundamento legal no artigo 222 do Código de Processo Penal (CPP). O legislador estabelece que sua admissibilidade depende do cumprimento de requisitos materiais, o que significa que esse meio de obtenção de prova apenas pode ser utilizado em situações específicas, que se enquadrem nos parâmetros legais, portanto, só admissível:

1.4.1. No âmbito da instrução preparatória[32]

Embora o legislador nacional não tenha delimitado expressamente o momento processual em que as escutas telefónicas podem ser utilizadas, entende-se, na prática, que sua aplicação se dá preferencialmente durante a fase de instrução preparatória, em virtude da sua finalidade de investigação quanto à prática ou não de um determinado crime.

[31] Cfr. Art. 222 do CPP e artigo 187.º do CPP de Portugal.

[32] Diferentemente do nosso legislador, o legislador português optou por deixar plasmado na lei quando é que podem ter lugar as escutas telefonicas, quando se refere no nº 1 do artigo 187 do CPP português que "... só podem ser autorizadas durante o inquerito...". O legislador nacional optou por não se referir especificamente quando as escutas telefónicas podem ter lugar, mas, na prática, só na instrução do processo pois, entende-se ser ineficaz fazer escutas quando o arguido já tem acesso ao processo.

As escutas telefônicas ocorrem quando já existe notícia de um crime, sendo necessária à sua averiguação, o apuramento dos seus agentes e a responsabilidade a si adstritas e, por fim, a recolha da respetiva matéria probatória, com vista à decisão de acusação ou não acusação, conforme o artigo 307 do CPP.

A instauração de escutas exige a existência de uma *notitia criminis*, seja em relação a factos já consumados ou ainda em curso. Contudo, a simples notícia do crime não é suficiente: exige-se, conforme referem autores como Manuel da Costa Andrade, "uma forma relativamente qualificada da suspeita da prática do crime"[33]. Por sua vez Paulo Pinto de Albuquerque, vai além, sustentando "é necessário que, antes, se tenham indícios da prática do crime e não, por si só, a notícia do crime"[34].

Importa destacar que esses indícios não precisam ser tão robustos quanto os exigidos para uma acusação formal ou para aplicação de medidas de coação mais gravosas. No entanto, devem configurar uma hipótese criminosa plausível, com base em elementos de prova identificáveis e processualmente admissíveis, ou como refere Paulo Albuquerque "Tais elementos, embora não precisem de ter a consistência necessária para a dedução de acusação ou para a imposição das medidas de coacção mais graves, devem permitir configurar uma séria e concreta hipótese criminosa" cuja verosimilhança só pode assentar em meios de prova identificáveis e utilizáveis no processo"[35].

Como já nos referimos anteriormente, o nosso legislador não consagrou quando é que as escutas telefônicas podem ter lugar, portanto, nada impede que as mesmas possam ter lugar na fase da audiência e debate preliminar.

No entanto, em nosso entender, não seria válida essa opção, de se poder realizar escutas telefônicas durante fase da audiência preliminar, pois, as escutas, no sentido de interceptar o que outros dizem ao telefone, só funcionam se quem estiver a ser escutado não souber que o está a ser. Não há sentido prático na realização de escutas após a fase de instrução pois, assim que esta fase termina com a dedução da acusação, o arguido obtém conhecimento destas pelo

[33] ANDRADE, Manuel da Costa, (2013), *Sobre as Proibições de Prova em Processo Penal*, Reimpressão, Coimbra, Coimbra Editora, pág. 290.
[34] ALBUQUERQUE, Paulo Pinto de, *Comentário ao Código de Processo Penal...,* op. cit., pág. 524.
[35] *Idem*, pág. 526.

direito que lhe é conferido de examinar o conteúdo do auto de intercepção relativos a conversações ou comunicações interceptadas, conforme dispõem o nº 5 do artigo 223 do CPP.

Excepcionalmente, pode haver necessidade de diligências complementares, como a verificação de chamadas efetuadas por determinado número ou da localização de um telemóvel. Nesses casos, tais elementos podem ser requisitados, inclusive pela defesa, sob a égide do regime das escutas, tal como previsto no nº 2 do artigo 189º do CPP português.

No regime processual penal português, os requisitos formais de admissibilidade das escutas telefónicas encontram-se no artigo 187 do CPP de Portugal. Estas são apenas admitidas na fase de inquérito e não são admitidas na fase de instrução, já que está fase não pressupõe a consumação ou não de um crime.

No que lhe concerne, no sistema português, esta é a fase em que, consoante o artigo 286º do CPP de Portugal, o JIC, assistido pelos OPC, se ocupará de verificar se a decisão, de deduzir acusação ou de arquivamento do inquérito, foi tomada, pelo MP, de forma correta para, se for o caso, submeter a causa a julgamento. Esta opção tomada pelo legislador português tem sido muito criticada por alguma doutrina, considerando que as escutas telefónicas deveriam ser admissíveis também na fase de instrução, na condição do juiz considerar imperioso novas diligências de prova[36].

Já no Brasil, pela interpretação que se faz do artigo 1º da lei nº 9.296 de 24 de Julho, as escutas telefônicas tem lugar na investigação criminal e na fase de instrução processual penal.
Na verdade, neste aspecto, os sistemas em análise são semelhantes diferenciando apenas a nomenclatura usada para cada fase e o facto de o nosso legislador não ter especificamente estatuído a fase processual que se pode usar das escutas telefônicas. Aquilo a que chamamos fase de instrução compreende a fase de inquérito no sistema português, e aquilo a que chamam de fase de instrução, o legislador nacional designou por audiência preliminar.

1.4.2. Em casos excepcionais

Tal como ocorre em Portugal, em Moçambique as escutas telefónicas apenas são admissíveis em casos excepcionais, justamente por implicarem restrições a direitos fundamentais, como previamente escrutinado. A sua utilização pressupõe a demonstração de que tal diligência é

[36] *Idem*, pág. 531.

indispensável para a descoberta da verdade ou que seria impossível ou extremamente difícil obter a prova por meios menos invasivos.

Em razão disso, exige-se que a escuta telefónica se apresente como único meio capaz de recolher o material probatório tido em vista, por impossibilidade dos restantes menos restritivos.

Quer isto dizer que "não será legítimo ordenar as escutas telefónicas nos casos em que os resultados probatórios almejados possam, sem dificuldades particularmente acrescidas, ser alcançadas por meio mais benigno de afronta aos direitos fundamentais"[37]. Ora, "desde que a motivação da decisão revele as razões para se acreditar que as escutas telefónicas são indispensáveis para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter, tal revelação (nos termos do n.º 1 do artigo 222 do CPP) será equivalente a considerarem-se as escutas telefónicas essenciais às finalidades da investigação"[38].

Nesta lógica, a utilização deste meio de obtenção de prova em última *ratio*, fortalece a aplicação dos princípios da necessidade, da adequação e da proporcionalidade, consagrados constitucionalmente pelo legislador nacional, sendo assim necessário que "a escuta telefónica se revele um meio em concreto adequado a mediatizar aquele resultado"[39].

Ainda que isto determine a diminuição da admissibilidade do recurso às intercepções telefónicas nos casos em que é possível recolher prova de outro modo, não se crê que o legislador tenha tido intenção de restringir esse recurso. Se essa fosse a sua intenção, não teria se quer introduzido o mecanismo em referência, pois como se sabe, esta constitui uma das inovações do legislador nacional.

Só serão, então, admissíveis as escutas telefónicas quando se demonstre a utilização ineficaz de outros meios de obtenção de prova ou a necessidade inevitável deste, face à natureza do crime e às circunstâncias que o rodeiam. Posto isto, o entendimento assente é de que as escutas telefónicas não devem ser ordenadas na qualidade de primeiro meio de obtenção de prova,

[37] ANDRADE, Manuel da Costa, *Sobre as Proibições...,* op. cit., pág. 291.
[38] *Idem*, pág. 291.
[39] *Idem*, pág. 293.

considerando-se prudente não as ordenar imediatamente após a abertura da instrução, 'sob pena' de se considerar demasiado prematuro.

Paulo Pinto de Albuquerque reconhece ser " (…) necessária a demonstração objetiva e explícita quanto à ineficácia dos meios de investigação até ali usados para a averiguação do crime ... "[40], e Manuel Guedes Valente afirma que "Os OPC não podem, após a notícia do crime, solicitar de imediato autorização para realizar escutas telefónicas sem que primeiro se fundamente que os meios de investigação, até então usados, não são adequados e proporcionais *stricto sensu* para prevenir e investigar o crime *sub judice*"[41].

Contrariamente, André Lamas Leite, crê "ser possível lançar-se mão as escutas telefónicas logo como primeiro meio de obtenção da prova utilizado, quando o JIC se convença, em face dos concretos dados factuais trazidos pelo MP, que ela é a única diligência capaz de fazer carrear para os autos elementos probatórios aptos à descoberta da verdade. Nessas situações, as escutas são, de idêntica forma, indispensáveis a esse desiderato"[42].

No Brasil, os requisitos materiais para a realização válida das escutas telefônicas encontram-se na constituição e na Lei nº 9.296/96 de 24 de Julho. Na Constituição Federal, é no inciso XII do art. 5º, que se estabelecem os requisitos mínimos: (a) exigência de ordem judicial devidamente fundamentada; (b) nas hipóteses e na forma que a lei estabelecer; c) que a interceptação seja realizada para fins de investigação criminal (medida cautelar) ou instrução processual penal (medida cautelar incidental).

Em complemento à Constituição Federal a Lei 9.296/96, em seu art. 2º e seus incisos, apresentou as hipóteses legais para utilização da interceptação telefônica. A lei mencionada, estabeleceu a necessidade de analisar-se os pressupostos básicos de uma medida cautelar, quais sejam, *fumus boni iuris*, no direito penal denominado como *fumus commissi delict* e *periculum in mora*, no direito penal chamado como *periculum in libertatis*, especialmente nos incisos I e II do artigo 2º ora analisado.

O primeiro requisito patente da Lei nº 9.296/96 é o *fumus commissi delicti* propriamente dito, ou seja, fumaça da prática de um facto punível. Aqui busca-se demonstrar a necessidade de se

[40] ALBUQUERQUE, Paulo Pinto de, *Comentário ao Código de Processo Penal...,* op. cit., pág. 524.
[41] VALENTE, Manuel Guedes, *Escutas Telefónicas...*, op. cit., p. 51.
[42] LEITE, André Lamas, (2007), *Entre Péricles e Sísifo: O novo regime legal das escutas telefónicas*, Coimbra, Coimbra Editora, pág. 620.

apresentar elementos que fundamentam a convicção de que o suspeito foi o autor daquele crime.

O segundo requisito previsto na lei é a contrário senso "a prova não puder ser feita por outros meios disponíveis" cumpre o pressuposto do *periculum in libertatis,* ou seja, verifica-se a urgência em determinar o uso da medida ao caso concreto, pois qualquer demora, poderá colocar em risco um direito ou interesse.

O terceiro, prevê a não utilização da interceptação de comunicações telefônicas quando o facto investigado constituir infração penal punida, no máximo, com pena de detenção, a *contrario sensu*, o legislador permitiu, portanto, tal ingerência nos crimes punidos com reclusão.

Este último requisito é alvo de várias críticas doutrinárias[43], uma vez que o legislador, com essa redação, por um lado, deixou de apreciar infrações penais que poderiam utilizar a interceptação telefônica, até como único meio de obter-se a prova, como é o exemplo da ameaça por telefone.

Por outro lado, há críticas doutrinarias[44] quanto a sua extensão, pois estaria abrangendo qualquer crime com pena de reclusão, tanto da legislação comum como especial, sem fazer distinção quanto ao grau de lesividade de cada um deles. Por meio de uma aplicação da letra fria da lei é possível o uso de interceptação telefônica para a investigação de furto simples, mesmo sendo reconhecido como um delito de pequena gravidade, pelo simples facto de ser punido com reclusão.[45]

Em comparação, o modelo moçambicano se mostra mais restritivo e adequado, ao estabelecer um catálogo fechado de crimes passíveis de escuta, conferindo maior segurança jurídica e respeito aos direitos fundamentais. A este proposito se referiu Grinover que "É evidente o excesso do legislador brasileiro, que não se deu conta da excepcionalidade da interceptação telefônica como meio lícito de quebrar o sigilo das comunicações, estendendo sua permissão a crimes que podem não ser de grande potencial ofensivo e, em contrapartida, excluindo-a de

[43] GOMES, Luiz Flávio. MACIEL, Silvio. (2011). *Interceptação Telefônica: comentários à Lei 9.296, de 24.07.1996. São Paulo*: Editora: Revista dos Tribunais. Pág. 93.
[44] *Idem*, Pág. 98
[45] *Idem*, Pág. 101

infrações penais de menor relevância social, mas que, por sua índole, só poderiam ser devidamente apuradas por intermédio da referida interceptação."[46]

Posto isto, é imperioso concluir que as interceptações telefônicas no sistema brasileiro, à semelhança do que ocorre no nosso sistema, somente deveriam ser concedidas em relação aos crimes que coloquem em risco à vida, à integridade física ou aqueles crimes que afrontem o Estado Democrático de Direito, visto que é bastante agressivo invadir a esfera da intimidade de um indivíduo por infração penal de pequeno valor social.

Independentemente da linha a seguir, fica assente que, nos ordenamentos em estudo as escutas telefónicas nunca poderão ser utilizadas por ser o meio mais célere ou o mais fácil/eficaz, tendo impreterivelmente de cumprir os respetivos requisitos materiais, tendo em conta os princípios da adequação e necessidade.

1.5. Órgãos Responsáveis

A autorização para a realização de escutas telefónicas está sujeita a um conjunto de requisitos formais rigorosos, cuja observância é essencial para garantir a legalidade da prova obtida. A exigência de tais formalidades visa proteger os direitos fundamentais do indivíduo e assegurar a validade processual da diligência.

A fase da instrução é dirigida pelo MP[47], mas, há certos actos que estão atribuídos ao juiz de instrução, nomeadamente a autorização, proferida através de despacho fundamentado, para a realização de escutas telefónicas[48], em razão da restrição de direitos, liberdades e garantias a que estas estão adstritas.

Esta exigência de fundamentação da decisão referente ao requerimento da diligência encontra justificação, não apenas no artigo 8 e o nº 1 do artigo 222, ambos do CPP, mas também, no nº 4 do artigo 107 do CPP e 215 da CRM. Portanto, ainda que o MP seja quem dirige a instrução, o JIC é o Juiz dos Direitos, Liberdades e Garantias. Sempre que lhe pareça estarem a ser postos em causa Direitos, Liberdades e Garantias, é da competência do Juiz *ex oficio*, pronunciar-se sobre tal questão mesmo que a matéria em causa, o seja da competência do MP.

[46] GRINOVER, Ada Pellegrini, GOMES FILHO, Antônio Magalhães; FERNANDES, António Scarance. *As nulidades no processo penal.* Op. Cit. pág. 170/171.
[47] Cfr. Artigo 52 conjugado com o artigo 308, ambos do CPP.
[48] Cfr. Nº 1 do artigo 222 do CPP e nº 1 do artigo 187 do CPP de Portugal.

No sistema português[49], o MP é a única entidade com legitimidade para requerer a diligência, não sendo então possível que o JIC autorize uma escuta telefónica por iniciativa própria, assim como nenhum dos restantes sujeitos processuais poderá requerer a realização deste meio de prova.

Este facto faz com que o JIC só possa autorizar a escuta telefónica nos termos requeridos pelo MP, na medida em que, não pode indicar que sejam realizadas escutas a pessoas ou telefones diversos dos indicados no requerimento do MP, uma vez que isso resultaria, indiretamente, numa autorização por iniciativa própria.

O nosso legislador deixou esta competência não só nas mãos do MP, mas do próprio Juiz[50], pois, refere no nº 1 do artigo 222 do CPP que"... só podem ser ordenadas ou autorizadas, por despacho do juiz...", portanto, o Juiz pode sim ordenar a realização desta diligência, sem que a direção desta fase deixe de pertencer ao MP. Pensamos nós, que andou bem o legislador nacional ao alargar o leque de pessoas legítimas para o efeito.

Exceptuam-se desta regra, os casos em que a competência para autorizar a realização de escutas pode caber "ao juiz dos lugares onde eventualmente se puder efetivar a conversação ou comunicação telefónica ou da sede da entidade competente para a investigação criminal", nos crimes previstos no nº 2 do artigo 222 do CPP e nº 2 do artigo 187º do CPP de Portugal.

O legislador português, estabeleceu que nesta circunstância, a autorização tem de ser levada ao conhecimento do juiz do processo (para a prática de actos jurisdicionais subsequentes), no prazo de 72 horas (nº 3 do artigo 187º do CPP de Portugal), diferentemente do nosso legislador que foi omisso neste aspecto, obrigando aos aplicadores da lei a recorrer às boas práticas ou a prazos gerais.

No Brasil, a interceptação das comunicações telefónicas poderá ser determinada pelo juiz[51], de ofício ou a requerimento da autoridade policial e do representante do Ministério Público. [52] Portanto, no Brasil é mais amplo o número de sujeitos com legitimidade para requerer a diligência comparativamente a nós e a Portugal, o que de certa forma, na nossa opinião é uma

[49] Cfr. Nº 1 do Artigo 187 do CPP de Portugal.
[50] Aqui apesar de a lei não se referir especificamente a um juiz, entendemos nós que tratar-se-á do juiz de instrução, nos lugares que houver e juiz da causa nos lugares em que não houver juiz de instrução criminal.
[51] Designado juiz das garantias, nos termos do artigo 3 do CPP do Brasil.
[52] Cfr. Artigo 3 da Lei nº 9.296 de 24 de Julho de 1996.

mais valia para o processo, na medida em que não se ficar-se-á preso ao impulso só ao juiz ou ao MP.

1.6. Duração

No CPP não se encontra na letra lei o prazo máximo para a realização de escutas e consequentemente não se pode falar de prazo para renovação, mas, entendemos que o prazo vai ter de ser igual ao da instrução, apesar de em termos práticos a ultrapassagem dos prazos de instrução não afectar a validade dos actos nele praticados, conforme se entende do artigo 323 do CPP.

Portanto, teria sido útil, se o nosso legislador tivesse fixado um prazo máximo pois, como já nos referimos anteriormente, este meio de obtenção de prova é delicado pois mexe com direitos constitucionalmente consagrados.

Nestas condições, corremos riscos de agentes de crime serem alvo deste procedimento por tempo indeterminado, enquanto se estiver a investigar, quando se sabe que nestes casos quanto maior o tempo, maiores são as exigências da proporcionalidade.

Importa desde já referir que, neste quesito, foi mais feliz o legislador português, na medida em que indicou um prazo máximo, que pode ser autorizado para a realização de escutas, que é de três meses, podendo ser renovado por períodos com o mesmo limite, isto se cumprirem os requisitos de admissibilidade, devendo cessar imediatamente logo que se torne desnecessária para a descoberta da verdade nos termos no disposto no nº 6 do artigo 187º do CPP de Portugal.

A lei portuguesa nada diz quanto ao número de renovações possíveis a que a escuta pode ser submetida, no entanto, é entendimento de Paulo de Alburquerque[53] que o limite dessas renovações seja o fim do inquérito, já que as escutas telefónicas só são legítimas nesta fase.

No ordenamento jurídico brasileiro, o prazo é de 15 dias renováveis por igual período, conforme dispõe o artigo 5 da Lei nº 9.296 de 24 de Julho de 1996. Embora o prazo seja de 15 dias prorrogáveis, nunca se sabe quanto tempo poderá levar a interceptação, até que produza os efeitos almejados, por isso, a jurisprudência brasileira acabou sepultando esta limitação. No Brasil, intercepta-se a comunicação telefônica enquanto for útil a colheita de prova.[54]

[53] ALBUQUERQUE, Paulo Pinto de, *Comentário ao Código de Processo Penal...,* op. cit., pág. 528.
[54] ROMÃO, Anderson Sérgio, *Interceptação De Comunicação Telefônica: Um viés da Execução Penal,* Revista da Escola Superior de Polícia Civil, Vila Izabel – Curitiba/PR—CEP: 80.320-290

Conclui-se assim que, nos ordenamentos jurídicos em estudo, as escutas telefônicas duram enquanto durar a instrução do processo e como tal, só é legitimo o recurso a ela enquanto decorrerem as investigações.

1.7. Os Tipos Legais Admissíveis

Nesta matéria, o legislador, entendeu que a admissibilidade de escutas telefónicas só pode ocorrer quanto a um catálogo fechado de ilícitos criminais, indo de encontro à previsão constitucional "salvo os casos previstos na lei em matéria criminal".[55] O legislador elencou um conjunto de ilícitos criminais, que considerou mais graves ou que podem ser cometidos através de telefone, estando todos enumerados de forma taxativa no artigo 222 do CPP.

Esta opção ilustra, novamente, a ideia de excepcionalidade que o legislador pretendeu conceder quanto à utilização deste meio de obtenção de prova. O legislador impede assim o recurso às escutas telefónicas para qualquer outro tipo de crime independentemente da sua gravidade.

Em Portugal a opção legislativa também foi no sentido de estabelecer um catálogo fechado de crimes, conforme se pode ver no artigo 187º do CPP de Portugal.

