Universidade do Minho
Escola de Direito

Bárbara da Rosa Lazarotto

A "desencriptação coativa de telemóveis" e as consequências em processo penal

setembro de 2021

A "desencriptação coativa de telemóveis" e as consequências em processo penal
Bárbara da Rosa Lazarotto
Uminho | 2021

Universidade do Minho
Escola de Direito

Bárbara da Rosa Lazarotto

A "desencriptação coativa de telemóveis" e as consequências em processo penal

Dissertação de Mestrado
Mestrado em Direito Judiciário

Trabalho efetuado sob a orientação da
Professora Doutora Flávia Noversa Loureiro

setembro de 2021

AGRADECIMENTO

Dirijo o meu profundo agradecimento à Prof.ª Doutora Flávia Noversa Loureiro, por ter aceitado percorrer ao meu lado esta longa e desafiante caminhada de trabalho e empenho. Agradeço sinceramente a dedicação, disponibilidade, paciência e profissionalismo.

Também agradeço meus colegas e amigos, que estiveram comigo neste percurso, no qual enfrentamos adversidades que pareciam intransponíveis.

Por fim, agradeço aos meus pais e familiares, por me acompanharem e apoiarem durante este percurso académico e ao longo da minha vida.

DECLARAÇÃO DE INTEGRIDADE

Declaro ter atuado com integridade na elaboração do presente trabalho académico e confirmo que não recorri à prática de plágio nem a qualquer forma de utilização indevida ou falsificação de informações ou resultados em nenhuma das etapas conducente à sua elaboração.

Mais declaro que conheço e que respeitei o Código de Conduta Ética da Universidade do Minho.

RESUMO

O presente estudo visa abordar a criptografia como obstáculo à realização de investigações criminais, tendo como principal foco a análise da possibilidade da transposição deste obstáculo através da desencriptação coativa de telemóveis. Neste contexto, encontramos um aparente conflito entre a prática de crimes com o auxílio de aparelhos eletrónicos como os telemóveis, que se utilizam da criptografia como método de proteção de dados, a necessidade do Estado de investigar tais ilícitos.

Para tanto, o presente trabalho está dividido em três partes. A primeira parte respeita à apresentação dos conceitos de criptografia e a exposição das questões relevantes a ela associadas, encerrando o capítulo com uma abordagem acerca da utilização da criptografia como método de acobertamento de crimes.

Na segunda parte, adentraremos na temática da desencriptação coativa de telemóveis, abordando se este método seria passível de ser utilizado em Portugal. Para tanto iremos apontar como outros países já se utilizam desta técnica, além de realizaremos uma profunda análise jurídica e jurisprudencial do dever de cooperação do arguido no âmbito do Direito Processual Penal.

Por fim, na terceira parte apresentaremos as eventuais consequências da desencriptação coativa de telemóveis. Para tanto, optamos por dividir o capítulo em duas partes, nomeadamente as consequências para os direitos fundamentais do arguido e consequências jurídico-processuais relativamente as proibições de prova e seus efeitos como o efeito à distância, a teoria das três esferas concêntricas e as invalidades processuais decorrentes de tal prática.

Palavras-chave: Arguido, desencriptação coativa, direitos fundamentais, telemóveis.

ABSTRACT

This study aims to address cryptography as an obstacle to criminal investigations, having as its main focus the analysis of the possibility of overcoming this obstacle through the coactive decryption of mobile phones. In this context, we find an apparent conflict between the practice of crimes with the aid of electronic devices such as mobile phones, which use cryptography as a method of data protection, the need for the State to investigate such crimes.

Therefore, this work is divided into three parts. The first part concerns the presentation of the concepts of cryptography and the exposure of relevant issues associated with it, closing the chapter with an approach to the use of cryptography as a method of covering up crimes.

In the second part, we will explore the theme of the coactive decryption of mobile phones, addressing whether this method could be used in Portugal. In order to do so, we will point out how other countries are already using this technique, in addition to carrying out a thorough legal and jurisprudential analysis of the defendant's duty of cooperation in the scope of Criminal Procedural Law.

Finally, in the third part, we will present the possible consequences of the coactive decryption of mobile phones. To this end, we chose to divide the chapter into two parts, namely the consequences for the defendant's fundamental rights and legal consequences -procedural regarding the prohibitions of proof and its effects such as the effect at a distance, the theory of the three concentric spheres and the procedural invalidities resulting from such practice.

Key-words: Cell phones, compelled decryption, defendants, fundamental rights.

ÍNDICE

SIGLAS E ABREVIATURAS

Ac. – Acórdão

a.C. – antes de Cristo

CEDH – Convenção Europeia dos Direitos do Homem

CPP – Código de Processo Penal

CRP – Constituição da República Portuguesa

EU – União Europeia

MP – Ministério Público

n.º · número

p. – página

pp. · páginas

ss. – seguintes

STJ – Supremo Tribunal de Justiça

TC – Tribunal Constitucional

TEDH – Tribunal Europeu dos Direitos do Homem

INTRODUÇÃO

A tecnologia tem uma relação simbiótica com o ser humano, faz parte, influencia e modifica o seu modo de viver ao mesmo tempo que é fortemente influenciada e modificada por ele. Passamos de seres completamente rudimentares para a invenção da roda, que nos propiciou desenvolver a agricultura, facto que milhares de anos depois nos levou à criação dos computadores e telemóveis.

A popularização da internet foi um dos maiores impulsionadores de avanços tecnológicos dos últimos séculos. Em poucas décadas passamos de ter apenas telefones residenciais para possuirmos aparelhos que detêm mais capacidade do que a foguete espacial que levou o homem à lua.

Atualmente, a maioria de nós tem um aparelho telemóvel com acesso à internet que nos permite consultar correio eletrónico, diversas redes sociais, realizar transações bancárias, nos conectarmos com pessoas a milhares de quilómetros de distância. Todas estas ações geram uma grande quantidade de dados que são armazenados nos telemóveis, que passaram a conter mecanismos de proteção de dados, chamados de encriptação. Contudo, à medida que a internet se popularizou, novas formas de crimes também se vulgarizaram. Assim, temos hoje os cibercrimes, cometidos inteiramente na internet, e os crimes comuns, que são cometidos fora da internet