Em relação a este catálogo de crimes colocam-se algumas questões na doutrina portuguesa[56], relativa a opção do legislador português ao incluir naquele catalogo de crimes passiveis de escutas telefônicas, o crime de evasão. Antes de mais, lembrar que este crime não consta do nosso catalogo de crimes, facto que nos faz parabenizar o legislador nacional pois, a escuta no caso de evasão, em nosso entender, será realizada para localizar o evadido e não para obter a prova do crime.

Aliás, o próprio artigo refere que é necessário que o arguido evadido tenha sido condenado quanto a algum dos crimes previstos nas demais alíneas, não cumprindo esta alínea a finalidade máxima das escutas, que é a indispensabilidade para a descoberta da verdade ou a impossibilidade ou elevada dificuldade na obtenção da prova.

Neste caso, a prova do crime já está feita, sendo esta permissão traduzida num meio de captura e não num meio de obtenção de prova, existindo quem defenda[57], assim como nós, a

[55] Cfr. Nº 2 do artigo 68 da CRM.
[56] ALBUQUERQUE, Paulo Pinto de, *Comentário ao Código de Processo Penal...,* op. cit., pág. 533. e SUSANO, Helena, (2009). *Escutas Telefónicas: Exigências e controvérsias do actual regime*, Coimbra, Coimbra Editora, pág. 28.
[57]ALBUQUERQUE, Paulo Pinto de, *Comentário ao Código de Processo Penal...,* op. cit., pág. 535

inadmissibilidade da autorização para a realização de escutas neste contexto. Neste sentido, Paulo Pinto de Albuquerque, crê que seja inconstitucional esta norma em razão de ser alheia ao que diz respeito à prova e da violação do nº 4 do artigo 32º conjugado com o artigo 18º, ambos da CRP[58].

No entanto, Helana Susano no caso de evasão defende que, poderá fazer-se uma ponderação entre os Direitos, Liberdades e Garantias da pessoa condenada e o interesse público na detenção desta. Neste sentido, ela considera não haver violação do princípio da adequação e da proporcionalidade, caso esta seja a única maneira de se localizar a pessoa condenada[59].

O legislador brasileiro não estabeleceu um catálogo de crimes possíveis como acontece em Moçambique e Portugal. No artigo 2º da Lei nº 9.296 de 24 de Julho de 1996, o legislador brasileiro estabelece as hipóteses em que a interceptação da comunicação telefônica não será permitida.

Gomes e Maciel criticam esta redacção, primeiro porque ao enumerar os casos em que a interceptação não será permitida, o legislador além de dificultar o entendimento, cria a expectativa equivocada de que a interceptação é a regra e o sigilo excepção, numa evidente e inadmissível inversão ao espirito normativo do texto constitucional. E segundo, ao invés de restringir os casos em que a interceptação telefônica poderia e deveria ser utilizada, amplia o seu universo de tal maneira, que a medida passa a ser utilizada em crimes cujo os bens jurídicos lesionados não justificam o uso desta para a sua investigação.[60]

1.8. Sujeitos

O legislador nacional assim como o brasileiro foram omissos neste aspecto, deixando este papel para os aplicadores da lei, que certamente terão de recorrer às boas práticas para identificar quem pode ou não ser alvo das escutas telefônicas.

Na situação que acima nos referimos, situações haverá em que as escutas telefônicas são contra incertos, correndo-se o risco de violação de direitos constitucionalmente consagrados de pessoas que nada tem a ver com o arguido, com a vítima ou mesmo com o processo. No entanto, em nossa opinião, os sujeitos das escutas telefônicas a identificar pelos aplicadores da lei,

[58] ALBUQUERQUE, Paulo Pinto de, *Comentário ao Código de Processo Penal...,* op. cit., pág. 533
[59] SUSANO, Helena, *Escutas Telefónicas: Exigências e controvérsias do actual regime*, op. cit. pág. 40.
[60] GOMES, Luiz Flávio. MACIEL, Silvio. *Interceptação Telefônica*, op. Cit. pág. 93.

devem ser os mesmos indicados pelo legislador português[61], pelas razões que abaixo faremos referência.

No ordenamento jurídico português, à semelhança do que acontece com o catálogo de crimes que admitem que se ordene escutas telefónicas, existe, também, uma delimitação quanto às pessoas que podem ser alvo de escutas, estando definida no n º 4 do artigo 187º do CPP português. São estas: "a) suspeito ou arguido; b) pessoa que sirva de intermediário, relativamente à qual haja fundadas razões para crer que recebe ou transmite mensagens destinadas ou provenientes de suspeito ou arguido; ou c) vítima de crime, mediante o respetivo consentimento, efectivo ou presumido".

Em princípio, o despacho de autorização judicial deve sempre identificar as pessoas que serão alvo de escutas, não sendo possível que se realizem escutas contra incertos. Tal como defende Paulo Pinto de Albuquerque: "A existência de um catálogo de alvos obsta à determinação de escutas telefónicas em processo contra incertos. O legislador português pretendeu que a autorização judicial tivesse por referência as conversações mantidas por pessoas concretas, ainda que não seja conhecida a sua identidade civil"[62].

Em Portugal apesar de a lei especificamente enumerar as pessoas sujeitas a escutas telefônicas, não significa, que não possam ser interceptadas e gravadas conversas de pessoas que nada têm a ver com a prática desse mesmo crime, e que não estão abrangidas no catálogo de pessoas que podem ser visadas numa escuta. São exemplo disso as conversações tidas entre o arguido e os seus amigos/conhecidos, em que o alvo da escuta é o arguido, em virtude da existência de indícios quanto à prática de crime de catálogo por parte deste.

Ainda relativamente às escutas as comunicações do suspeito e do arguido, questiona-se se tal não contende com o direito ao silêncio e à garantia contra a autoincriminação?

Relativamente ao "suspeito", esta problemática nem sequer se põe, porque é no momento da constituição de arguido que esse sujeito passa a usufruir de um estatuto híbrido, que lhe confere direitos e deveres. Portanto, o problema em questão, entendemos nós que não se vai colocar se a escuta telefónica tiver sido feita antes da constituição como arguido, ou seja, quando o visado é mero suspeito.

[61] Cfr. Nº 4 do artigo 187 do CPP de Portugal
[62] ALBUQUERQUE, Paulo Pinto de, *Comentário ao Código de Processo Penal...,* op. cit., pág. 509.

É necessário entender que a escuta telefónica não poderá ser uma forma de subverter o princípio do direito à não autoincriminação, que é uma manifestação do princípio da presunção de inocência.[63] Parte-se do pressuposto de que não é lícito obter através de uma escuta telefónica aquilo que o arguido recusou dar em interrogatório. Assim, as escutas telefônicas enquanto meio de obtenção de prova acabam por derrogar este direito ao silêncio do arguido, já que, quando o arguido é sujeito a escuta, há a possibilidade de obter-se conhecimentos relativos à prática do crime, que resultam das comunicações tidas por si através do telemóvel e que, noutra circunstância, não seriam por sua vontade reveladas.

No entanto, é nosso entendimento que, apesar de já constituído arguido, a escuta telefónica visa obter prova sobre actividade criminosa futura ou ainda em curso, nesse caso, o arguido ainda não foi interrogado quanto a esses novos/futuros actos, logo não pode haver subversão do direito ao silêncio.

Assim, não se pode entender que o direito ao silêncio do arguido é violado pela utilização das intercepções telefónicas pois ter-se-á subjacente uma deturpação da teleologia do processo penal, quando não uma visão alheia à princípios fundamentais, entre os quais se encontra o da procura da verdade, seguindo pelos caminhos delimitados pelo respeito dos direitos e garantias dos intervenientes processuais, que, diga-se de passagem, não se resumem aos direitos do arguido e que, em última análise, é o direito da própria comunidade à exigência de um processo penal justo.[64]

Outra figura elencada pelo código processual português é o "intermediário". Este faz parte do elenco de pessoas que podem ser sujeitas à intercepção e gravação de comunicações, tal como consta da alínea b) do nº 4 do artigo 187º do CPP de Portugal. Este estipula a possibilidade de execução de escutas a determinadas pessoas que não têm qualquer envolvimento na execução do crime. O que difere esta situação da situação anteriormente observada, é o facto de que, nesta, a pessoa é passível de ser sujeita a escuta telefónica mesmo não sendo suspeito ou arguido, porque sobre ela recaem razões para crer que possa receber ou transmitir mensagens destinadas ou provenientes do suspeito ou arguido.

[63] Cfr. Ac. do STJ, de 02/04/2008, proc. 08P578, disponível em http://www.dgsi.pt. Acesso em 08 de Novembro de 2024
[64] Cfr. Ac. do STJ, de 02/04/2008, proc. 08P578, disponível em http://www.dgsi.pt. Acesso em 08 de Novembro de 2024

Melhor definindo intermediário é "todo aquele que, pela sua proximidade com o arguido ou suspeito, seja por razões de ordem familiar, seja por razões de amizade, ou por quaisquer outras, que levem ao contacto entre ambos, ainda que ocasional ou forçado, se prefigure como potencial interlocutor, por qualquer uma das formas previstas nos artºs. 187º e 189º do CPP de Portugal.

E ainda sobre o qual, pela respectiva autoridade judiciária, recaiam suspeitas fundadas de, nos referidos contactos, serem discutidos assuntos que, directa ou indirectamente, se prendam com o crime em investigação e, tal como anteriormente se indicou, "a sua acção pode ser puramente passiva, pois que não é o seu comportamento que aqui se visa, mas, tão só, o de alguém que, sendo suspeito ou arguido da prática de um crime, com aquele se possa relacionar, e com fortes probabilidades de, nos respectivos contactos, falarem do mesmo crime. Nestes casos, não se pressupõe que o referido interlocutor (…) tenha um papel activo na recepção ou transmissão da mensagem"[65].

A última alínea deste catálogo indicado pela lei portuguesa abrange a vítima, que pode ser alvo de escuta, se prestar o seu consentimento efetivo ou presumido.

Tendo em vista garantir o direito de defesa do arguido, o legislador nacional apesar de não ter indicado os sujeitos passiveis deste meio de obtenção de prova, estatuiu no nº 3 do artigo 222 do CPP, a proibição das intercepções e gravações a conversações ou comunicações entre o arguido e o seu defensor, excepto quando o juiz tem fundadas razões para crer que essas constituem objeto ou elemento de crime.

A questão que se coloca aqui é de que não haverá igual restrição quanto às restantes pessoas abrangidas pelo segredo profissional, consignado no artigo 168 do CPP? Aqui concordamos com a opinião de Paulo Pinto de Albuquerque, que crê que o fundamento da proibição das escutas telefónicas relativamente ao arguido e seu defensor é válido para as pessoas sujeitas a segredo profissional e que, neste sentido, o legislador alargou o leque no seu nº 3 do artigo 223 do CPP, contemplando-as também[66].

As conversas entre o arguido e os demais constantes no artigo 168 do CPP, só devem ser objeto de escuta telefónica quando o juiz tenha "fundadas razões para crer que elas constituem objeto

[65] Ac. do Tribunal da Relação de Lisboa, de 06/12/2007, proc. 10278/07-9, disponível em https://www.dgsi.pt. Acesso em 28 de Novembro de 2024.
[66] ALBUQUERQUE, Paulo Pinto de, *Comentário ao Código de Processo Penal...,* op. cit., pág. 527.

ou elemento do crime". Já não se entende o mesmo quanto às pessoas do artigo 167 do CPP, que detêm o direito à recusa de depoimento, sendo possível que estas sejam alvo de escutas, como vimos anteriormente[67].

"O fundamento que justifica a proibição no que respeita às pessoas obrigadas a segredo profissional, não se aplica a estas pessoas. O direito à recusa de depoimento resulta do facto de este poder ser deturpado, por estarem em causa relações familiares. O mesmo não acontece nas escutas telefónicas, porque a pessoa em questão não sabe que está a ser escutada, não havendo o "dilema" quanto a dizer ou não a verdade, sabendo que esta poderá incriminar o suspeito/arguido"[68].

Concorda-se com este entendimento por se entender que, posto o analisado, as pessoas abrangidas pelo artigo 167 do CPP usufruem de um direito ao silêncio, enquanto as pessoas englobadas no artigo 168 do CPP, por estarem sujeitas a segredo profissional, têm o dever de silêncio.

No ordenamento jurídico português, relativamente a proibição das interceptações e gravações a conversações ou comunicações entre o arguido e o seu defensor opera de forma semelhante ao nosso ordenamento, conforme se pode ver no nº 5 do artigo 187º do CPP de Portugal. Naquele ordenamento o fundamento da proibição das escutas telefónicas relativamente ao arguido e seu defensor também é válido para as pessoas sujeitas a segredo profissional conforme, alínea *b)* do nº 6 do artigo 188º do CPP de Portugal.

Na legislação brasileira não encontramos regra semelhante à acima referida, portanto, não está especificamente legislado se há restrição do uso deste meio de prova tratando-se de determinadas pessoas. Cremos que isto se deve ao facto de a legislação brasileira ser já antiga e ainda não ter ainda acompanhado as novas dinâmicas sociais. Portanto, seria de bom grado que numa futura revisão da referida legislação se incorporasse esse aspecto pelos motivos já acima referidos.

1.9. Requisitos formais das escutas telefónicas

[67] VALENTE, Manuel Guedes, *Escutas Telefónicas...*, op. cit., pág. 93:
[68] Idem, pág. 101.

A realização de escutas telefónicas, para além de depender da verificação cumulativa dos requisitos materiais anteriores estudados, tem ainda de cumprir requisitos formais.

A lei processual penal impõe a obrigação de a SERNIC, após a realização da escuta telefónica, lavre o auto correspondente em que indique as passagens mais relevantes para a prova, descreva o conteúdo das conversações e explique o alcance que tem para a descoberta da verdade.[69]

O CPP português exige para além do auto, um relatório nos termos do que dispõem o nº 1 do artigo 188º do CPP de Portugal. No sistema português, o auto e o relatório, assim como os suportes técnicos, devem ser apresentados ao MP até ao décimo quinto dia a contar da data da primeira intercepção efetuada.[70] Este procedimento repete-se daí em diante, de 15 em 15 dias, até ao fim da diligência. O MP, por seu turno, dispõe do prazo de 48 horas para a comunicação desses elementos ao juiz, conforme o nº 2 do artigo 188º do CPP de Portugal.

No sistema brasileiro, exige-se apenas o auto de transcrição. Nos termos do artigo 5º da Lei nº 9.296 de 24 de Julho de 1996, a autoridade policial encaminhará o resultado da interceptação ao juiz, acompanhado de auto circunstanciado, que deverá conter o resumo das operações realizadas. A autoridade policial no decurso da diligência vai dando ciência sempre ao MP, que poderá acompanhar a diligência.[71]

Contrariamente ao que se sucede no sistema português e brasileiro, a nível nacional o auto, junto com as fitas gravadas, é imediatamente levado ao conhecimento do juiz que tiver ordenado ou autorizado, nos termos do que dispõe o nº 1 do artigo 223 do CPP. Em nosso entender, não foi muito feliz o legislador nacional ao assim estatuir, pois excluiu totalmente a participação do MP nestas diligências, quando se sabe que é necessário que o MP, proceda com o controle das escutas telefónicas a partir da sua autorização por exigência de controlo da cadeia de custódia, pois como refere Benjamim Silva "a jurisdicionalização de todo o processo de produção de prova por intermédio das escutas telefónicas ou monitorização dos fluxos de informação e comunicação digital, requer a participação do MP para garantir que as gravações não foram nem serão alvo de qualquer manipulação por entidades não legalmente autorizadas"[72].

[69] Cfr. Nº 1 do artigo 223 do CPP
[70] Cfr. N º 3 do artigo 188º do CPP de Portugal
[71] Cfr. Artigo 6 da Lei nº 9.296 de 24 de Julho de 1996
[72] RODRIGUES, Benjamim Silva, (2008). *Das Escutas Telefónicas: A Monitorização dos Fluxos Informacionais e Comunicacionais*, *Tomo I*, Coimbra: Coimbra Editora, pág. 356.

Não se encontra na nossa lei qualquer justificação para que assim se proceda. É incompreensível que o MP depois de requerer a diligência de escutas telefônicas não tenha conhecimento imediato do resultado delas, não só na qualidade de órgão requerente, mas também como fiscal da legalidade.

O nosso legislador afastou por completo a acção do MP nesta fase, quando se sabe perfeitamente que ele é o titular da instrução. Incluir o MP nesta fase, está indubitavelmente relacionado com o facto de ser, cada vez mais, necessária uma actuação de diversos sujeitos processuais nesta fase, por razões de urgência face à evolução da criminalidade.

André Lamas Leite afirma que levar ao conhecimento do MP em primeiro plano é conferir a aquele órgão a função de confirmar a relevância probatória das passagens indicadas pelo SERNIC e se essas vão de acordo com as exigências vinculadas às escutas, nomeadamente as do artigo 222 do CPP. Isto não quer dizer que, não concordando, na íntegra ou em parte, com a relevância do material probatório recolhido pelos agentes, possa ordenar a sua destruição[73].

O MP não tem competência para ordenar a destruição de elementos resultantes das escutas telefónicas, sendo essa uma competência exclusiva do Juiz, tal como decorre do nº 3 do artigo 223 do CPP.

Na legislação portuguesa e brasileira acontece de forma semelhante, o MP também não tem competência para ordenar a destruição de elementos resultantes das escutas, conforme n º 6 do artigo 188º do CPP de Portugal e artigo 9 da Lei nº 9.296 de 24 de Julho de 1996, respectivamente. No sistema português apesar de o MP tomar conhecimento do conteúdo das escutas em primeiro lugar, este facto só lhe dá permissão para requerer a suspensão das escutas, caso se verifique uma violação extrema dos requisitos do artigo 187º do CPP de Portugal.

O legislador português fixou o prazo de 48 horas para que o MP leve ao conhecimento do Juiz o conteúdo das escutas, este prazo inicia-se então assim que sejam recebidos os expedientes pelos serviços do MP. Já o nosso legislador assim como o brasileiro não fixou prazo algum para o mesmo efeito.

Concordamos com a opção portuguesa como a mais correta, face à celeridade que se pretende alcançar e por em causa estarem restrições altamente danosas a direitos constitucionalmente

[73] LEITE, André Lamas, *Entre Péricles e Sísifo.* (2007). *O novo regime legal das escutas telefónicas*, Coimbra, Coimbra Editora, pág. 622.

consagrados, assim, cremos que a fixação do prazo é importante e deveria começar a contar assim que a informação chegasse aos serviços do MP. Este prazo pode evitar a existência de vastos períodos de falta de controlo judicial às escutas e que se faça, de forma constante, uma ponderação e fundamentação da decisão da sua manutenção.[74]

Embora exista a incumbência de transmissão do conteúdo da comunicação interceptada por parte do SERNIC ao Juiz[75], a lei permite-lhes que antes dessa transmissão, conheça previamente o conteúdo da comunicação interceptada e, a esse fim, realize, actos cautelares necessários e urgentes para que se assegurem os meios de prova.

Esta possibilidade visa a tomada de conhecimento prévio do conteúdo das gravações com o intuito de evitar ou atenuar os efeitos de determinado crime praticado, ou que se pretende praticar, sucede que o nosso legislador não enuncia que actos cautelares poder-se-á fazer o uso nestas situações.

Situação diferente ocorre em Portugal, em que o legislador claramente enuncia que um dos meios usados para assegurar os meios de prova é a prisão preventiva, efectuada logo após o OPC tomar conhecimento do conteúdo da comunicação interceptada, conforme nº 7 do artigo 188 do CPP de Portugal. Mas deverá se ter por base que, não será possível que a detenção em flagrante delito se encontre como justificativa para que sejam realizadas escutas telefónicas "sob pena da já massificada vulgarização e futura inutilização do meio excepcional descredibilizar, ainda mais, a justiça penal"[76].

Conforme já nos referimos anteriormente, a nível nacional não encontramos disposição igual, no sentido de fundamentar a prisão preventiva para assegurar os meios de prova, portanto, em nosso entender a prisão preventiva só vai ter lugar nos casos previstos no artigo 243 do CPP.

Nos termos legislados no nosso CPP, não é possível fundamentar a prisão preventiva para garantir a conservação dos meios de prova, mesmo se SERNIC tiver tomado conhecimento de que alguns meios de prova correm risco de ser destruídos ou adulterados. Entendemos nós não fazer sentido este vazio legal, numa altura que se pretendia inovar, que legislador nacional não

[74]RODRIGUES, Benjamim Silva, op. Cit., pág. 356.
[75] Cfr. Nº 1 artigo 223 do CPP.
[76] VALENTE, Manuel Guedes, Teoria Geral..., op. cit., pág. 81.

tivesse incluído essa disposição legal, fazendo-nos correr o risco de não poder assegurar meios de prova, que já se tem conhecimento por meio das escutas telefônicas, que serão destruídos.

Dando prosseguimento ao estudo dos requisitos formais da escutas telefônicas, como já nos referimos anteriormente, nos termos do nº 3 do artigo 223 do CPP, o juiz pode mandar proceder a destruição imediata dos suportes e relatórios manifestamente estranhos ao processo em 3 situações: a) que disserem respeito a conversações em que não intervenham pessoas com vínculo com o crime; b) que abranjam matérias cobertas pelo segredo profissional, de funcionário ou de Estado; ou c) cuja divulgação possa afectar gravemente direitos, liberdades e garantias; ficando todos os intervenientes vinculados ao dever de segredo relativamente às conversações de que tenham tomado conhecimento.

Quanto a este tema, surgiu a problemática de se saber se, não dando conhecimento ao arguido antes da destruição desses suportes técnicos e relatórios, esta norma violava as garantias de defesa previstas na Constituição, uma vez que, ao arguido é dada a possibilidade de conhecer, no fim do inquérito, as escutas telefónicas realizadas no âmbito do processo, como em seguida ver-se-á.

Entendemos nós que esta norma não viola as garantias de defesa do arguido por não estar em causa nenhuma interpretação de qualquer autoridade judiciária relativa à relevância para a prova do conteúdo das conversações, mas sim o facto das conversações gravadas dizerem respeito a pessoas que não podem legalmente ser objecto de escuta, considerando que "a destruição de suportes técnicos e relatórios manifestamente estranhos ao processo, ao abrigo do disposto no supra citado artigo, tem por base a protecção do direito ao sigilo das telecomunicações e da reserva de intimidade da vida privada de terceiros, em relação aos quais a lei de processo criminal não autoriza a intercepção e a gravação de conversações. Assim, defender a destruição destes suportes técnicos e relatórios, apenas depois do arguido deles ter conhecimento e de poder pronunciar-se sobre a sua relevância, comportaria uma desnecessária e inaceitável compressão daqueles direitos constitucionalmente consagrados"[77].

Como supra se começou a tratar, finda a instrução, o arguido e o assistente podem aceder ao auto de transcrição das conversações ou comunicações de que tenham sido alvo e, à sua custa, obter cópia dos elementos naquele referido.

[77] Ac. do Tribunal Constitucional de 29/05/2008, proc. 304/08, disponível em https://www.tribunalconstitucional.pt/. Acesso em 30 de Novembro de 2024.

O legislador nacional não estabeleceu nenhum prazo para esse efeito, mas cremos que o prazo limite será o termo do prazo para requerer-se a audiência preliminar a semelhança do que se sucede no sistema português, em que o prazo é o termo dos prazos previstos para requerer a abertura da instrução ou a apresentação da contestação.

Um aspecto que merece menção é o facto de o nosso legislador ter estatuído que arguido, o assistente e outros interessados só tem acesso ao auto de transcrição, quer isto dizer que, só tem acesso aos elementos que o juiz considerar/escolher relevante para a prova.[78]

Os elementos que o juiz não considerar relevantes não poderão ser usados pelos requerentes como meio de prova, limitando assim a actuação do arguido e outros interessados. É da competência do juiz a escolha dos elementos relevantes para a prova a serem transcritos, nem ao MP, na qualidade de titular da acção penal foi dada essa competência.

Diferentemente acontece no sistema português, em que o arguido e o assistente têm acesso aos suportes técnicos das conversações ou comunicações e podem transcrever para juntar ao processo, não estão limitados a escolha do JIC, naquilo que aquele acha ou não relevante. O arguido e o assistente têm a vantagem de poder escolher o que é relevante para a sua defesa.

Assim, as transcrições feitas pelo arguido ou assistente, dentro do prazo estipulado, que forem junto ao processo como anteriormente indicado, valerão como prova, conforme as alíneas *b)* e *c)* do nº 9 do artigo 188º do CPP de Portugal, a par das transcrições mandadas efetuar pelo MP ao OPC que efetuou a intercepção, e indicadas como meio de prova na acusação (alínea *a)* do nº 9 do artigo 188º do CPP de Portugal).

Julgamos melhor a posição adoptada pelo legislador português comparativamente ao nosso uma vez que nos parece bastante plausível e lógica, já que é ao MP que cabe a direção da instrução, como previamente se constatou.

Para além disto, confere ao arguido a extensão de direitos processuais, nomeadamente, o direito de defesa e o direito ao contraditório, na medida em que deixa de ter apenas a oportunidade de examinar os autos transcritos por ordem do juiz e passa a poder, ele próprio, recolher prova, através da transcrição de conversações ou comunicações que considere que lhe são favoráveis.

[78] Cfr. Nº 3 do artigo 223 do CPP.

O mesmo acontece quanto ao assistente, uma vez que, salvo raras exceções, a sua actividade está subordinada à intervenção do MP.

Neste sistema verifica-se um plano de igualdade entre o MP, o arguido e o assistente no que diz respeito à relevância probatória. A seleção dos elementos relevantes quanto às comunicações que integrarão a prova, é feita por estes sujeitos processuais, não valendo como prova outras comunicações além dessas.

O CPP de Portugal[79] estabelece que independentemente das transcrições que venham a ser ordenadas, os suportes técnicos de conversações ou comunicações são conservados em envelope lacrado, à ordem do tribunal, até que a decisão que pôs termo ao processo transite em julgado, sendo depois disso destruídos. Os que não forem destruídos depois de transitada a decisão, "são guardados em envelope lacrado, junto ao processo, e só podem ser utilizados em caso de interposição de recurso extraordinário"[80].

Os intervenientes na intercepção e gravação de qualquer conversa ou comunicação ficam sujeitos ao dever de segredo de todas as informações que advieram destas operações ao seu conhecimento, segundo o nº 6 do artigo 188º, *in fine* do CPP de Portugal.

Mais uma vez, verifica-se a oportunidade que o nosso legislador perdeu de ter inovado, pois na nossa legislação não se encontra dispositivo legal que estabelece o destino a dar as gravações depois do trânsito em julgado da decisão. Não se sabe se ficaram para sempre junto aos autos ou se não chegam sequer a acompanhar os autos, uma vez que existe o auto de transcrição. Cremos que será uma daquelas situações em que os bens aprendidos nos autos muitas das vezes não acompanham os autos e ficam perdidos em alguma instituição, se não tiverem sido apoderados por alguém de má-fé.

Quanto ao órgão com competência para realizar as interceptações telefônicas, que constitui quanto a nós um dos requisitos de admissibilidade material ou substancial das escutas telefônicas, importa referir que, estabelece a Lei de segurança interna portuguesa no seu artigo 24 que a PJ é o OPC com competência para executar a interceptação e a gravação das comunicações.

[79] Cfr. nº 12 do art. 188º.
[80] Cfr. nº 13 do art. 188º.

"Com o aval do JIC, proferido por meio de um despacho devidamente fundamentado, indicando a matéria de facto e de direito, o OPC está autorizado a proceder às interceptações, que devem iniciar-se o mais rapidamente possível, de forma a produzir efeitos naquelas circunstâncias de tempo.

A Unidade de telecomunicações e informática (doravante UTI) de Lisboa (unidade central) oficia as operadoras (Vodafone, MEO, NOS, etc.) da autorização concedida pelo juiz para se proceder às interceptações telefónicas, com o propósito de haver duplicação de linha do número do suspeito. Esta linha entra num computador central da PJ que grava as comunicações, além de disponibilizar em tempo real as comunicações.

Preenchidos todos os requisitos burocráticos supramencionados, encontram-se, agora, os investigadores em condições de acederem aos terminais de interceptação, localizados na PJ. À vista disto, para acederem aos terminais, os investigadores com intenção de gravar em suporte técnico ou de escutar em tempo real, dirigem-se às instalações da PJ.

Uma vez no interior das instalações, o investigador dirige-se para o local onde se encontram os terminais. Nesse espaço, denominado Centro de Controlo de Monitorização (MCC), cada terminal disponibilizado encontra-se já previamente afeto a um determinado OPC (PSP, GNR, SEF), cabendo ao investigador aferir se algum dos terminais imputados ao OPC que representa se encontra livre, com o intuito de iniciar a audição ou gravação das comunicações interceptadas"[81].

No nosso caso é da competência do SERNIC de acordo com o CPP[82]. Sucede que, continuamos a proceder de forma semelhante à maneira como se procedia no CPP de 1929, não existe duplicação de linha do número do suspeito e muito menos uma linha que entra no computador central do SERNIC, ou seja, o nosso CPP não estabeleceu a forma técnica de proceder a interceptação e gravação.

O que acontece é que, os aplicadores da lei vão se socorrendo de dispositivos legais avulsos tais como a lei das telecomunicações, que no seu artigo 64 prevê a derrogação do sigilo das telecomunicações nos casos previstos na lei em matéria criminal ou que interessem à segurança

[81] Silva, Hugo Franco Gomes da, 2019, *o acesso a terminais de intercepção de comunicações pelos órgãos de polícia criminal,* Dissertação de mestrado, Instituto Superior de Ciências Policiais e Segurança interna, pág. 44 e 45.
[82] Cfr. Nº 2 do artigo 223 do CPP.

nacional e à prevenção do terrorismo, criminalidade e delinquência organizadas e nº 1 do artigo 66 que impõe a todo o operador de telecomunicações o dever de ter um sistema devidamente operacional e eficiente de interceptação legal de comunicação para efeitos de investigação criminal.

No mesmo fio lógico, a Lei nº 15/2023, de 28 de Agosto, que aprova a Lei do Terrorismo, também prevê a intercepção do fluxo de comunicações em sistema de informática ou telemática, bem como a ordem a um provedor de serviço de comunicações para interceptar e reter comunicação específica, de uma descrição especificada recebida ou transmitida, ou prestes a ser recebida ou transmitida por um prestador de serviços de comunicação.

A questão que nos colocamos é, será que o operador da telefonia móvel vai saber dar o devido tratamento a esses dados? Poderá quebrar o sigilo profissional que tem para com os seus clientes? Efectuará uma devida colheita e conservação da prova obtida até ser entregue aos agentes dos serviços de investigação? Terá o operador de telefonia móvel perfil adequado para ter contacto com este tipo de prova, atendendo que as escutas telefônicas constituem um meio de obtenção de prova gravoso, na medida em que se revela numa ingerência nas telecomunicações e uma ofensa à privacidade e a palavra, direitos constitucionalmente protegidos?

Verifica-se que as empresas de telefonia móvel foram colocadas na posição de desempenhar as funções do Estado, quando se sabe que a acção criminal não pode ser exercida por privados, o ideal seria que os agentes do SERNIC tivessem acesso a uma linha duplicada na própria instituição e não na operadora de telecomunicações.

Por outro lado, o agente da operadora não é a pessoa ideal, na medida em que não possui competências técnicas para o efeito, sem contar que este terá acesso a um conjunto de informações atinentes a vida privada de pessoas e não há garantias no tratamento a ser dado a aquele tipo de informação. Facto é que, o SERNIC não dispõe nem de meios materiais e nem de técnicos especializados para o cabal desempenho da diligência.

Em suma, como refere-se a PGR[83] no seu informe anual, "... a dinâmica desta criminalidade impõe a aprovação de uma lei específica ... e estabeleça, na componente processual, medidas

[83] Informe anual da PGR à Assembleia da República do ano de 2023, pág. 35 e 36.

especiais de recolha, conservação e manutenção da prova, bem como de análise forense, prevenção de perdas, manejo de incidentes e avaliação de risco...".

"Por outro lado, é nosso desafio potenciar a área de tecnologias de informação e comunicação, com pessoal especializado, impondo-se, assim, a formação de peritos informáticos para auxiliarem na investigação, sobretudo, na recolha e tratamento da prova digital ou eletrônica."[84]

No ordenamento jurídico brasileiro, apesar de dispor de uma lei sobre as escutas telefônicas com certa vivência, em termos de interceptação telefônica, dos três países em estudo é o que apresenta um sistema de interceptação mais avançado. Peritos da Polícia Federal construíram o novo Sistema de Interceptação de Sinais (SIS), que dispensa os serviços das operadoras de telefonia ou de qualquer empresa que atue em outros ramos de comunicação, como internet, rádio ou mecanismos que usem sinais via satélite. O referido sistema é um conjunto de softwares, acoplado a equipamentos que funcionam numa central operada pela polícia, sob o controle online do juiz que autoriza a interceptação, Ministério Público e, especialmente, do Conselho Nacional de Justiça (CNJ) – o maior parceiro da Polícia Federal na empreitada.

1.10. Consequências da violação dos requisitos legais das escutas telefónicas

As escutas telefónicas são reguladas enquanto meio de obtenção de prova pelo artigo 222 e ss do CPP, sendo que, nesses artigos, se estipulam os meios e as condições legais para que se possa realizar a intercepção de uma comunicação telefónica, mas, depois, a escuta, enquanto meio de obtenção de prova, dá origem a um resultado, que é o conteúdo dessas conversações ou comunicações. Estas passarão, na parte que interessa, para o auto e para o processo, como deriva do artigo 223 do CPP. O auto de transcrição das conversas registadas são já um meio de prova, neste caso, a prova documental.

O nº 1 do artigo 400 do CPP dispõe que "não valem em julgamento, nomeadamente para o efeito de formação da convicção do tribunal, quaisquer provas que não tiverem sido produzidas ou examinadas em audiência", levantando-se o problema de saber se é essencial que o juiz do julgamento proceda à leitura do auto de transcrição da escuta para que esta tenha valor de prova documental.

[84] Idem, pág. 35 e 36.

A jurisprudência portuguesa tem entendido, de forma maioritária que, a partir do momento em que as escutas telefónicas passam para os autos, valem como prova autónoma, mesmo que não sejam lidas ou reproduzidas[85].

A verdade é que, em nosso entender a leitura das transcrições das escutas telefónicas que fundamentam a tese da acusação é a melhor opção pois, visa garantir o cumprimento das máximas garantias do arguido como o direito de defesa e acreditamos que a leitura seja útil para o tribunal no sentido de poderem ser esclarecidas as transcrições juntas aos autos através da explicação do arguido.

Não se pode confundir meios de obtenção de prova com meios de prova. Os meios de obtenção de prova são mecanismos processuais capazes de proceder à recolha de elementos suscetíveis de evidenciar que os factos tidos por penalmente relevantes, ocorreram[86], enquanto que, os meios de prova têm "aptidão para serem, por si mesmo, fonte de convencimento"[87].

Em princípio, não há hierarquia no valor dos meios de prova, podendo qualquer facto ser provado com qualquer meio de prova, de acordo com o princípio da livre apreciação da prova. Isto é, não haverá vinculação entre certos factos e certos meios de prova, sendo apenas necessário que um seja idóneo para provar o outro.

Ainda que não se queira entrar de forma profunda neste tema, há que referir que há situações em que certos factos estão dependentes de certo tipo de prova. Quer isto dizer que, por exemplo, quando se quer demonstrar a paternidade por ser relevante para o crime em causa, está só ficará demonstrada com documento autêntico com força para o efeito.

1.10.1. Vícios

A prova, como se tem conhecimento, é um dos elementos mais significativos para o processo penal, no entanto, não vale de tudo para que se obtenha a descoberta da verdade, mas apenas aquilo que processualmente esteja estipulado, concretizando o princípio da dignidade humana.

Quanto a isto, Manuel da Costa Andrade assinala que "nem sempre o interesse do esclarecimento do crime e da perseguição de um suspeito será, só por si, bastante para dirimir

[85] A título de exemplo, Ac. do Tribunal da Relação de Coimbra, de 09/05/2012, proc. 222/09.9JACBR.C2, disponível em http://www.dgsi.pt. Acesso em 12.01.2025
[86] SANTOS, Manuel Simas; LEAL-HENRIQUES, Manuel; SANTOS, João Simas, (2011), *Noções de Processo Penal*, 2ª Ed., Lisboa: Rei dos Livros, pág. 223.
[87] SILVA, Germano Marques da, *Curso de Processo Penal...*, op. cit., pág. 280.

a ilícitude material indicada pela tipicidade das pertinentes formas de produção ou valoração de prova"[88].

Não sendo a recolha de prova arbitrária e ilimitada, a obtenção de prova adversa ao direito vigente tem irrefutavelmente consequências, principalmente quando em causa esteja o caráter lesivo de direitos fundamentais.[89]

O sistema de invalidades do CPP abrange quatro grupos, as provas proibidas, nulidades insanáveis, nulidades sanáveis e irregularidades.

A verdade é que, ainda que estejam todas tipificadas, parece-nos que a lei processual não delimita estes conceitos. Assim, é importante definir cada um dos conceitos, mais ainda quando o legislador, por vezes, não indica de forma expressa e concisa, quando está em causa uma prova proibida ou, por outro lado, uma "simples" nulidade processual referente a uma prova que, ainda assim, seja admissível (por não ser proibida).

Isto é, no artigo disposto para cada um dos grupos apresentados o legislador indica em que é que cada um se enquadra, mas, por exemplo, no artigo 224 do CPP, o legislador limita-se a determinar que "os requisitos e condições referidos nos artigos 222 e 223, respectivamente, são estabelecidos sob pena de nulidade", sem estipular a nulidade a que se refere, assim, é importante ter noção de:

1.10.1.1. Provas nulas (stricto sensu)

A sua primordial função é a de ordenamento do próprio processo e da maneira como este se desenvolve (quem, quando e em que medida é que pode praticar determinado acto processual). Ou seja, entendemos que "as nulidades a que se referem os artigos 134 a 139 do CPP reportam-se apenas aos vícios formais, isto é, à inobservância das prescrições legais estabelecidas para a prática dos actos processuais. [90]

Estas podem dividir-se em sanáveis ou insanáveis. As nulidades sanáveis podem regularizar-se e são dependentes de arguição, tal como indica a epígrafe do artigo 136 do CPP, enquanto

[88] ANDRADE, Manuel da Costa, *Sobre as Proibições...*, op. cit., pág. 15.
[89] SILVA, Germano Marques da, *Curso de Processo Penal...*, op. cit., p. 280.
[90] Ac. do TC de 06/07/1995, proc. 520/94, disponível em http://www.tribunalconstitucional.pt/ acesso em 12.01.2025

as nulidades insanáveis são mais raras e podem ser conhecidas em qualquer momento do processo.

1.10.1.2. Provas proibidas

Estão intrinsecamente ligadas à proteção dos Direitos Fundamentais, sendo consequência de vícios substanciais. Estas têm um regime específico no nº 2 do artigo 156 do CPP, apesar de na epígrafe referir métodos proibidos de prova, diz respeito a uma proibição de obtenção de prova.

Da análise do regime das proibições de prova, deve ser sempre acompanhado do nº 1 do artigo 156 do CPP, na medida em que prevê a nulidade das provas que forem obtidas através de abusiva intromissão na vida privada, no domicílio, na correspondência ou nas telecomunicações, assim como à proibição de ingerência nas telecomunicações, ressalvando os casos em que é passível de ser permitida, quando feita por autoridades públicas no âmbito de um processo penal.

Neste contexto, segue-se o entendimento de Germano Marques da Silva de que as proibições de prova ultrapassam o regime das nulidades processuais, já que, "a consequência essencial que a obtenção de uma prova proibida provoca vem a ser a sua não utilização e ao analisarmos as invalidades, classificámos as nulidades em insanáveis e dependentes de arguição. A nulidade correspondente à proibição de prova enquadrar-se-á nalguma delas? Cremos que não"[91].

No sentido de se considerarem realidades diferentes, e por isso, autónomas, o professor acrescenta ainda que, ao contrário da nulidade que fica sanada após trânsito em julgado da decisão, quando esteja em causa uma prova proibida, atendendo-se à gravidade desta, mesmo depois de transitada em julgado, a sentença pode ser alvo de revisão[92].

Por último, enquanto a lei processual penal, estabelece a possibilidade de repetição do acto considerado nulo, as provas proibidas não podem ser repetidas, uma vez que isso poderia dar resultado a nova lesão de direitos fundamentais, que é exatamente o que se pretende evitar.

Constata-se então a diferença entre os regimes, na medida em que, apesar do artigo 156 do CPP utilizar a palavra "nula", as provas proibidas não dependem de declaração de nulidade, não

[91] SILVA, Germano Marques da, *Curso de Processo Penal...*, op. cit., p. 126.
[92] Idem, pág. 127.

podendo, tal como a letra da lei determina, subsistir no processo e de alguma forma serem utilizadas, contrariamente às nulidades processuais que produzem efeitos até à declaração de nulidade. Concluindo-se então que as proibições de prova não seguem o regime das nulidades insanáveis ou os efeitos da nulidade de um acto.

Voltando para o tema que nos ocupa, todas estas questões resultam da necessidade de se perceber o sentido e a natureza que se deve atribuir à sanção de nulidade estabelecida no artigo 224 do CPP, quando desrespeitados os requisitos materiais e formais das escutas telefónicas: Deve ser entendida como proibição de prova, nos termos do nº 4 do artigo 156 do CPP? Ou, por outro lado, deve ser considerada nulidade sanável ou insanável, dos artigos 134 e ss do CPP?

Quanto à nulidade insanável não há qualquer dúvida que essa não será a opção a seguir, já que o artigo 135 do CPP apresenta um caráter fechado, não se subsumindo a violação desse artigo a nenhuma das situações elencadas. Ainda assim, da omissão do legislador advém a falta de consenso quanto à solução do problema, registando-se diferentes posições doutrinárias e na jurisprudência portuguesa.

Uma das posições defendidas entende que a solução será distinta conforme a violação que se pratique seja referente aos requisitos materiais para a realização de escutas ou aos requisitos formais. O incumprimento dos requisitos materiais ocasiona uma nulidade sanável, em que, se for arguida tempestivamente, a prova não é admitida, mas não sendo a nulidade arguida, é prova admissível[93].

A posição aqui adotada tem a ver com o facto de se considerar díspar o grau da gravidade da violação dos requisitos formais e materiais, porque não se entende, neste cenário, que o incumprimento de formalidades efetiva uma verdadeira violação de direitos fundamentais, sujeita a proibição de prova[94]. Isto é, a não observância desses requisitos não inviabiliza a validade do meio de prova em consideração.

Podemos sintetizar a defesa desta posição no entendimento de que, no artigo 223 do CPP, estão em causa essencialmente interesses procedimentais, como por exemplo, a celeridade e a

[93] Cfr. Ac. do STJ de 14/11/2007, proc. 07P3165 de 03/11/2016, proc. 63/10.0P6PRT.P1.S1, disponíveis em https//www.stj.pt.
[94] DIAS, Figueiredo, (2016). *Revisitação de algumas ideias-mestras da teoria das proibições de prova em processo penal.* Revista de Legislação e Jurisprudência, A.146:4000, pág. 3-16.

eficácia, sendo, nesta lógica, excessivo aceitar que, por exemplo, a entrega dos autos e relatórios ao Juiz, depois do prazo estipulado, tenha a mesma repercussão que a realização de uma escuta quanto a pessoas não abrangidas pelo crime ou sem autorização do juiz.

Figueiredo Dias defende esta tese, mas acrescenta a necessidade de se fazer uma interpretação da lei face ao caso concreto para que não se corra o risco de se registarem "violações do direito sérias, conscientes e objetivamente arbitrárias, através das quais tenham sido sistematicamente ignoradas garantias jurídicas fundamentais"[95].

Ou seja, esta análise do caso concreto, actua exatamente enquanto justificação para a utilização da tese anteriormente apresentada, na medida em que, não se evidenciando uma violação séria e concisa de direitos fundamentais, quando haja violação dos requisitos formais das escutas telefônicas, considera-se estar em causa uma nulidade sanável.

Por sua vez, a última corrente e a que consideramos adequada, admite não haver razão para defender a distinção da violação dos requisitos referidos no artigo 222 e 223 do CPP, sublinhando que nem a própria lei os distingue, pelo contrário, unifica-os no artigo 224 do CPP.

Como assinala Germano Marques da Silva "o referido artigo teve como fonte o artigo 271º do CPP italiano que dispõe que os resultados das intercepções não podem ser utilizados quando sejam obtidos fora dos casos consentidos na lei ou quando não sejam observadas as disposições relativas às formalidades das operações, não distinguindo a violação das condições de admissibilidade da das formalidades das operações"[96].

Deste modo, na nossa opinião, dúvidas inexistem de que a inobservância das regras inerentes às escutas origina um meio proibido de prova, por intromissão ilegal nas telecomunicações, por força do nº 4 do artigo 156 do CPP. Neste sentido, a prova não sendo obtida consoante as disposições legais que excepcionam a intromissão nas telecomunicações de terceiros, dá resultado à sua nulidade[97].

A nulidade aí estabelecida, acarreta a impossibilidade de utilização da prova, ou seja, a expressão "nulidade" "só pretende remeter o julgador para o regime das provas proibidas"[98].

[95] *Idem*, pág. 12.
[96] SILVA, Germano Marques da, *Curso de Processo Penal...*, op. cit., pág. 310.
[97] *Idem*, pág. 258.
[98] ALBUQUERQUE, Paulo Pinto de, *Comentário ao Código de Processo Penal...,* op. cit., pág. 550.

Não se aplica então o regime das nulidades, em razão desse não prejudicar as normas relativas às proibições de prova.[99]

Acresce-se, na nossa humilde perspectiva, que os requisitos formais e materiais das escutas telefônicas não visam apenas a celeridade processual e a própria eficácia do processo, como se defendeu na primeira tese exposta, pretendendo também impor determinadas garantias processuais fundamentais.

O legislador ao admitir o regime de escutas hoje tutelado, já consagra a possibilidade de se transpor certos direitos e valores fundamentais em função dos interesses constitucionalmente tutelados da vítima, como o da realização de justiça. Mas, não se pode esquecer que, havendo restrição de direitos constitucionalmente consagrados, há que respeitar os princípios da proporcionalidade, da necessidade e da adequação.

Sendo que, nesta óptica, o próprio legislador estabeleceu requisitos substantivos e formais para que se encontre exatamente um balanço entre a procura da verdade material face à exigência penal do caso concreto e a salvaguarda de direitos fundamentais, com fundamento no respeito pela dignidade humana, dentro da sua viabilidade.

Assim, o princípio da verdade material encontra-se aqui também consagrado pela possibilidade que nos é facultada pelo legislador de usufruir deste meio de prova, verificando-se, justificadamente, requisitos a serem cumpridos, estabelecendo assim um meio termo entre direitos e interesses bastante conflitantes.

O seu incumprimento acarreta uma maior transgressão dos valores e direitos fundamentais do arguido, do que aquela que é permitida pelo regime estabelecido. Por exemplo, sendo possível restringir o direito à inviolabilidade das telecomunicações, por se encontrarem preenchidos os respetivos requisitos, não quer dizer que não se tenham de garantir outros direitos do arguido, como o direito de defesa, através da possibilidade de examinar o auto de transcrição das comunicações, concluída a instrução.

Em suma, evidencia-se que o regime a aplicar é o das proibições de prova por estarem em causa imperativos constitucionais colocados em perigo, enquanto que, o regime das nulidades se funda, essencialmente, em razões de economia processual.

[99] Cfr. Nº 3 do artigo 134 do CPP.

Resta referir que, o nosso regime das nulidades das escutas telefônicas é semelhante ao Português, sucede, porém, que tanto no sistema português como no nosso, há necessidade de uma alteração legislativa que venha esclarecer a posição adotada pelo legislador, pois corre-se o risco de, *ad infinitum*, se aplicar um critério diferente consoante o entendimento obtido pelo aplicador da lei.

A Lei nº 9.296 de 24 de Julho, não estabelece uma sanção para as provas obtidas com violação dos requisitos materiais e formais das escutas telefônicas. No entanto, o artigo 5º do inciso LVI da CRFB veda expressamente o uso de provas obtidas por meios ilícitos, quando se refere que "São inadmissíveis no processo as provas obtidas por meios ilícitos". Deste modo, é compreensível que, desde que não ofenda a Constituição e as demais leis, a prova obtida por meio de escutas é válida no processo.

CAPÍTULO II

2. O DILEMA DA TRICOTOMIA DAS TEORIAS DOS CONHECIMENTOS FORTUITOS

2.1. Breve distinção entre conhecimentos fortuitos e conhecimentos de investigação

Importa antes de mais referir que, nem todos os conhecimentos decorrentes de legal intercepção e gravação de conversações e comunicações telefónicas são entendidos da mesma forma. O SERNIC ao efetuar a intercepção de comunicações telefónicas autorizadas pelo Juiz, por não ser possível que se faça uma seleção prévia e objetiva do conteúdo a ouvir, entra constantemente em contacto, com factos sem qualquer interesse processual.

Nunca se sabe quem e o que vai aparecer neste âmbito, sendo as escutas telefónicas, definitivamente, uma fonte extraordinária de conhecimentos. Ao contrário destes, podemos ter outro tipo de conhecimentos que já poderão ser relevantes, ainda que surjam para além daquilo que importará para a diligência em curso ou que, ainda que não tenham qualquer relação directa com o crime que se pretendia ver investigado quando se legitimou a realização da escuta telefónica, que com ele têm conexão.

Antes de centrarmos-nos na distinção dos conhecimentos de investigação e conhecimentos fortuitos, será conveniente atender aos conhecimentos ocasionais, já que estes compreendem ambos. Estes abrangem qualquer conhecimento que, até então, era desconhecido, independentemente de existir, ou não, conexão entre esses e o crime legitimador da escuta telefónica.

Inaugurando agora o tema que nos ocupa aqui, depreende-se facilmente que os conhecimentos fortuitos se encontram em contexto oposto aos conhecimentos de investigação, em virtude de estes serem obtidos no âmbito de determinado processo e que se imputam à própria investigação que aí decorre[100], ou seja, são factos que constituem o objeto da investigação em curso.

Manuel da Costa Andrade considera que se fala de conhecimentos de investigação quando "a investigação do crime originário já leva consigo a investigação dos crimes novos, como conhecimentos da(quela) investigação de que fazem parte"[101]. O que realmente define os

[100] ANDRADE, Manuel da Costa, *Sobre o regime processual penal das escutas telefónicas*, op. cit. pág. 301.
[101] Idem, pág. 306.

conhecimentos de investigação é a particular conexão entre os crimes que originaram a escuta telefónica e os novos crimes "expostos" por essa.

Para Fonseca de Aguilar, consideram-se conhecimentos de investigação "os factos, obtidos através de uma escuta telefónica legalmente efectuada, que se reportam ao crime cuja investigação legitimou a realização daquela ou a um outro delito (pertencente ou não ao catálogo legal) que esteja baseado na mesma situação histórica da vida daquele"[102].

Estes institutos jurídicos requerem uma intervenção processual diferente, essencialmente, no que diz respeito à valoração da prova, por isso é necessário estabelecer fronteiras entre eles. Apesar de se reconhecer que as definições anteriormente apresentadas se completam, não existindo consenso na identificação e delimitação destes conceitos, são vários os critérios adotados pela doutrina e jurisprudência portuguesa, decorrentes exatamente do silêncio assumido pelo legislador.

Pela importância já retratada que, tanto os conhecimentos fortuitos como os conhecimentos de investigação têm, não nos parece que possam continuar a ser vistos como conceitos indeterminados, sendo imperativo estabelecer um raciocínio lógico e concreto que os defina e distinga.

Neste seguimento, pertencem à categoria dos conhecimentos de investigação[103], os factos que se encontrem em concurso ideal e aparente com o crime que originou a escuta telefónica; também os ilícitos alternativos que estejam numa relação de comprovação alternativa de factos com o crime que suscitou a escuta telefónica; mas os crimes que, no momento em que é dedicada a escuta em relação a uma associação criminosa, surgem como constituindo a sua finalidade ou atividade; e, por fim, qualquer forma de comparticipação (autoria e cumplicidade), assim como as diversas formas de favorecimento pessoal, auxílio material ou receptação. [104]

[102]AGUILAR, Francisco Manuel Fonseca de, (2004). ***Dos conhecimentos fortuitos obtidos através de escutas telefónicas: contributo para o seu estudo no ordenamento jurídico alemão e português***, Coimbra: Almedina, pág. 19.
[103] ANDRADE, Manuel da Costa, *Sobre as Proibições...*, op. cit., pág. 306.
[104] *Idem,* pág. 306.

Resta aludir ao caráter não fechado, nem esgotante destas constelações elencadas por Manuel da Costa Andrade, sendo possível que outras circunstâncias possam ser aqui incluídas, designando-se também conhecimentos de investigação[105].

Aos conhecimentos fortuitos é atribuído um caráter residual, porque se definem negativamente face aos conhecimentos de investigação. Quer dizer que, serão conhecimentos fortuitos todos aqueles que não forem considerados conhecimentos de investigação.

A propósito, Fonseca de Aguilar, enquanto antagonista deste ponto de vista, justifica a sua posição precisamente com o facto de não concordar com o caráter não fechado e não taxativo[106] das circunstâncias elencadas, e considerar essencial que se estabeleça um critério objetivo e legal, tendo em conta a importância desta distinção, tanto a nível constitucional como processual.

Este critério legal pretende concretizar "a ideia de unidade de investigação processual entre o crime cuja investigação legitimou a vigilância telefónica e o crime (pertencente ou não ao catálogo) a que respeitam os resultados da mesma escuta"[107].

Demonstrado que a unidade de investigação processual e/ou a mesma situação histórica de vida são os conceitos chave do autor para a distinção entre uns conhecimentos e outros, entendeu que o critério objetivo e legal a estabelecer para se determinar as situações abrangidas pelos conhecimentos de investigação, seria o n º 1 do artigo 28 do CPP por este consagrar um conceito de "unidade processual" através da conexão de processos[108].

Sendo ainda que, neste artigo, as constelações típicas enunciadas por Costa Andrade conseguem encontrar cobertura legal já que, a 1ª constelação típica referente a casos de concurso ideal e aparente está abrangida pela alínea a) do n.º 1 do artigo 28 do CPP; a 2ª constelação típica respeitante à delitos alternativos também encontra fundamento de aplicação nessa alínea por se impor "a mesma qualificação *a fortiori* para os casos em que, tendo sido praticado apenas um crime, se trate de um facto em relação de alternatividade em face do facto

[105] *Idem*, pág. 306 e 307.
[106] Nesta circunstância, impõe-se à doutrina e à jurisprudência que estabeleçam essa delimitação, que poderá resultar numa "situação limite a *ad terrorem*, poderá esvaziar de tal maneira o conceito de conhecimento fortuito que deixe de fazer sentido qualquer referência à destrinça entre estes dois institutos processuais". AGUILAR, Francisco Manuel Fonseca de, *Dos conhecimentos fortuitos*..., op. cit., pág. 20.
[107] Neste sentido, Ana Raquel Conceição, por considerar também elementar a existência de um critério objetivo e entender que o caráter não fechado das constelações pode motivar a confusão jurídica entre os institutos jurídicos. CONCEIÇÃO, Ana Raquel, op. cit., pág. 232.
[108] AGUILAR, Francisco Manuel Fonseca de, *Dos conhecimentos fortuitos*..., op. cit., pág. 20.

legitimador da escuta telefónica"[109]; a 3ª constelação típica referente a casos de atividade ou finalidade de associação criminosa é suscetível de ser resolvida por aplicação da alínea b) e d) do nº 1 do mesmo normativo; a 4ª constelação típica concernente aos casos de comparticipação é reconduzida à aplicação das alíneas b) e c) do nº 1 do artigo 28 do CPP; e por fim, a 5ª constelação, que diz respeito a diversos casos de favorecimento pessoal, auxílio material ou receptação, é suscetível de determinar a aplicação das alíneas a) e c) do mesmo artigo, respectivamente, que estabelecem as situações ligadas à ocultação de crimes.

Construída esta ideia, os conhecimentos fortuitos serão identificados por exclusão de partes[110], tal como entende Costa Andrade na sua argumentação. Isto significa que, se os factos obtidos através de uma escuta não se enquadrarem em nenhum dos cenários elencados serão encarados como conhecimentos fortuitos.

Serão, portanto, conhecimentos de investigação, os factos ocasionalmente conhecidos através de uma escuta telefónica que se reconduzam ao crime que legitimou a escuta telefónica ou que se reconduzam a crimes que manifestem conexão com esse crime legitimador, suscetíveis de integrar uma das circunstâncias catalogadas no nº 1 do artigo 28 do CPP, independentemente de caber, ou não, no catálogo de crimes enunciado no nº 1 do artigo 222 do CPP.

Por último, mas não menos relevante para esta contenda, ainda que, aparentemente e equivocadamente se possa pressupor, o conhecimento descoberto de forma ocasional que não pertença ao catálogo estipulado no nº 1 do artigo 222 do CPP, não é pura e simplesmente por essa razão entendido conhecimento fortuito. Pode acontecer que o conhecimento de investigação diga respeito a conhecimento diverso dos definidos no catálogo, como se referiu previamente.

A delimitação dos conceitos de conhecimentos de investigação e de conhecimentos fortuitos depende sempre da análise dos fatores de conexão compreendidos no nº 1 do artigo 28 do CPP. Posto isto, só depois de se proceder a essa averiguação, se o crime ocasionalmente descoberto não puder ser subsumido à categoria dos conhecimentos de investigação por ser completamente alheio ao delito e à situação factual que originou a autorização da intercepção, é que é, por exclusão, considerado conhecimento fortuito.

[109] *Idem*, pág. 22.
[110] ANDRADE, Manuel da Costa, *Sobre as Proibições...*, op. cit., pág. 306.

2.1.1. Admissibilidade e valoração dos conhecimentos fortuitos: POSIÇÃO ADOPTADA

Apesar da recente revisão do pacote penal e processual penal, o nosso legislador permaneceu inerte quanto a admissibilidade e valoração de conhecimentos fortuitos. Não foi legislado se são ou não admissíveis os conhecimentos fortuitos e neste contexto não se pode falar, pelo menos a quanto a nós, de valoração dos mesmos.

Já o sistema português no nº 7 do artigo 187 do CPP admite e valora os conhecimentos fortuitos. Compreende-se da própria lei que existe uma regra geral de transmissibilidade, isto é, que aquele sistema admite, em regra, transferências de prova. Estabelece o nº 7 do artigo 187º do CPP de Portugal, a possibilidade e os limites da utilização extraprocessual de conhecimentos obtidos através de escutas telefónicas[111]. Admite-se, neste sistema, que os conhecimentos fortuitos sejam valorados em processo diverso, "em curso ou a instaurar"[112], "alargando por isso os requisitos de admissibilidade da escuta telefónica"[113].

A utilização dos chamados conhecimentos fortuitos — informações obtidas acidentalmente durante escutas telefónicas, sem relação com o crime que originou a sua autorização — suscita intensos debates doutrinários e jurisprudenciais**,** especialmente quanto à sua admissibilidade como meio de prova em novos processos penais. Três posições teóricas principais se formaram em torno do tema.

2.1.1.1.Teoria da admissibilidade ampla

Este ponto de vista baseia-se na valoração dos conhecimentos fortuitos sem qualquer ressalva ou limitação, os dois principais fundamentos deste pensamento são: a ideia de continuidade entre a produção de prova e a sua valoração; e a aplicação analógica do regime das buscas quanto aos conhecimentos fortuitos.

[111] Nesta perspectiva, notem-se as seguintes afirmações: "A lei regula o aproveitamento extraprocessual dos conhecimentos fortuitos […] " ALBUQUERQUE, Paulo Pinto de, *Comentário ao Código de Processo Penal...,* op. cit., pág. 511, nota 13; "Como vimos já, o nº 7 do 187º admite que os conhecimentos fortuitos possam ser utilizados noutro processo […] " SILVA, Germano Marques da, *Curso de Processo Penal...*, op. cit., pág. 256.
[112] Cfr. art. 187.º, nº 7 do CPP.
[113] SILVA, Germano Marques da, *Curso de Processo Penal...*, op. cit., pág. 256.

Entende-se que, no caso de apreensões, se o motivo da investigação for um, mas se encontrarem elementos de outros crimes, estes são apreendidos de forma legítima e o processo alarga-se no seu objeto.

A única coisa que se tem de ter em conta, relativamente às apreensões resultantes de conhecimentos fortuitos, será confirmar se em causa não estará um regime especial ou específico para que possam ser apreendidos, como é exemplo a correspondência. Ou seja, permite-se que sejam apreendidos todos os objetos deixados pelo agente ou que possam servir de prova à prática de um crime, mesmo que estes não se relacionem com o crime inicial em causa. É esta lógica que pretendem seguir os defensores desta tese quanto aos conhecimentos fortuitos resultantes de determinada escuta telefónica.

Ora, entendemos nós que é de desatender este raciocínio pois, para além de se encontrar em contradição com o especificado no nº 7 do artigo 187º do CPP de Portugal, frustraria a distinção que se assenta entre o conceito de conhecimento fortuito e conhecimento de investigação, já que essa distinção importa essencialmente para a valoração de cada um dos conhecimentos, como atrás nos referimos.

Nesse caso, havendo esta equiparação, a valoração dos conhecimentos fortuitos exigiria apenas que a escuta referente ao crime que a originou fosse lícita, tal como acontece com a valoração dos conhecimentos de investigação. Esta situação não apresenta ser uma solução adequada por duas razões:

I. Os conhecimentos de investigação, por se integrarem na "unidade processual" do crime que fundamentou a realização da escuta telefónica e estarem interligados com a matéria factual que nesse caso estará a ser investigada, foram, ainda que de forma indireta, escrutinados quanto aos pressupostos do artigo 187º do CPP de Portugal e ao princípio da proporcionalidade antes do despacho fundamentado do juiz que permitiu aquela escuta.
Admitir a valoração dos conhecimentos fortuitos de forma absoluta e incondicional, sem que fossem submetidos a análise por parte do juiz, causaria uma devassa injustificada e ilícita de diversos direitos fundamentais, como o direito à inviolabilidade das telecomunicações e o direito à reserva da intimidade da vida privada. Assim como, determinaria uma violação do princípio da reserva de lei, já que a restrição de direitos, liberdades e garantias só se pode verificar por via da lei.

Tudo isto se deve, uma vez mais, ao facto dos conhecimentos fortuitos não terem a conexão com o crime impulsionador da escuta telefónica que se impõe aos conhecimentos de investigação, não tendo sido previamente analisados, terão de o ser antes da sua admissão e valoração.

II. Esta corrente admite que se valorem tanto conhecimentos fortuitos enunciados como não enunciados, sendo assim permitido que se admitam e valorem conhecimentos fortuitos relativos a crimes que não se integram no catálogo de crimes que admitem as escutas telefónicas.

Na eventualidade disto acontecer, estar-se-ia a dar a possibilidade de se realizarem escutas com o propósito de se alcançarem conhecimentos de crime diverso ao que motivou a escuta e não admissível pelo regime das escutas. Isto é, a escuta pode ter por base um crime enunciado, mas tencionar-se adquirir prova de crime diverso não enunciado, traduzindo-se, na nossa ideia, num completo contorno à lei.

Esta conjuntura, tal como afirma Francisco Aguilar[114] e Manuel Guedes Valente[115], poderia incentivar as autoridades responsáveis pela investigação criminal a dedicarem-se à descoberta de eventuais delitos diversos da finalidade probatória de determinada escuta telefónica. Mais ainda, estando em causa conhecimentos fortuitos, não será sequer necessário que exista a conexão entre os crimes, tornando ainda mais propícia a "tentação" das autoridades de investigação criminal em procurar descobrir o cometimento de outros crimes além daquele que sustentou a admissão da escuta telefónica.

2.1.1.2. Teoria da inadmissibilidade absoluta

Damião da Cunha, um dos principais defensores desta teoria, sustenta o seu raciocínio no facto destes conhecimentos não terem sido sujeitos ao crivo do juiz, sem que este, dessa forma, admitisse a sua intercepção e gravação[116], uma vez que essa autorização é um dos requisitos para a admissibilidade da escuta telefónica.

---

[114] AGUILAR, Francisco Manuel Fonseca de, *Dos conhecimentos fortuitos*..., op. cit., pág. 42.
[115] VALENTE, Manuel Guedes, *Conhecimentos fortuitos: A Busca de um Equilíbrio Apuleiano*, Almedina, 2006, pág. 111.
[116] O Prof. Doutor Damião da Cunha manifestou a sua discordância em relação à utilização dos conhecimentos fortuitos como meio de prova. Na sua opinião, a utilização desses conhecimentos pode padecer de inconstitucionalidade. São meios de prova que não foram objecto de despacho fundamentado de autorização.

Para estes, os conhecimentos fortuitos que venham a ser valorados, destoantes do crime que fundamentou a escuta são considerados nulos, gerando uma prova proibida. Sob o princípio da reserva de lei, só serão válidos os conhecimentos de investigação, exactamente por não haver tipificação legal quanto à admissibilidade de outros e por estar em causa um método oculto de obtenção de prova que derroga de forma "qualificada", se assim pudermos dizer, vários direitos.

Para sustentar esta teoria faz-se referência ao requisito de admissibilidade da escuta telefónica por parte do juiz, determinando que "só em relação à investigação do caso em concreto se formula o juízo de idoneidade e subsidiariedade que constitui o crivo da admissibilidade da escuta"[117]. Então, os conhecimentos fortuitos que venham a ser valorados, destoantes do crime que fundamentou a escuta são considerados nulos, gerando uma prova proibida.

Do acima exposto, depreende-se que o legislador nacional assim como o brasileiro é adepto desta teoria, pois desvalorizou por completo a admissão de conhecimentos fortuitos. Na medida em que, o facto de não existir um preceito na nossa lei processual que admita, de forma expressa, a valoração total ou parcial dos conhecimentos fortuitos e, face a essa inexistência não se pode fazer uma interpretação extensiva ou análoga do artigo 222 do CPP para supri-la, por essas ocasionarem um desrespeito pela CRM, já que em nosso entender seria o intérprete e, não o legislador, a estabelecer uma restrição a um direito, liberdade e garantia.

Ou seja, tendo em conta o dano que as escutas telefónicas representam para os cidadãos, nomeadamente no que toca a direitos constitucionalmente consagrados como já se evidenciou, só se poderá considerar legítimo os conhecimentos que derivem diretamente do crime que se pretende ver investigado, isto é, aquele que justificou a escuta telefónica, uma vez que só estes se encontram acautelados na lei.

Assim, nos termos estabelecidos pelo legislador nacional, entendemos que só vai impender sobre os agentes da SERNIC a obrigatoriedade de transmitirem a notícia desse crime ao MP, procedendo este à abertura da instrução, relativamente a crimes públicos, assegurando-se o princípio da oficialidade, pois por crimes semi-públicos e particulares o MP não deve tomar a

[117] A autorização para a realização de determinada escuta telefónica "esgota-se na obtenção de conhecimentos relativos à investigação que originou a escuta". AGUILAR, Francisco Manuel Fonseca de, *Dos conhecimentos fortuitos*..., op. cit., pág. 77.

dianteira. Cremos que esta teoria compromete a eficácia da investigação criminal**,** especialmente quando os dados obtidos fortuitamente revelam crimes graves ou iminentes.

2.1.1.3. Teoria da admissibilidade condicionada (posição intermediária)

Esta é a tese que encontra maior defesa na ordem jurídica portuguesa, quer pela doutrina, assim como pela jurisprudência, existindo inúmeros autores com variadas correntes a considerar.

Manuel da Costa Andrade ocupa, a posição dianteira neste debate, definindo que para haver valoração de conhecimentos fortuitos, estes teriam de se remeter a um crime de catálogo previsto no nº 1 do 187º do CPP de Portugal concluindo que isto "viria a converter-se num dos tópicos mais pacíficos entre os tribunais e os autores e, nessa medida, numa como que exigência mínima do regime processual penal dos conhecimentos fortuitos"[118].

Costa Andrade, entende que, quanto aos conhecimentos fortuitos, é impreterível que se tivesse em consideração "o juízo de proporcionalidade a que o regime das escutas telefónicas presta homenagem"[119]. Significa isto que, a admissibilidade e valoração de um conhecimento fortuito está dependente de um juízo de ponderação dos interesses em causa.[120]

Nesta lógica, e não podendo descurar a danosidade e o caráter profundamente abusivo das escutas telefónicas em relação aos direitos, liberdades e garantias do cidadão, não se poderá também valorar conhecimentos fortuitos se não ficar comprovada a indispensabilidade da sua utilização no processo autónomo, instaurado ou a instaurar, atribuindo-lhe assim um "estado de necessidade investigatório"[121].

Isto é, há que fazer um juízo hipotético em que o juiz avalia se, quando admitiu determinada escuta telefónica tivesse informações sobre a possível prática de outro crime de catálogo, determinaria a execução de escuta telefónica com vista à sua investigação.

Tanto Germano Marques da Silva[122], como Paulo Pinto de Albuquerque[123], apoiam a interpretação realizada por Costa Andrade, reconhecendo que se possam admitir e valorar conhecimentos fortuitos que se incluam naqueles que o legislador entendeu tipificar para este

[118] ANDRADE, Manuel da Costa, *Sobre as Proibições...*, op. cit., pág. 403.
[119] *Idem*, pág. 406.
[120] *Idem*, pág. 312.
[121] VALENTE, Manuel Guedes, *Conhecimentos fortuitos...,* op. cit., pág. 118
[122] SILVA, Germano Marques da, *Curso de Processo Penal...*, op. cit., pág. 255 e 256.
[123] ALBUQUERQUE, Paulo Pinto de, *Comentário ao Código de Processo Penal...,* op. cit., pág. 511, nota 14.

efeito, realização de escuta telefónica como método de obtenção de prova, e que demonstrem ser imperiosos para a prova do crime sobre que versa a investigação.

Quanto à delimitação subjetiva, Germano Marques da Silva, reconhece a valoração dos conhecimentos fortuitos que digam respeito tanto ao suspeito/arguido, como a terceiro, na condição do meio de comunicação através do qual se adquiriu o conhecimento ter sido utilizado pela pessoa a quem a escuta se refere.

Por sua vez, Paulo Pinto de Albuquerque, neste contexto subjetivo, determina que, para que sejam valorados os conhecimentos fortuitos, basta que a pessoa escutada seja passível de se "encaixar" no catálogo de alvos do nº 4 do artigo 187º do CPP de Portugal.

Manuel Guedes Valente[124], acompanha também a concepção acima apresentada, considerando que a valoração dos conhecimentos fortuitos está subordinada à licitude da escuta em que foram obtidos e que estes têm de ter em vista a investigação de um dos crimes de catálogo do artigo 187º do CPP de Portugal, isto é, suscetível de legitimar a execução de uma escuta telefónica.

Quanto à questão de se saber sobre quem podem incidir estes conhecimentos suscetíveis de valoração, o autor considera que os factos em causa têm de se relacionar com o suspeito da escuta telefónica que está a ser realizada ou com qualquer terceiro, com a condição de que este seja participante nessa comunicação[125].

Significa isto que, se o terceiro não for interveniente dessa escuta telefónica não poderá ser valorado o conhecimento fortuito que a ele diga respeito. A não ser, porém, como indica o autor, que seja cúmplice ou comparticipante do crime, senão esse apenas poderá dar resultado à notícia do crime[126].

Importa referir que, quando não se encontrem cumpridos os requisitos essenciais à sua valoração probatória e não possam ser probatoriamente valorados, impende sobre os OPC a obrigatoriedade de transmitirem a notícia desse crime ao MP, procedendo este à abertura do inquérito, assegurando-se o princípio da oficialidade.

Desta situação excetuam-se aquelas em que estejam em causa crimes semi-públicos ou particulares. Isto porque, os crimes semi-públicos são dependentes da apresentação de queixa

[124] VALENTE, Manuel Guedes, *Conhecimentos fortuitos...,* op. cit., pág. 133-136.
[125] Idem, pág. 133.
[126] Idem, pág. 133.

por parte dos ofendidos ou de quem a lei legitime para tal e, os crimes particulares dependem da apresentação de queixa ou de participação do ofendido, tendo esse de se constituir assistente.

Ademais, a admissão de conhecimento fortuito que se remeta à prova de crime não previsto no nº 1 do artigo 187º do CPP de Portugal, como analisa André Lamas Leite, violará o princípio da proporcionalidade do nº 2 do artigo 18 da CRP, uma vez que o catálogo de crimes sujeitos a escuta telefónica foi delimitado com base numa determinada gravidade conjugado com os interesses em causa quando se recorre a essa medida – por exemplo, eficácia do *ius puniendi* e, por outro lado, a garantia dos direitos, liberdades e garantias fundamentais dos cidadãos, nomeadamente do suspeito/arguido.

Quer dizer que, se se permitisse a admissão e a valoração de conhecimentos fortuitos fora deste catálogo, não haveria esta ponderação, sendo possível determinar as mesmas consequências para qualquer conhecimento fortuito independentemente do crime em causa, mesmo que esse não revelasse a gravidade exigida para que possam outros direitos ser também derrogados.

Além disto, este caminho poderia resultar num abuso de poder por parte das entidades a quem a investigação está entregue, podendo valer-se de um crime de catálogo para, única e exclusivamente, descobrir crimes fora desse domínio.

Finalizando, parece-nos que esta opção seja lógica por ser necessário que se proceda da mesma forma que se procede para a admissão de uma escuta telefónica e essa só pode ser efectuada se tiver por base um dos crimes previstos pelo legislador, esse será o mesmo critério para que se admitam e valorem os conhecimentos fortuitos.

Abordadas as teorias supra, há que saber quais são os requisitos impostos para que um conhecimento fortuito relativo a crime enunciado seja admitido e valorado. Entendemos que, no fundo os requisitos de admissão e valoração de conhecimentos fortuitos serão semelhantes aos requisitos exigidos para o facto que ordenou a realização da escuta.

No que diz respeito à indispensabilidade, exige-se que a diligência seja "indispensável para a descoberta da verdade".

Esta indispensabilidade para a prova ou para a descoberta da verdade material, traduz-se num dos requisitos de admissibilidade e valoração dos conhecimentos fortuitos, em que se impõe que não haja um outro método de obtenção de prova, menos intrusivo e menos restritivo de

liberdades, direitos e garantias dos cidadãos, apto ao apuramento dos factos penalmente relevantes.

Já quanto aos sujeitos, entende-se de forma lógica, que o legislador tencionou incluir os conhecimentos fortuitos de qualquer pessoa, incluindo terceiros, desde que esses advenham de intercepção de meio de comunicação utilizado por uma das pessoas referidas no nº 4 do artigo 187 do CPP de Portugal e sinalizada no despacho de autorização da escuta, ou seja, basta a participação de terceiro na conversa telefónica com o suspeito, com o arguido, com a vítima ou com o intermediário, para que o conhecimento fortuito que daí resulta possa ser valorado.

Em sentido oposto, há quem descarte a valoração de conhecimentos fortuitos contra terceiros apartados do processo, justificando a sua posição com o facto destes se encontrarem fora do nº 4 do artigo em questão e esse referir "só podem ser autorizadas (…) contra", não sendo admissível a valoração de conhecimentos fortuitos a pessoa diversa da ali estipulada.

A opção que nos parece razoável para este efeito é a de que a condição essencial, segundo a lei, para que se possam valorar conhecimentos fortuitos, é que na conversa de que esses advieram tenha participado pessoa que se enquadre no nº 4 do artigo 187º do CPP de Portugal e que tenha sido identificada aquando do despacho de autorização da escuta telefónica.

Uma vez que, é essa autorização por parte do JIC que legitima a intromissão nas conversações ou comunicações telefónicas. A par disto, deve-se fazer uma interpretação restritiva, por ser uma norma que restringe direitos fundamentais.

Posto isto, acreditamos ser mais proveitoso, a interpretação que realmente o legislador pretendeu aludir, a valoração dos conhecimentos fortuitos independentemente da pessoa que se reporta esse conhecimento, mesmo que o terceiro não participe na conversa,[127] exigindo-se apenas a participação na conversa por parte de pessoa tipificada no nº 4 do artigo e indicada no despacho de autorização, como se viu.

André Lamas Leite, tende a seguir este entendimento, afirmando que "será de admitir a valoração dos conhecimentos fortuitos sempre que se possa concluir que, se o Tribunal, no momento em que ordenou a dada escuta, tivesse elementos para suspeitar da prática, pelo arguido ou por um terceiro, de outros crimes que admitissem o recurso às escutas telefónicas,

[127] TEIXEIRA, Carlos Adérito, (2008). *Escutas telefónicas: a mudança de paradigma e os velhos e novos problemas, Revista do CEJ, nº 9, pág.* 275.

teria ordenado a execução desse meio de obtenção de prova"[128]. Quer isto dizer que os conhecimentos fortuitos podem ser imputados tanto a um, como a outro.

Concluímos, assim, pela intenção do legislador em admitir a valoração dos conhecimentos fortuitos contra terceiros, independentemente da sua participação na conversa, desde que nessa tenham participado o suspeito ou outra qualquer pessoa do artigo nº 4 do artigo 187º do CPP de Portugal.

A valoração condicional dos conhecimentos fortuitos é, sem dúvida, a posição que é seguida pelo legislador português, em que se pretende estabelecer uma harmonia entre valores sujeitos à colisão entre si, subordinando essa valoração ao cumprimento de determinados requisitos, nomeadamente os requeridos para a autorização da execução de escutas telefónicas, com vista à sua adequação e proporcionalidade.

Assim, tal como outras normas que regem o regime jurídico das escutas telefónicas, o nº 7 do artigo 187º do CPP de Portugal também incide sobre direitos fundamentais dos cidadãos e o interesse da sociedade na realização da justiça penal, seja através do cumprimento das normas, como a responsabilização de quem as viole.

2.1.1.4.Posição adotada neste trabalho

Relativamente a admissibilidade e valoração de conhecimentos fortuitos, acreditamos que o legislador nacional ao não permitir qualquer aproveitamento de conhecimentos fortuitos, pode conduzir a uma violação do Estado de Direito Democrático, já que poderá resultar na impossibilidade de se assegurar uma tutela efetiva de certos direitos dos cidadãos e do próprio Estado.

Para além disto, também não nos parece coerente que se determine, neste caso, aos agentes do SERNIC que ignorem os conhecimentos que adquirirem durante uma escuta telefónica, ainda que estes não digam respeito à investigação em causa e não preencham determinados requisitos, já que isso contraria e desrespeita a sua própria missão e responsabilidade. Assim, o mínimo exigível é que estes conhecimentos possam ter relevância enquanto notícia de um crime público.

[128] LEITE, André Lamas, Separata da *Revista da Faculdade...,* op. cit., pág. 40 e 41.

Considerando os princípios constitucionais moçambicanos, especialmente o da proporcionalidade, e as melhores práticas nos ordenamentos comparados, adota-se aqui a posição intermediária da admissibilidade condicionada.

A escuta telefónica não pode servir de pretexto para devassa generalizada da vida privada. Todavia, não se deve ignorar a possibilidade de aproveitamento de informações relevantes obtidas de forma incidental, desde que:

- Haja relevância penal e gravidade concreta do facto fortuitamente revelado;
- Seja promovido o controle judicial imediato quanto ao novo conteúdo;
- Seja garantido contraditório e ampla defesa ao visado.

Essa solução evita tanto o desperdício probatório quanto a violação de direitos fundamentais, promovendo uma aplicação ponderada e constitucionalmente adequada da escuta telefónica como meio de obtenção de prova.

CAPÍTULO III

3. A PROBLEMÁTICA DA PROVA DIGITAL NO PROCESSO PENAL

3.1. Generalidades

Antes de mais, importa referir que a mesma tutela constitucional e processual conferida as escutas telefónicas, como atrás nos debruçamos, é também conferida a prova digital.

O CPP, assim como demais legislação avulsa não nos faculta o conceito de prova digital enquanto que tal, sendo, portanto, para o efeito recorrer a doutrina. Benjamim Rodrigues, refere que " A prova electrónico-digital pode definir-se como qualquer tipo de informação, com valor probatório, armazenada em qualquer dispositivo de armazenamento digital ou transmitida em sistemas e redes informáticas ou redes de comunicações electrónicas, privadas ou publicamente acessíveis, sob a forma binária ou digital". [129]

A Prova Digital, tal como qualquer outra prova, tem de reter o seu valor probatório, para que este seja susceptível de ser valorada pelo julgador, e crie a sua convicção de veracidade do facto. Por sua vez, a diferença que se encontra entre esta e as demais provas, é a característica do formato digital. Sendo assim, pode esta ser armazenada ou transmitida também no meio digital, seja num computador, ou qualquer dispositivo capaz de conservar com segurança a Prova.

O formato digital desta prova, responde também à necessidade que a sociedade actual vai apresentando, no combate à criminalidade. Torna-se então possível a localização, identificação, e delimitação dos infractores, no que diz respeito a crimes que pela sua natureza tecnológica, seria impossível ou muito complicado, extrair uma prova sustentada, capaz de criar convicção, de todo o modo operacional praticado pelos executantes do crime ou ilícito[130].

A importância no que concerne ao combate da criminalidade informática e demais, é absoluta, e especialmente sustentada, quando ultimamente se tem produzido, uma transferência criminosa para a Internet, resultando em que cada vez mais utilizadores observam a internet como meio para as suas práticas criminosas, ou mesmo a arriscar-se na consumação de crimes,

[129] RODRIGUES, Benjamim Silva, 2009, *Direito Penal. Parte Especial, I, "Direito Penal Informático-Digital*", Coimbra, Coimbra Editora, pág. 39.
[130] Idem, pág. 49.

o que por outros meios não praticariam, ou pelo menos com a mesma certeza de que se torna complicada a identificação do agente, e do local.

Nos crimes informáticos, é necessária, e praticamente exclusiva a utilização da Prova Digital, no sentido em que o ilícito é praticado em ambiente electrónico, e quer em fase de investigação, ou de produção de prova, a prova a recolher, é esta apreendida de algum dispositivo electrónico, seja computador, servidor, telemóvel ou equivalente.[131] Certo é que com os demais meios de prova tradicionais, não seria então possível dar resposta à necessidade de demonstrar de forma probatória a existência ou não da conduta criminosa.

Ressalta Dario José Kist que a prova digital, ao possuir uma realidade própria, muito diferente dos demais meios de provas - perceptíveis aos sentidos, demanda a utilização de métodos compatíveis e diferenciados de investigação, obtenção e armazenamento.[132]

Isso ocorre em virtude das suas características peculiares, entre as quais, Denise Provasi Vaz destaca a imaterialidade e desprendimento do suporte físico originário, volatilidade, suscetibilidade de clonagem e fácil dispersão e, por fim, a necessidade de intermediação de equipamento para ser acessada.[133]

São características da prova digital a imaterialidade, no sentido de que são dados eletrônicos armazenados em dispositivos físicos, contudo, independentes desses e que podem ser transmitidos sem a necessidade de movimentação física. São voláteis pois, facilmente se submete a alterações ou desaparecimento, bastando a modificação da sequência numérica que o compõe. As provas digitais são ainda susceptíveis de clonagem pois, podem ser facilmente copiadas e transmitidas a outros dispositivos eletrônicos, oferecendo risco à preservação da originalidade do arquivo utilizado como meio de prova. São prova de fácil dispersão na medida em que podem ser transmitidas a qualquer dispositivo eletrônico.

3.2. Regime Jurídico

---

131 NEVES, Rita Castanheira, (2011). *As Ingerências nas Comunicações Eletrônicas em Processo Penal: Natureza e Respectivo Regime Jurídico do Correio Eletrônico enquanto Meio de Obtenção de Prova*. Coimbra: Coimbra Editora, pág. 170.

132 KIST, Dário José. *Prova digital no processo penal*. Leme (SP): JH Mizuno, 2019. pág. 117.

133 VAZ, Denise Provazi. Provas Digitais no Processo Penal: *formulação do conceito, definição das características e sistematização do procedimento probatório*. Orientador António Scarance Fernandes. 2012. 198 f. Tese (Doutorado em Direito) - Faculdade de Direito da Universidade de São Paulo. São Paulo. 2012, pág. 67.

A necessidade de actualização normativa face aos avanços tecnológicos resultou no alargamento do conceito de escutas a outros meios de comunicação electrónica. A Prova digital, no que diz respeito ao regime jurídico, é entendida no artigo 225 do CPP.

Por sua vez, não encontramos neste artigo um regime legal especifico relativo à Prova Digital, mas antes uma remissão para o regime jurídico das escutas telefônicas. Tendo o artigo 225 do CPP estendido o seu regime às "conversações ou comunicações transmitidas por qualquer meio técnico diferente do telefone, designadamente telemóvel, correio electrónico ou outras formas de transmissão de dados por via telemática, e à interceptação das comunicações entre presentes".[134]

A mistura de conceitos e, consequente, remissão para o regime das escutas telefónicas, originou, na doutrina e jurisprudência portuguesa, elevadas críticas e consideráveis dúvidas pois, os problemas levantados na necessidade de uma intercepção de uma Prova Digital, são muitas vezes, diferenciados das exigências das escutas telefónicas. [135]

O que se pode considerar como conversações transmitidas por qualquer meio técnico diferente do telefone? A verdade é que pode abranger, hoje em dia, qualquer tipo de programa de mensagens instantâneas, tal como o *Twitter, Whatsapp*, *Telegram*, *Instagram, Facebook* entre outras.[136] Ao mesmo tempo, evidencia-se a diversidade da natureza do telefone e do correio eletrônico ou outras formas de transmissão de dados, desde logo pela destrinça entre a palavra falada e escrita, já que "numa conversação telefónica, a palavra é dirigida para se extinguir naquele mesmo tempo e propósito. Não é suposto haver qualquer tipo de perpetuação do que vai dito. [137]

Ao contrário, quando se escreve, sabe-se que se eterniza uma mensagem, seja privada ou não"[138]. Existindo, neste domínio, ao inverso da palavra falada que se extingue no momento em que finda, o acesso à palavra escrita que fica à disposição de quem a obtém, é necessário determinar o momento em que se consuma uma comunicação. Quer isto dizer que, o correio electrônico pode ser acedido em diversos momentos:

---

[134] Cfr. Artigo 225 do CPP.
[135] ANDRADE, Manuel da Costa, *"Bruscamente no Verão Passado"...,* op. cit., pág. 156-159.
[136] Idem, pág. 178.
[137] Idem, pág. 178.
[138] NEVES, Rita Castanheira, *As Ingerências nas Comunicações Eletrônicas em Processo Penal: Natureza e Respectivo Regime Jurídico do Correio Eletrônico enquanto Meio de Obtenção de Prova*. Coimbra: Coimbra Editora, 2011, pág. 173.

1. No momento da intercepção da comunicação, em que A está a enviar determinada mensagem a B;
2. No sistema informático de quem envia/recebe a mensagem (por exemplo, a caixa de entrada do e-mail) ou, até mesmo, de sistemas informáticos de arquivo (conhecidas como *clouds*).

Conforme entendimento de Manuel da Costa Andrade, quando o acesso é realizado já em sistemas informáticos (por exemplo no computador de A), após a sua leitura e arquivamento, já não se está perante uma comunicação activa, em tempo real, não havendo comunicação telefónica ou equiparada, não se aplicando, por sua vez, o regime das escutas[139]. Não parece que faça sentido aplicar um regime que, na sua própria letra, se refere a "intercepção" a algo que não se trata já de uma comunicação, mas sim de um ficheiro gravado, uma vez que tal comunicação se encontra finda. Não havendo comunicação, não há intercepção, logo não parece coerente aplicar o regime da extensão.

Quanto às conversas entre presentes, a doutrina questiona, desde logo, a opção do legislador em optar por aplicar o regime das escutas telefónicas ao invés de conceber um regime próprio mais exigente."[140]

Ora, o Direito à reserva da intimidade privada e familiar e o Direito à inviolabilidade do domicílio, na Constituição da República, restringem quaisquer intromissões nessa esfera. Desta forma, segundo Paulo Pinto de Albuquerque, a intercepção das comunicações entre presentes, tidas no domicílio do suspeito, é considerada inconstitucional[141]. Podemos assim concluir que, há violação do regime de proteção do domicílio quando são captadas conversas entre presentes, dentro do domicílio, sem prévia autorização para tal. Os meios de obtenção de prova utilizados no domicílio têm de respeitar essas regras.

O legislador processual penal deu um contributo decisivo para a incerteza e para a insegurança jurídicas e dificultou a tarefa dos aplicadores da lei ao remeter o regime da prova digital para as escutas telefônicas.

Com efeito, a desconsideração dos interesses da investigação era, ainda, visível na impossibilidade de interceptar as comunicações eletrônicas ou sequer de obter os respectivos

[139] ANDRADE, Manuel da Costa, ***"****Bruscamente no Verão Passado"...,* op. cit., pág. 156-159.
[140] Idem, pág. 156-159.
[141] ALBUQUERQUE, Paulo Pinto de, *Comentário ao Código de Processo Penal...,* op. cit., pág. 580.

dados de tráfego, no caso de crimes informáticos ou de injúria, ameaça, coação ou devassa da vida privada cometidos por via informática. [142]

Devido àquela cláusula de extensão, estes crimes também não beneficiavam destes meios, excepcionais, de investigação. O legislador esqueceu assim as situações em que, paradoxalmente a intromissão é mais necessária e legítima, tornando quase impossível investigar estes crimes com sucesso.

Importa referir que, no sistema português também existe a cláusula de extensão a semelhança da nossa, no artigo 189º do CPP. Não querendo enveredar à conceitos técnicos, na previsão do art. 189º do CPP de Portugal, prevê a extensão do regime das escutas telefónicas ao correio eletrônico mesmo que este se encontre "guardado em suporte digital". Ora, cumpre-nos dizer que as ingerências nas comunicações, por exemplo telefónicas, ocorrem em tempo real, isto também poderá acontecer com o correio eletrônico e as SMS quando estas se encontrem em trânsito. No entanto, surge a dúvida de saber como se processa esta ingerência quando a mensagem chega ao domínio do seu destinatário e já estiver lida?

De acordo com Rita Castanheira Neves, não é possível uma intercepção pois, "chegada ao seu destino final e depois de aberta e lida, a mensagem de correio eletrônico já não é nenhuma telecomunicação, ela é já apenas um suporte informático. Já não está em trânsito. Já não é passível de ser interceptada"[143].

Pelo acima referido e seguindo o pensamento de Manuel da Costa Andrade acima exposto, pensamos que andou melhor o legislador nacional ao não prever a extensão do regime das escutas telefônicas ao correio eletrônico guardado em formato digital, não entendemos o porquê de o legislador português submeter ao regime das escutas telefónicas um ficheiro que por si só já não constitui uma comunicação. Desta forma, não haverá uma ingerência propriamente dita o que poderá ocorrer será uma busca ou gravação do documento.

Para além da cláusula de extensão, em Portugal, a prova digital está ainda formalmente regulada, na Lei 32/2008, de 17/07 e na Lei 109/2009, de 15/09, a lei do cibercrime. Apesar de, com três leis existirem problemas teóricos e práticos que se levantam no sistema português

[142] Idem, pág. 591.
[143] NEVES, Rita Castanheira, "As ingerências nas Comunicações eletrônicas em Processo Penal", *ob. cit.* pág. 182 e ss.

atinentes a prova digital, importa referir que o nosso sistema que conta apenas com um artigo levanta muitos mais problemas teóricos e práticos do que os que se suscitam em Portugal.

De facto, a teia legislativa portuguesa é muito complexa, mas apesar disso, nalgum momento parecem convergir e superar-se sucessivamente, tornando menos dramática a tarefa do intérprete, pensamos nós que, na situação em que se encontra o sistema português o grande calcanhar de Aquiles para além de questões técnicas obviamente é a inconveniência prática, para os operadores judiciários, de ver sistematizados todos os normativos referentes a um sector especifico da criminalidade, entendimento este também partilhado por Rita Castanheira.[144]

Não foi aproveitada a oportunidade de inovar e escolheu-se uma via incerta, onde, nem a letra, nem o seu espírito, nem, tão pouco, a sua história fornecem a bússola necessária para encontrar o caminho mais seguro, aliado ao facto de não existir ainda no País jurisprudência sobre a matéria. O nosso regime jurídico relativo a prova digital, tal como se encontra não é capaz de responder a questões como: a preservação da Prova Digital, o regime de apreensão da correspondência, a entidade competente para o armazenamento da prova digital, os prazos, a revelação expedita de dados de tráfego, entre muitas outras.

Posto isto, entendemos ser de crucial importância falar e abordar um pouco sobre a convenção do cibercrime do conselho da Europa, a qual Moçambique não aderiu, a lei nº 109/2009 de 15/09, que aprova a lei do cibercrime portuguesa e a Lei nº 32/2008, de 17/07, que aprova a conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas portuguesa, para se possível inspirar o nosso legislador, (pois apesar de não serem perfeitas, conseguem dar resposta a muitos questionamentos) e de certa forma contribuir para integração de melhores práticas para os nossos interpretes e aplicadores da lei.

3.2.1. A Convenção de Budapeste

A convenção do Cibercrime, ou também intitulada de 'Convenção de Budapeste', é um acordo assinado entre vários Estados-membros pertencentes à união europeia, e não só, que foi adoptada com o intuito de controlar, e regular, os vários crimes cometidos através de dados electrónicos. A convenção foi adoptada pelo Comité de Ministros do Conselho da Europa na Sessão nº 109 de 08 de Novembro de 2001. Só posteriormente, em 23 de Novembro do mesmo

[144] NEVES, Rita Castanheira, ob.cit. pág. 182 e ss.

ano, foi aberta à assinatura em Budapeste, tendo entrado em vigor, em 01 de julho de 2004. A Convenção foi ratificada por 69 Estados de todos os continentes e assinada por mais dois.

Esta convenção teve por objectivo principal, a harmonização entre os vários países signatários, dos elementos relativos às infracções, do direito penal, respeitantes a crimes realizados através de meios electrónicos, ou seja, a Cibercriminalidade. Por outro lado, consagra a implementação de um sistema de cooperação internacional, para que as infracções cometidas por meio de sistema informático, tenha o acompanhamento, auxílio, e apoio dos demais Estados-Membros.

Pode ler-se na minuta do relatório explicativo da convenção de Budapeste, que a mesma foi adoptada com o sentido de fazer acompanhar o processo penal, a esta nova criminalidade informática, visto que as novas tecnologias começaram a demonstrar-se um novo desafio, face aos conceitos jurídicos existentes.

Assim, a convecção é necessária para impedir actos, praticados contra a confidencialidade, integridade e disponibilidade de sistemas informáticos, de redes e dados informáticos, bem como a utilização fraudulenta desses sistemas, redes e dados, assegurando a incriminação desses comportamentos, e da adopção de poderes suficientes para combater eficazmente essas infracções, facilitando a detenção, a investigação e o procedimento criminal relativamente as referidas infracções, tanto a nível nacional como internacional, e estabelecendo disposições materiais com vista a uma cooperação internacional rápida e fiável.

Importa ainda referir que, a convecção de Budapeste é o único tratado internacional em vigor sobre a cibercriminalidade, contendo um quadro legal de referência em termos de direito penal substantivo, ferramentas processuais e normas de cooperação internacional. Moçambique foi convidado a aderir à Convenção de Budapeste à 7 de fevereiro de 2024, no entanto, até a presente data não aderiu. Pensamos que é o momento exacto para aderir aos apelos da PGR, quando se refere, no seu informe anual que, "... a adesão de Moçambique à Convenção de Budapeste sobre o cibercrime contribuiria para facilitar a cooperação internacional, nesta matéria, pois estamos em face da criminalidade organizada com natureza transnacional."[145]

Portugal assinou a Convenção de Budapeste, em 23 de Novembro de 2001 e só em 2009 foi ratificada pelo Decreto do Presidente da República n.º 91/2009. Já o Brasil depositou a carta

[145] Idem, pág. 184.

de adesão ao Conselho da Europa em 30 de Novembro de 2022. O decreto de promulgação da convenção no Brasil foi publicado em 12 de Abril de 2023 através do Decreto nº 11.419.

3.2.2. A lei nº 32/2008 de 17 de Julho

Esta lei transpôs para a ordem jurídica portuguesa a diretiva nº 2006/24/CE referente à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrônicas publicamente disponíveis ou de redes públicas de comunicações, bem como os dados conexos necessários para identificar o assinante ou o utilizador registado para fins de investigação destes e repressão de crimes graves.[146]

Nos termos desta Lei, a transmissão destes dados só é admissível num catálogo restritivo de crimes; por despacho fundamentado do JIC, quando houver razões para crer que são indispensáveis para a descoberta da verdade ou para a prova daqueles e que esta será de outra forma impossível ou muito difícil de obter; e deve respeitar os princípios de adequação, necessidade e proporcionalidade.[147]

Para além disso só podem ser transmitidos dados relativos: ao suspeito ou arguido, à pessoa suspeita de receber ou transmitir mensagens destinadas ou provenientes daqueles ou, mediante consentimento, à própria vítima, vide artigo 9º, nº 3. A referida lei, no seu artigo 4º, plasma que a conservação e preservação dos dados, deve existir durante um ano.

A competência das autoridades judiciárias, dos OPC's quanto à preservação dos dados informáticos, estende-se de igual modo quanto à pesquisa destes, e mesmo à sua apreensão. Explica-nos o mesmo diploma que as entidades competentes têm o dever de cooperação com as entidades competentes estrangeiras quando do mesmo modo, se tratar de crimes em que envolva a pesquisa, análise, apreensão, preservação de dados informáticos e especialmente recolha de prova.

Todas estas manobras de investigação, seja de investigação no âmbito interno, ou de cooperação com entidades estrangeiras, devem, e estão ao abrigo da referida lei, respeitando por sua vez o acordo com as normas sobre transferência de dados pessoais.

[146] Idem, pág. 190 e ss.
[147] Cfr. Nº 1 e 2 do artigo 9º da Lei nº 32/2008, de 17 de Julho.

Normas essas, que debruçam especial atenção, ao tratamento de dados pessoais, salvaguardando que este processo se deva realizar de forma transparente e no estrito respeito pela reserva da vida privada. São considerados sensíveis, todos os dados que incidem de alguma forma em direitos fundamentais, como as convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem racial ou étnica, no fundo, direitos esses inalienáveis e constitucionalmente protegidos.[148] Nesses casos, são necessárias condições especiais para que seja então permitido o tratamento desses dados.

Da análise desta lei, verifica-se em suma que, está, ainda que incompleta, consegue dar resposta a um número maior de questionamentos que se levantam sobre a prova digital, portanto, entendemos que tenha sido um bom pontapé de saída para a complementaridade da regra do CPP sobre a prova digital.

3.2.3. A Lei do Cibercrime Portuguesa

Apenas em 2009, entrou em vigor a Lei nº 109/2009, designada Lei do Cibercrime, cumprindo assim Portugal as obrigações resultantes da ratificação da Convecção do conselho da Europa sobre o Cibercrime – Convenção de Budapeste. Com a publicação desta nova lei, o legislador português consagrou, finalmente, um verdadeiro sistema processual da prova digital.

Em vez de proceder a alterações legislativas, nomeadamente no CPP, o legislador português optou por criar um diploma onde englobasse todas as disposições legais referentes à cibercriminalidade, uma vez que esta opção legislativa vai ao encontro da tradição portuguesa, onde existem, especificamente na área penal, outros diplomas estruturantes de matérias na especialidade.

Não se pode deixar de mencionar a importância da LC para o ordenamento jurídico português, visto que, foi o primeiro diploma legal a prever meios de obtenção de prova num contexto digital.

O âmbito de aplicação das disposições processuais da LC abrange, aos crimes aí previstos (crimes informáticos *stricto sensu*), aos crimes cometidos por meio de um sistema informático e, ainda, aos crimes em que seja necessário proceder à recolha de prova em suporte digital. [149]

[148] NEVES, Rita Castanheira, *"As ingerências nas Comunicações eletrônicas em Processo Penal", ob. cit.* pág. 193.
[149] Cfr. Artigo 2 da Lei do Cibercrime Portuguesa.

A relação entre a LC e a Lei nº 32/2008 não é de todo pacífica. Paulo Dá Mesquita entende que a primeira veio revogar o artigo 9º da Lei nº 32/2008, uma vez que a panóplia de dados abrangido pela LC é mais abrangente que os contidos na Lei nº 32/2008, porém o mesmo autor frisa a importância deste diploma "(…) sobretudo, no estabelecimento dos deveres dos fornecedores de serviços de conservação e protecção desses dados, bem como das condições técnicas operativas e destruição desses bens."[150]

Já Benjamim Silva Rodrigues e Renato Lopes Militão entendem que os dois diplomas legais se complementam, como aliás resulta expressamente da letra do artigo 11º nº 2 da LC, que desde já sublinhamos o pensamento desses autores, pois entendemos nós que, o próximo passo do legislador português será unificar os diplomas legais relativos a prova digital num único e mesmo instrumento.

3.2.3.1. Os Meios de Obtenção de Prova digital na Lei do Cibercrime Portuguesa

É o capítulo III da LC, que mais nos interessa pois lá se encontram às disposições processuais, entre os artigos 11º a 19º, relativas a obtenção da prova digital.

O art. 11º refere-se ao âmbito de aplicação das disposições processuais. De acordo com o nº 1 desta norma as disposições processuais da LC, à excepção dos artigos 18º e 19º, aplicam-se: a) aos crimes previstos na LC; b) crimes cometidos por meio de um sistema informático; ou c) em relação aos quais seja necessário proceder à recolha de prova em suporte digital. É a al. c) que mais nos interessa e que mais nos debruçaremos seguidamente.

A preservação expedita de dados encontra-se consagrada no art. 12º LC, sendo que o legislador português optou por abranger numa única norma a preservação de dados informáticos e dados de tráfego, e regular no art. 13º LC a revelação expedita de dados de tráfego, diferentemente, do que sucedia na CCiber, que previa na norma 16ª a conservação expedita de dados informáticos armazenados e na norma 17º a conservação expedita e divulgação parcial dos dados de tráfego.

O art. 12º da Lei nº 109/2009, de 15 de setembro, debruça-se especialmente na matéria da preservação da Prova Digital, definindo que se desse modo se tornar necessário, compete à

[150] MESQUITA, PAULO DÁ, *"Processo Penal, Prova e Sistema Judiciári*o", Coimbra Editora, 2010, pág. 108.

autoridade judiciária ordenar que os dados em apreço possam ser guardados, armazenados de forma a garantir uma posterior consulta ou análise. "Se no decurso do processo for necessário à produção de prova, tendo em vista a descoberta da verdade, obter dados informáticos específicos armazenados num sistema informático, incluindo dados de tráfego, em relação aos quais haja receio de que possam perder-se, alterar-se ou deixar de estar disponíveis, a autoridade judiciária competente ordena a quem tenha disponibilidade ou controlo desses dados, designadamente a fornecedor de serviço, que preserve os dados em causa"[151].

Como se viu, é da competência da autoridade judiciária ordenar a preservação dos danos, contudo, pode ainda a preservação ser ordenada por OPC, desde que devidamente autorizada pela autoridade judiciária competente ou em situações de urgência ou de perigo na demora, desde que tal seja imediatamente transmitido à autoridade judiciária competente e, acompanhado de relatório nos termos do art. 253º do CPP de Portugal.[152]

A ordem de preservação terá que indicar: a) a natureza dos dados; b) a sua origem e destino e c) o período de tempo pelo qual deverão ser preservados, até um máximo de três meses, sob pena de nulidade.[153]

São definitivamente musculadas nesta lei, as formalidades das medidas exigidas para que seja possível a preservação da Prova Digital. A LC, atenta também, ainda em sede de preservação dos dados, a sua ordem, o intransigente sigilo, e os prazos, ao que, não sendo estes requisitos cumpridos, considerar-se-ão nulas todas elas, nos termos do artigo 12 da LC. Significa isto que, mesmo sendo os OPC's a proceder à sua preservação, são estes obrigados a respeitar a ordem de armazenamento, sigilo, e prazos, para que possam ser obtidos e posteriormente utilizados pelas autoridades judiciárias, no estrito cumprimento da lei.

Como refere Benjamim da Silva Rodrigues, "Importa notar que o período máximo de três meses não deverá ser ultrapassado, não sendo de discutir a possibilidade de renovação, à semelhança do que ocorre com as escutas telefónicas, mas haverá que atentar ao prazo absoluto de conservação dos dados gerados e tratados no âmbito das comunicações electrónicas, disposto no artigo 6º da Lei nº 32/2008: um ano"[154]. Daí que, e tal como salienta o mesmo

[151] Cfr. Art. 12º da Lei nº 109/2009, de 15 de setembro.
[152] Cfr. Art. 12º nº 2 da nº 109/2009, de 15 de setembro.
[153] Cfr. Art. 12º nº 3 da nº 109/2009, de 15 de setembro.
[154] RODRIGUES, Benjamim Silva, (2011). *Da Prova Penal Tomo IV – Da Prova – Electrónico – Digital e da Criminalidade Informático – Digital*, pág. 522.

autor, "o nº 5 do art. 12º determine expressamente que o período de três meses possa ser renovado até ao limite máximo de um ano."[155]

Por último, o nº 4 deste preceito legal assegura que com a ordem de preservação, quem disponha ou controle os dados, deve "preservar de imediato os dados em causa, protegendo e conservando a sua integridade pelo tempo fixado, isto é, deve congelar os dados"[156], além de que fica obrigado a assegurar a confidencialidade do processo em curso.

Já o art. 13º regula a revelação expedita de dados de tráfego, este artigo visa que o fornecedor de serviços a quem tenha sido ordenada a preservação dos dados, identifique os demais fornecedores de serviços através dos quais, aquela comunicação foi efetuada, de forma a que a autoridade competente possa identificar a origem da comunicação, bem como o destino da mesma.

Segue-se a injunção para apresentação ou concessão do acesso a dados, prevista no art. 14º da LC, que visa que a autoridade judiciária competente ordene, a quem tenha disponibilidade ou controlo sobre determinados dados armazenados num sistema informático: a) que os comunique ao processo ou, b) que permita o acesso aos mesmos, sob pena de punição por crime de desobediência, conforme se depreende do nº 1 do art. 14º da LC e art. 348º CP de Portugal.

A injunção tem que identificar os dados em causa, aliás como sucede com a ordem de preservação de dados (art. 14º nº 2 LC). Este preceito legal aplica-se também aos fornecedores "(…) a quem pode ser ordenado que comuniquem ao processo dados relativos aos seus clientes ou assinantes, neles se incluindo qualquer informação diferente dos dados relativos ao tráfego ou ao conteúdo, contida sob a forma de dados informáticos ou sob qualquer outra forma, detida pelo fornecedor de serviços, e que permita identificar: a) o tipo de serviço de comunicação utilizada, as medidas técnicas tomadas a esse respeito e o período de serviço; b) a identidade, a morada postal ou geográfica e o número de telefone do assistente, e qualquer outro número de acesso, os dados respeitantes à facturação e ao pagamento, disponíveis com base num contrato ou acordo de serviços; ou c) qualquer outra informação sobre a localização do equipamento de comunicação, disponível com base num contrato ou acordo de serviços." [157]

[155] Idem, pág. 522.
[156] Idem, pág. 524.
[157] Cfr. Art. 14º nº 4 da Lei nº 109/2009, de 15 de Setembro.

O nº 5 do art. 14º faz uma ressalva, que nos parece de maior importância, a injunção não pode ser dirigida ao arguido ou suspeito. Desta forma o legislador salvaguardou o direito à não autoincriminação por parte do arguido ou suspeito, uma vez que, se a injunção pudesse ser dirigida ao suspeito ou arguido, este poderia ter uma participação activa na sua incriminação na medida em que seria obrigado a comunicar ao processo os dados, objectos da investigação ou teria que permitir o acesso aos mesmos, sob pena de incorrer num crime de desobediência.

A apreensão de dados informáticos vem regulada no art. 16º da LC, nos termos do nº 1 desta norma, a autoridade judiciária competente pode ordenar, mediante despacho, a apreensão de dados ou documentos informáticos, descobertos durante uma pesquisa ou outro acesso legítimo a um sistema informático.

Todavia, existem duas situações, em que os órgãos de polícia criminal podem proceder à apreensão, sem prévia autorização da autoridade judiciária competente, "no decurso de pesquisa informática legitimamente ordenada e executada nos termos do artigo anterior, bem como quando haja urgência ou perigo na demora ", nos termos do nº 2 do art. 16º da LC.

O nº 3 do art. 16º merece especial destaque, uma vez que com este preceito, o legislador pretendeu salvaguardar informação pessoal e que poderia implicar um obstáculo a este meio de obtenção de prova, já que poderia pôr em causa direitos fundamentais do suspeito ou arguido ou até de terceiro, assim, caso sejam apreendidos dados ou documentos informáticos cujo conteúdo seja susceptível de revelar dados pessoais ou íntimos, que possam pôr em causa a privacidade do respectivo titular ou de terceiro, sob pena de nulidade esses dados ou documentos são apresentados ao juiz, que ponderará a sua junção aos autos tendo em conta os interesses do caso concreto.

De forma a validar as apreensões levadas a cabo por órgão de polícia criminal, estas terão de ser apresentadas à autoridade judiciária competente, num prazo máximo de 72 horas, nos termos do art. 16º nº 4 da LC.

No nº 7 do art. 16º da LC estão previstas diferentes formas de apreensão que passam pela a) apreensão do suporte onde está instalado o sistema ou apreensão do suporte onde estão armazenados os dados; b) cópia dos dados em suporte autónomo; c) preservação dos dados; d) eliminação não reversível e bloqueio de acesso aos dados.

O art. 17º da LC regula a apreensão de correio eletrônico e registo de natureza semelhante, que prevê a possibilidade de o juiz poder autorizar ou ordenar, a apreensão de mensagens de correio eletrônico ou registo de natureza semelhante, aplicando-se o regime de apreensão de correspondência previsto no art. 179º CPP de Portugal.

É de salientar que não se aplicará neste contexto a al. b) do nº 1 do art. 179º CPP de Portugal, ou seja, quando estejam em causa crimes puníveis com pena de prisão, no seu máximo, superior a três anos. Isto porque, o art. 11º da LC especifica que o art. 17º LC aplica-se a crimes previstos na LC, a crimes cometidos por meio de um sistema informático e aos crimes em que seja necessário proceder à recolha de prova em suporte electrónico, conforme já nos referimos anteriormente.

Analisaremos agora a intercepção de comunicações regulada no art. 18º LC, esta norma aplica-se a crimes previstos na LC, bem como a crimes cometidos por meio de um sistema informático ou em relação aos quais seja necessário proceder à recolha de prova em suporte digital, quando tais crimes estejam previstos no art. 187º CPP de Portugal.

A intercepção é autorizada por despacho do JIC, mediante requerimento do MP, apenas durante a fase de inquérito, desde que: a) haja razões para crer que a diligência é indispensável à descoberta da verdade ou, b) que de outra forma a prova seria muito difícil, ou até impossível, de obter, de acordo com o que dispõe o art. 18º nº 2 LC.

Salienta o nº 3 do preceito em análise, que o despacho do JIC deve especificar o âmbito da intercepção, atendendo às necessidades da investigação.

Por último o art. 18 da LC remete, em tudo o que não seja contrário, para os artigos 187º, 188º e 190º CPP de Portugal. Assim, torna-se evidente que a semelhança das escutas telefônicas esta medida apenas poder ser utilizada contra: a) suspeito ou arguido; b) pessoa que sirva de intermediário, desde que haja fundados motivos para crer que recebe ou transmite mensagens destinadas ou provenientes do arguido ou suspeito; c) vítima do crime, desde que com o seu consentimento.

Além disso, importa referir que as intercepções de comunicação como refere Rita Castanheira, são autorizadas pelo prazo máximo de três meses, renováveis por períodos sujeitos ao mesmo limite. [158]

Assim, quando estejam em causa intercepções referentes a crimes cometidos no âmbito da LC, bem como do art. 187º do CP de Portugal, quando sejam cometidos por meio de um sistema informático ou em relação aos quais seja necessário proceder à recolha em suporte eletrônico, aplica-se o regime do art. 18º LC, verificando-se apenas a realização de algum dos crimes previsto no art. 187º CPP de Portugal então o regime aplicável já será o do art. 188º CPP de Portugal.

Esta lei parece-nos um exemplo a seguir pois prevê normas para a captação, armazenamento, reprodução e inserção válida no processo penal, mas apesar deste facto, parece-nos importante trazer para este contexto as críticas levantadas para que na feitura de um regime jurídico autônomo da prova digital, o nosso legislador possa ter em conta os aspectos levantados.

3.2.3.2. Críticas ao actual regime processual da prova digital portuguesa

Apesar de no nosso contexto o regime processual da prova digital parecer perfeito, este tem sido alvo de várias críticas doutrinais, que em nosso entender importa trazer para este contexto, para que com elas se possa desenhar no nosso contexto, um modelo de lei capaz de responder as principais inquietações relativas ao regime processual da prova digital. As críticas aqui suscitadas são de natureza material e formal.

A primeira crítica lançada é o facto de a opção legislativa portuguesa ter escolhido a legislação extravagante, em detrimento do aconselhável regime geral, fazendo com que em vez de uma, as fontes da prova digital passassem, a ser três, pois, a coexistência formal destas três normas gera extensas zonas de confronto e de atrito, porventura imperceptíveis ao observador menos atento.[159] Em nossa opinião, é legítimo o uso de legislação extravagante, principalmente atendendo aos custos de uma revisão ao CPP, pois, o importante é suprir as lacunas legislativas.

A segunda crítica é o facto de parte da doutrina[160] entender que a Lei 32/2008 e, depois, a Lei 109/2009 revogaram tacitamente parcelas importantes do regime consagrado no artigo 189º do

[158] NEVES, Rita Castanheira, *"As ingerências nas Comunicações eletrônicas em Processo Penal",* ob. cit. pág. 182 e ss.
[159] NEVES, Rita Castanheira, ob. cit. pág. 190 e ss.
[160] MESQUITA, Paulo Dá, ob. cit., pág. 120 e ss.

CPP português, reduzindo muito o seu alargado âmbito de aplicação inicial. Estas leis extravagantes sobrepõem-se àquele regime geral, que só subsiste naquilo que não foi depois especialmente regulado.

Outra crítica que merece a nossa atenção é o facto de uma tese doutrinaria minoritária[161] referir que as relações entre a Lei nº 32/2008 e a Lei nº 109/2009 serem mais complexas, no sentido de que, a lei 32/2008 só sobrevive naquilo que não foi expressamente regulado pela LC.

Em sentido contrário, a tese maioritária[162] advoga que a relação será antes de pura complementaridade. O próprio legislador afirmou-o solenemente na LC no artigo 11.º, nº 2. Assim, restaria ao intérprete o pesado ónus de determinar os respetivos âmbitos de aplicação, delimitando campos que parecem sobrepostos, mas são afinal contíguos.[163]

A jurisprudência portuguesa[164] conclui que o regime processual da Lei 32/2008, designadamente o artigo 3º, nº 1 e 2 e o artigo 9º: - mostra-se revogados e substituído pelo regime processual contido na Lei nº 109/2009 para todos os dados que não estejam especificamente previstos no artigo 4º, n. 1 da Lei nº 32/2008 ou seja, dados conservados em geral; - revela-se vigente para todos os dados que estejam especificamente previstos no artigo 4º, n. 1 da Lei nº 32/2008, isto é, para os dados conservados relativos à localização celular.

A doutrina portuguesa[165] refere que, para além destes problemas formais, resultantes de uma técnica legislativa desadequada, também as próprias soluções legais suscitam algumas reservas materiais. Nuns casos foram claramente esquecidas as exigências de uma acção penal eficaz, como novo e autónomo bem jurídico, constitucionalmente reconhecido e sancionado. Noutros é a proteção dos direitos individuais, enquanto inquestionável finalidade primária do próprio processo penal, que ficou demasiado fragilizada.

Um dos pontos mais discutíveis (e carecidos de reforma) do regime legal da prova digital consiste na tutela processual penal conferida ao correio eletrônico já recebido, que para o nosso caso não se aplica, pois, o nosso legislador foi em sentido contrário e mais acertado.

---

[161] Idem, pág. 120 e ss.
[162] Neste sentido MESQUITA, Paulo Dá, ob. cit., pág. 120 e ss., e NEVES, Rita Castanheira, *"As ingerências nas Comunicações eletrônicas em Processo Penal***"**, *ob.cit.* pág. 192 e ss.
[163] Idem.
[164] Acórdão do Tribunal da Relação de Coimbra, de 28-04-2009, processo nº 92/08.4GDCTB-A.C1. Disponível em http://www.dgsi.pt
[165] Neste sentido autores como MESQUITA, Paulo Dá, ob. cit., pág. 121 e ss.

Todavia, em nosso entender apesar de o legislador português não ter efectuado qualquer distinção legal do correio eletrônico já lido, somos de concordar com os autores[166], no sentido de que depois de recebido, lido e guardado no computador do destinatário, um e-mail deixa de pertencer à área de tutela das telecomunicações, passando a valer como um normal escrito, portanto, sujeito aos meios de obtenção de prova tradicionais.

Outra incongruência do legislador apontada pela doutrina[167] consiste na aparente impossibilidade formal de realizar intercepções de comunicações, ou sequer de obter os respetivos dados de tráfego, para prova dos crimes previstos na LC ou de injúrias, de ameaças, de coação, de devassa da vida privada cometidos por meio de Correio Eletrônico.

Nos termos do artigo 18º da LC a intercepção das comunicações só é aqui admissível quando os crimes se encontrem previstos no artigo 187º do CPP. Uma leitura literal tenderá, portanto, a excluir todos os outros crimes.

Já a outra parte da doutrina[168] afirma que, esta tese, que parte da manutenção formal do artigo 189º do CPP português, é inadmissível: primeiro, porque nos casos previstos no artigo 18, n,º 1, a) a intercepção não depende de qualquer outro requisito adicional, *maxime* da respetiva moldura penal abstrata (foi, por isso mesmo, que o legislador autonomizou as duas alíneas do referido artigo, ainda que os requisitos adicionais, previstos na alínea b), só se aplicam aos casos aí referidos); e segundo, porque a remissão para o catálogo de crimes constante do artigo 189º do CPP deverá, numa interpretação actualista, incluir os crimes de injúria, ameaça, coação ou devassa da vida privada cometidos através de sistema informático.

O propósito do legislador, foi, justamente, permitir a realização de intercepção de comunicações eletrônicas e, sobretudo a obtenção de dados de tráfego nos processos crimes em que se investiguem crimes cometidos por via das redes de comunicações.

A remissão legal é, assim, para o tipo de crime e não para a forma como ele é cometido, pois essa passa necessariamente por um sistema informático, como resulta da primeira parte da alínea b) do nº 1 do artigo 18.º (cometidos por meio de um sistema informático).

---

[166] Neste sentido MESQUITA, Paulo Dá, ob. cit., pág. 122 e ss., ANDRADE, Manuel da Costa, 2009, ob. cit. e Rita Castanheira, *ob.cit.* pág. 190 e ss.
[167] DIAS, Figueiredo, *Revisitação de algumas ideias-mestras da teoria das proibições de prova em processo penal* Revista de Legislação e Jurisprudência, A.146:4000, 2016, pág. 101 ss.
[168] RODRIGUES, Benjamim Silva, *Da Prova Penal Tomo IV – Da Prova – Electrónico – Digital e da Criminalidade Informático – Digital*, 2011, pág. 522.

Na opinião de Benjamim Rodrigues, que desde já sublinhamos, o que ali é autorizado para os crimes praticados através do telefone é aqui permitido para os crimes cometidos através de um sistema informático. Na verdade, não podemos esquecer que a Constituição não prevê formas de utilização abusiva deste direito. O sigilo das comunicações não foi concedido para, a seu coberto, se poder insultar, ameaçar ou coagir outrem ou para se poder devassar a sua vida privada.

Nestes casos, apesar da sua reduzida relevância penal, o Estado deve ter legitimidade para intervir. Nada justifica, por isso, destacar as ofensas cometidas por telefone, conferindo-lhes uma tutela processual penal muito superior às restantes.

Importa referir que até ao presente momento, as críticas levantadas aplicam-se também ao legislador nacional, no sentido de que, não definiu a possibilidade de incluir os crimes de injúria, ameaça, coação ou devassa da vida privada cometidos através de sistema informático. Neste quesito, julgamos acertadas as posições doutrinarias acima enunciadas e pelas razões já referidas.

3.3. A prova digital no Brasil

No sistema processual penal brasileiro, verificamos que ainda não consta alguma forma de obtenção de prova direcionada especificamente à prova digital. O que se verifica, no entanto, é que as partes e o próprio Estado se utilizam analogicamente dos meios já previstos na legislação processual penal brasileira para a coleta das Provas Digitais, estes compreendidos, basicamente, pela busca e apreensão, interceptação, a perícia e o mais importante o Sistema de Interceptação de Sinais.

3.3.1. A Busca e a apreensão

Refere-se que a busca é meio de obtenção de prova que visa à localização de pessoas ou coisas. Segundo o CPP Brasileiro, pode haver busca domiciliar e busca pessoal. A apreensão, por sua vez, constitui acto de apossamento de coisas, tornando-as indisponíveis, sob custódia do Estado, enquanto importarem à persecução penal. No cotejo com o mundo digital, convém destacar que as provas digitais não são percebidas a olho nu. Assim, as buscas somente são capazes de identificar os dispositivos informáticos em seus componentes externos, como os

smartphones, tablets, computadores e hard drives. Isso significa que a autorização para a apreensão dos dispositivos é insuficiente para que os dados neles contidos sejam acessados. [169]

A autorização para o acesso aos dados em si deve ser fundamentada em elementos concretos que permitam concluir que (i) os vestígios digitais de um determinado crime encontram-se, de facto, em um sistema informático e (ii) que esses vestígios serão úteis e necessários para os fins da investigação. Do contrário, permitir-se-á que ocorra o levantamento de sigilos protegidos pela Constituição da República sem a devida e fundamentada autorização judicial.[170]

Entendemos que a ausência de parâmetros legais claros para a coleta de dados digitais presentes nos dispositivos informáticos apreendidos pode resultar em autorizações judiciais genéricas para o acesso a todo e qualquer conteúdo armazenado nesses dispositivos. Ademais a aplicação direta do artigo 240 e seguintes do CPP brasileiro, que versam sobre busca e apreensão física, para o acesso a dados em dispositivos eletrônicos implica equiparação entre coisas materiais e dados, muito embora o grau de invasão seja significativamente maior nos meios digitais, o que pode aumentar o potencial de afectação a direitos fundamentais.

3.3.2. A interceptação de Dados Digitais

Além da apreensão do suporte físico nos quais os dados digitais estão armazenados, a evolução tecnológica permite, hoje, o acesso e apreensão desses dados de forma oculta e remota. No Brasil, a Lei 9.296/96 de 24 de Julho foi responsável por regulamentar a parte final do inciso XII do art. 5.º da Constituição Federal, conferindo à interceptação telemática *status* constitucional.

Tornou-se tecnologicamente viável que, de forma escamoteada, os agentes de persecução explorem vulnerabilidades dos sistemas alvo para acessar informações, inclusive aquelas protegidas por sigilo, driblando mecanismos estabelecidos de criptografia. Nesse contexto, duas medidas para obtenção de dados podem ser destacadas: o *hacking* estatal e a infiltração por *malware*.[171]

[169] BADARÓ, Gustavo. *A cadeia de custódia da prova digital. Direito probatório*. Lodrina, Editora Toth, 2023, pág. 20.
[170] Idem. Pág. 20.
[171] Idem. Pág. 22.

Através do *hackeamento* estatal, os órgãos de investigação infiltram-se de forma oculta e remota em algum dispositivo e/ou sistema de interesse, valendo-se de falhas e aberturas previamente identificadas.[172] Essa prática depende, necessariamente, de conexão com a internet. Um exemplo desta actuação é a quebra de uma senha de acesso, que permite o ingresso no dispositivo informático alvo de modo a viabilizar o acesso a arquivos protegidos.

Os *malwares*, por sua vez, são programas instalados no sistema alvo, inseridos, evidentemente, sem autorização prévia do investigado. Registra-se que a instalação desses softwares visa promover a abertura de uma espécie de portal de acesso remoto, conhecido como "mecanismo de acesso excepcional" ou *backdoor*. A partir desta abertura, as informações podem ser acessadas e transmitidas.[173]

A partir da utilização de *malwares*, por exemplo, os agentes de persecução penal podem executar diversas funcionalidades, tais como: interceptar comunicações telemáticas (obtendo os dados na ponta, não em fluxo); efectuar buscas por dados armazenados ou produzidos; encetar captação ambiental, gravando áudio, pelo microfone do dispositivo, e vídeo, por sua *webcam*; estabelecer formas de vigilância *online*, acompanhando as atividades travadas pelo alvo em ambiente digital; realizar observação em tempo real mediante o monitoramento por vídeo.[174]

Ora, tendo em vista o grau de invasão, a eventual utilização dessas técnicas depende de norma expressa, que regule hipóteses, pressupostos, requisitos, forma de execução, tempo de duração e, sobretudo, que discipline a preservação da cadeia de custódia dos elementos, com demonstração dos procedimentos técnicos executados, com objetivo de assegurar a autenticidade e a confiabilidade dos elementos recolhidos. Portanto, é imprescindível que o legislador brasileiro estabeleça regras específicas para as provas digitais, definindo de forma clara os procedimentos de obtenção, admissão, produção e valoração.

1.4.3. Prova Digital obtida por perícia

[172] Idem, Pág. 25-26.
[173] Idem, pág. 25-26.
[174] Idem, pág. 26.

Por fim, outra forma de captação das Provas Digitais ocorre por meio da realização de um exame pericial nos dados constantes dos dispositivos eletrônicos.

De acordo com Denise Vaz, a necessidade de uma análise técnica, por meio do uso de perícia, pode ocorrer em diversos momentos, em virtude das características intrínsecas a essa fonte de prova. Faz-se necessária a realização da perícia para a própria pesquisa da prova, uma vez que existem diversos dispositivos eletrônicos que demandam conhecimento técnico para o acesso ao seu conteúdo; para a análise dos dados apreendidos, a fim de que sejam extraídos somente aqueles que interessam ao processo e por fim para ser constatada a veracidade e autenticidade das provas digitais.[175]

Tratando-se de fonte de prova complexa, a qual demanda procedimentos técnicos para sua captação, assevera a autora supramencionada que é conveniente a adopção dos procedimentos já vinculados à perícia, regulamentados na legislação brasileira, no artigo 159 e seguintes do CPP.[176]

Dessa forma, havendo indícios de que certo dispositivo contempla uma Prova Digital, proceder-se-á perícia, a qual "deve ser realizada por Perito Oficial, portador de diploma de curso superior" ou, em sua falta, "por 2 (duas) pessoas idôneas, portadoras de diploma de curso superior na área específica".[177]

Após a realização do exame nos dispositivos eletrônicos, "o perito oficial ou os dois peritos nomeados deverão apresentar um laudo minucioso sobre o examinado, bem como responderão os eventuais quesitos que lhes forem feitos pelo juiz, MP ou querelante, assistente de acusação e defesa", nos termos do artigo 160 do CPP brasileiro.[178]

Pese embora o CPP brasileiro seja omisso quanto às especificidades da prova digital, verificamos que a par das normas gerais acima referidas, existem normas técnicas que tratam da gestão desse tipo de prova e de sua cadeia de custódia, além de estabelecerem diretrizes específicas ao tratamento a ser dado às evidências digitais. A exemplo, cita-se a norma técnica

[175] VAZ, Denise Provazi. Op. Cit., pág. 116.
[176] Idem, pág. 116-117.
[177] "Art. 159 do CPP brasileiro. O exame de corpo de delito e outras perícias serão realizados por perito oficial, portador de diploma de curso superior. § 1º Na falta de perito oficial, o exame será realizado por 2 (duas) pessoas idôneas, portadoras de diploma de curso superior preferencialmente na área específica, dentre as que tiverem habilitação técnica relacionada com a natureza do exame. "
[178] "Art. 160. Os peritos elaborarão o laudo pericial, onde descreverão minuciosamente o que examinarem, e responderão aos quesitos formulados. Parágrafo único. O laudo pericial será elaborado no prazo máximo de 10 dias, podendo este prazo ser prorrogado, em casos excepcionais, a requerimento dos peritos. "

ABNT ISO IEC 27037:2013, vigente no Brasil desde 2014, gerida pela ABNT — órgão brasileiro de normatização técnica, reconhecido pelo governo brasileiro e por outros organismos internacionais do sector.[179]

A referida norma prevê procedimentos próprios a serem observados para que haja a adequada custódia das evidências digitais. Em resumo, conforme refere Dário Jóse[180] esses procedimentos são: (1) a devida identificação dos dispositivos de armazenamento de mídia digital e aqueles Que podem conter evidência digital relevante; (2) a coleta da evidência digital, que será removida da localização original em que ocupa e será remetida a um ambiente controlado; (3) a aquisição consistente na produção de cópia da evidência digital e documentação dos métodos utilizados; e (4) a preservação da evidência, consistente na proteção desta contra possíveis adulterações.

Da análise efectuada, é possível concluir-se que não há óbice à inclusão da prova digital no Processo Penal brasileiro, utilizando-se de formas já constantes da legislação, como a busca e apreensão, interceptação telemática, perícia e a norma ABNT ISO IEC 27037:2013. Contudo, considerando a complexidade de suas características, é evidente que a questão pende de regulamentação específica, com o intuito de que a Prova Digital seja devidamente extraída, permaneça íntegra e, assim, esteja apta a produzir efeitos quando da sua introdução no processo penal.

[179] KIST, Dário José. *Prova Digital no Processo Penal*. Leme (SP): JH Mizuno, 2019, pág. 296-303.
[180] Idem, pág. 305.

CONCLUSÃO

Este trabalho teve como objetivo analisar, sob uma perspectiva crítica e comparada, o regime jurídico das escutas telefónicas e da prova digital nos ordenamentos jurídicos de Moçambique, Portugal e Brasil. Pretendeu-se, com isso, evidenciar os principais desafios legais e operacionais enfrentados na adoção desses meios de obtenção de prova, especialmente diante do avanço da criminalidade organizada e do cibercrime.

A análise permitiu constatar que, embora Moçambique disponha actualmente de um regime legal que prevê as escutas telefónicas no seu Código de Processo Penal (CPP), esse regime revela-se incompleto, tecnicamente limitado e desatualizado, sobretudo se comparado ao ordenamento português, do qual parece ter sido parcialmente transposto, mas com cortes significativos.

Verificou-se que não existe previsão legal para situações como os conhecimentos fortuitos, o que dificulta o aproveitamento de informações colhidas incidentalmente durante uma escuta. Além disso, a prova digital carece de regulamentação própria no sistema moçambicano, estando resumida a uma única norma genérica (art. 225 do CPP), que remete ao regime das escutas telefónicas, sem considerar as especificidades técnicas e jurídicas da prova eletrônica.

Ao contrário, Portugal já possui um regime mais completo e articulado, com legislação complementar como a Lei do Cibercrime (Lei n. º 109/2009) e normas sobre a retenção de dados de tráfego. O Brasil, por sua vez, ainda que não disponha de um regime coeso para a prova digital, conta com legislação específica para interceptações (Lei nº 9.296/1996), desenvolveu práticas jurisprudenciais e técnicas (como a adopção da norma ABNT ISO/IEC 27037) para assegurar a cadeia de custódia das provas digitais, sem esquecer o SIS.

Diante desse panorama, conclui-se que Moçambique não aproveitou plenamente a Revisão de 2019 do CPP para regulamentar adequadamente os novos meios de obtenção de prova, mantendo-se atado a um modelo pensado para um tempo já ultrapassado, como afirmou Manuel da Costa Andrade em relação ao CPP português: “esta Revisão ao Código de Processo Penal foi uma oportunidade perdida de, pela primeira vez, assegurar reconhecimento e tratamento adequado aos problemas polarizados pelo uso e abuso das telecomunicações, em geral. E, por vias disso, continuámos atavicamente amarrados a uma equacionação dos

problemas a partir das escutas telefónicas e do seu regime, no essencial, pensado e estruturado na perspectiva do velho telefone fixo".[181]

Conclui-se também que Moçambique e Brasil carecem de regulamentação específica, técnica e actualizada que discipline a obtenção, preservação, tratamento e admissibilidade da prova digital. Reafirma-se, por fim, a necessidade de criar normas processuais penais específicas para a prova digital, idealmente incorporadas ao próprio CPP[182]; Completar o regime das escutas telefónicas, prevendo expressamente aspectos como conhecimentos fortuitos, prazos, sujeitos, suporte técnico e garantias procedimentais; Capacitar tecnicamente os agentes do SERNIC, formando peritos informáticos qualificados; e a adesão urgente de Moçambique à Convenção de Budapeste sobre o Cibercrime, passo fundamental para a cooperação internacional no combate à criminalidade transnacional digital.

A omissão legislativa nesta matéria não só compromete a eficácia da investigação criminal moderna, como também fragiliza as garantias constitucionais dos cidadãos, tornando urgente e inadiável uma intervenção legislativa séria, técnica e voltada para os desafios da sociedade digital.

[181] ANDRADE, MANUEL DA COSTA, *ob.cit.* Pág. 97 e ss.

[182] Pensando e refletindo na lei que deveríamos ter, entendemos que numa primeira fase, o legislador deve criar normas processuais penais especiais relativas a prova digital, no entanto, que fique claro que o ideal seria que se criasse uma secção II com o título "da prova eletrônica", dentro do Capítulo IV "Outros meios de prova", do Título III "Meios de obtenção de prova" do Código de Processo Penal, pois a legislação especial é acessória, técnica e expcecional. Normas como as que preveem a prova digital, pela sua importância, pelos interesses que regulam, pelas consequências que desencadeiam e, até, pela frequência com que são utilizadas devem constar do CPP

RECOMENDAÇÕES

Tendo em vista as lacunas jurídicas identificadas no ordenamento moçambicano no que tange à regulação das escutas telefónicas e da prova digital, e considerando a análise comparativa com os sistemas de Portugal e Brasil, propomos as seguintes recomendações:

Levando-se em conta as características singulares das provas digitais, bem como o facto de que tais provas, muitas vezes, estão intimamente vinculadas a direitos fundamentais dos cidadãos e constitucionalmente garantidos, percebe-se a necessidade de uma regulamentação própria e específica para a produção de tais provas, a qual deve abarcar as formas de sua captação, armazenamento, reprodução e inserção válida no processo penal, assim como a manutenção, bem como análise forense, prevenção de perdas, manejo de incidentes e avaliação de risco.

Na fase de obtenção, deve-se instituir normas técnicas acerca dos meios que serão utilizados, uma vez que estas podem ser facilmente modificadas, rapidamente disseminadas ou exterminadas. As normas Técnicas, permitirão assegurar que os meios utilizados na obtenção da prova digital sejam fiáveis, auditáveis e protegidos contra adulterações.

Além disso, também devem ser instituídas regras procedimentais destinadas ao armazenamento das provas, com o intuito de que se resguarde a sua integridade e autenticidade.

Desse modo, também é fundamental que a prova digital seja armazenada em dispositivos que permitam a conservação da integridade da prova e, ao mesmo tempo, sejam de fácil acesso por aqueles envolvidos no caso.[183]

Isso, aliado à necessidade de positivar-se regras referentes aos cuidados que devem ser observados na coleta das provas digitais, a fim de garantir a inviolabilidade de Direitos Fundamentais, após a sua inserção no processo penal, deve estar prevista a possibilidade de manifestação das partes, respeitando também os princípios e garantias constitucionais do Contraditório e da Ampla Defesa.[184]

O legislador deve completar o regime das escutas telefônicas prevendo a forma técnica de efectuar a interceptação, tratando dos conhecimentos fortuitos, dos prazos, dos sujeitos, da autorização do assistente e do arguido para o exame dos suportes técnicos das conversações,

[183] Idem, pág. 118 ségs
[184] Este também é o entendimento de Dario José Kist, segundo o qual "a prova constituída pelo conteúdo de arquivos digitais será objeto de escrutínio pelas partes, no exercício do direito ao contraditório". Ob cit, pág. 309.

da autorização do arguido e do assistente de poderem requerer a junção das conversações interceptadas aos autos, o destino dos suportes técnicos referentes as conversações ou comunicações.

Por outro lado, é necessário dotar o SERNIC com pessoal especializado, impondo-se, assim, a formação de peritos informáticos para auxiliarem na investigação, sobretudo, na recolha e tratamento da prova digital ou eletrônica.[185] Essa medida permitirá uma actuação mais eficaz na recolha, preservação e análise da prova digital e eletrônica, garantindo o respeito à cadeia de custódia e à integridade probatória. É necessário ainda dotar o SERNIC de meios materiais adequados a função.

E por fim, entendemos ser crucial a adesão de Moçambique à Convenção de Budapeste sobre o cibercrime, pois contribuiria para o fortalecimento da cooperação internacional no combate à criminalidade organizada, digital e transnacional, a harmonização legislativa com padrões internacionais e o acesso a instrumentos técnicos e jurídicos modernos, fundamentais para a persecução penal na era digital.

[185] Informe anual da PGR à Assembleia da República do ano de 2023, pág. 35 e 36.

REFERÊNCIAS BIBLIOGRÁFICAS

Livros e Manuais

- Aguilar, F. M. F. (2004). *Dos conhecimentos fortuitos obtidos através de escutas telefónicas*. Almedina.
- Albuquerque, P. P. de. (2011). *Comentário do Código de Processo Penal à luz da Constituição da República Portuguesa e da Convenção Europeia dos Direitos do Homem* (4ª ed.). Universidade Católica Editora.
- Andrade, M. da C. (2009). Bruscamente no verão passado: A reforma do Código de Processo *Penal – Observações críticas sobre uma lei que podia e devia ter sido diferente*. Coimbra Editora.
- Andrade, M. da C. (2013). *Sobre as proibições de prova em processo penal* (Reimpressão). Coimbra Editora.
- Badaró, G. (2023). *A cadeia de custódia da prova digital*. Editora Thoth.
- Conceição, A. R. (2009). *Escutas telefónicas: Regime processual penal*. Quid Juris.
- Correia, J. C. (2004). *Afirmar a advocacia: Reflexões sobre a cidadania e a justiça*. Almedina.
- Gil, A. C. (2017). *Como elaborar um projeto de pesquisa* (6ª ed.). Atlas.
- Gomes, L. F., & Maciel, S. (2011). *Interceptação telefônica: Comentários à Lei 9.296, de 24.07.1996*. Revista dos Tribunais.
- Grinover, A. P., Gomes Filho, A. M., & Fernandes, A. S. (2009). *As nulidades no processo penal* (11ª ed.). Revista dos Tribunais.
- Kist, D. J. (2019). *Prova digital no processo penal*. JH Mizuno.
- Lakatos, E. M., & Marconi, M. A. (1991). *Metodologia científica* (2ª ed.). Atlas.
- Leite, A. L. (2007). *Entre Péricles e Sísifo: O novo regime legal das escutas telefónicas*. Coimbra Editora.
- Mesquita, P. D. (2010). *Processo penal, prova e sistema judiciário*. Coimbra Editora.
- Neves, R. C. (2011). As ingerências nas comunicações eletrônicas em processo penal: Natureza e respetivo regime jurídico do correio eletrónico enquanto meio de obtenção de prova. *Coimbra Editora*.
- Rodrigues, B. S. (2008). *Das escutas telefónicas: A monitorização dos fluxos informacionais e comunicacionais* (Tomo I). Coimbra Editora.

- Rodrigues, B. S. (2011). *Da prova penal: Tomo IV – Da prova eletrónica e da criminalidade informático-digital* (1ª ed.). Rei dos Livros.
- Rodrigues, C. L. (2013). *Dos pressupostos materiais de autorização de uma escuta telefónica*. Verbo Jurídico.
- Santos, M. S., Leal-Henriques, M., & Santos, J. S. (2011). *Noções de processo penal* (2ª ed.). Rei dos Livros.
- Saad, M., Rossi, H. C., & Partata, P. H. (2024). A obtenção das provas digitais no processo penal demanda uma disciplina jurídica própria? Uma análise do conceito, das características e das peculiaridades das provas digitais. *Revista Brasileira de Direito Processual Penal, 10*(3), e1071.
- Silva, G. M. da. (2008). *Curso de processo penal* (4ª ed.). Editorial Verbo.
- Susano, H. (2009). *Escutas telefónicas: Exigências e controvérsias do atual regime*. Coimbra Editora.
- Valente, M. G. (2008). *Escutas telefónicas: Da excecionalidade à vulgaridade* (2ª ed.). Almedina.
- Valente, M. M. (2010). *Processo penal* (Vol. I). Almedina.

Leis e Normas jurídicas

- Assembleia da República. (2007). Lei nº 53/2007, de 31 de agosto. Aprova a orgânica da Polícia de Segurança Pública Portuguesa. *Diário da República*, 1.ª série, nº 168, 6065–6074.
- Assembleia da República. (2008). Lei nº 37/2008, de 6 de agosto. Aprova a orgânica da Polícia Judiciária Portuguesa. *Diário da República*, 1.ª série, nº 151, 5281–5289.
- Assembleia da República. (2008). Lei nº 49/2008, de 27 de agosto. Aprova a Lei de Organização da Investigação Criminal. *Diário da República*, 1.ª série, nº 165, 6038–6042.
- Convenção de Budapeste.
- Brasil. (1988). *Constituição da República Federativa do Brasil*. Brasília, DF.
- Brasil. (1996). Lei nº 9.296, de 24 de julho de 1996. Regulamenta o inciso XII do art. 5º da Constituição Federal. *Diário Oficial da União*.
- Brasil. (1962). Lei nº 4.117/1962, de 27 de Agosto. Código Brasileiro de Telecomunicações.
- Brasil. Código de Processo Penal Brasileiro.

- Brasil. ABNT ISO IEC 27037:2013.
- Moçambique. (2018). *Constituição da República de Moçambique*.
- Moçambique. (2016). Lei nº 4/2016, de 3 de junho. Lei das telecomunicações.
- Moçambique. (2017). Lei nº 3/2017, de 9 de janeiro. Lei das transações eletrônicas.
- Moçambique. (2017). Lei nº 34/2014, de 31 de Dezembro. Lei de proteção de dados eletrônicos.
- Moçambique. (2016). Lei nº 27/2016 de 18 de Julho. Regulamento da Lei de Defesa do Consumidor.
- Moçambique. (2013). Lei nº 16/2013, de 12 de Agosto. Lei Orgânica da Polícia da República de Moçambique.
- Moçambique. (2019). Decreto nº 44/2019, de 22 de maio. Regulamento de proteção do consumidor dos serviços de telecomunicações.
- Moçambique. (2023). Lei nº 15/2023, de 28 de Agosto. Lei de prevenção, repreensão e combate ao Terrorrismo.
- Moçambique. Código de Processo Penal.
- Portugal. (2005). *Constituição da República Portuguesa* (7ª revisão).
- Portugal. (2008). Lei nº 32/2008, de 17 de julho. Conservação de dados de comunicações eletrónicas. *Diário da República*.
- Portugal. (2009). Lei nº 109/2009, de 15 de setembro. Lei do cibercrime. *Diário da República*.
- Portugal. Dec. Lei nº 78/87, de 17 de Fevereiro. Código de Processo Penal Português.
- Portugal. Dec. nº 16 489, de 15 de Fevereiro. Código de processo penal de 1929.
- Portugal. DL nº 377/77, de 6 de Setembro. Disposições relativas às alterações da legislação de Processo Penal de Portugal.
- Convenção de Budapeste.

Jurisprudência

- Supremo Tribunal de Justiça. (2006, 29 de março). Processo 607/06. http://www.dgsi.pt
- Supremo Tribunal de Justiça. (2006, 31 de maio). Processo 06P1412. http://www.dgsi.pt
- Tribunal da Relação de Coimbra. (2009, 28 de abril). Processo 92/08.4GDCTB-A.C1. http://www.dgsi.pt

- Tribunal da Relação de Évora. (2012, 7 de dezembro). Processo 1/20.2GABJA-A.E1. http://www.dgsi.pt
- Tribunal da Relação de Évora. (2015, 20 de janeiro). Processo 648/14.6GCFAR-A.E1. http://www.dgsi.pt
- Tribunal da Relação de Lisboa. (2007, 6 de dezembro). Processo 10278/07-9. http://www.dgsi.pt
- Tribunal da Relação de Coimbra. (2012, 09 de Maio), Processo. 222/09.9JACBR.C2. Disponível em http://www.dgsi.pt

Publicações Periódicas

- Andrade, M. de. (1991, julho). Sobre o regime processual penal das escutas telefónicas. *Revista Portuguesa de Ciência Criminal*, 1, 369–408.
- Correia, J. C. (2014, julho-setembro). Prova digital: As leis que temos e a lei que devíamos ter. *Revista do Ministério Público*, 139.
- Dias, F. (2016). Revisitação de algumas ideias-mestras da teoria das proibições de prova em processo penal. *Revista de Legislação e Jurisprudência*, 146(4000).
- Maurício, N., & Iria, C. (2006, janeiro-junho). As escutas telefónicas como meio de obtenção de prova – Necessidade de uma reforma legislativa ou suficiência de uma interpretação conforme?: Ponto de situação numa já *vaexata quaestio*. *Polícia e Justiça. Instituto Superior de Polícia Judiciária e Ciências Criminais*, III Série, 7, 93.
- Rodrigues, O., & Santos, [Nomes próprios faltando]. (2021). Pesquisas qualitativas e quantitativas na educação. *Revista Prisma*, 2(1), 154–174.
- Romão, A. S. (n.d.). Interceptação de comunicação telefônica: Um viés da execução penal. *Revista da Escola Superior de Polícia Civil*. Vila Izabel – Curitiba/PR.
- Teixeira, C. A. (2008). Escutas telefónicas: A mudança de paradigma e os velhos e os novos problemas. *Revista do Centro de Estudos Judiciários*, 9, 244.

Outras fontes

- Procuradoria-Geral da República. (2023). *Informe anual à Assembleia da República – 2023*.
- Silva, H. F. G. da. (2019). *O acesso a terminais de intercepção de comunicações pelos órgãos de polícia criminal* (Dissertação de mestrado, Instituto Superior de Ciências Policiais e Segurança Interna).

- Vaz, D. P. (2012). *Provas digitais no processo penal: Formulação do conceito, definição das características e sistematização do procedimento probatório* (Tese de doutorado, Faculdade de Direito da Universidade de São Paulo).

Sites

- Pereira, M. (1990). *Política de segurança interna*. Repositório Comum. https://comum.rcaap.pt/bitstream/10400.26/2686/1/NeD54_ManuelPereira.pdf
- Ministério Público. (n.d.). *Notas práticas sobre cibercrime*. http://cibercrime.ministeriopublico.pt/notas-praticas
- Direção-Geral da Política de Justiça. (n.d.). *Base de dados jurídicas*. http://www.dgsi.pt
- Dicionário Priberam da Língua Portuguesa. Dicionário online de Português. https://dicionario.priberam.org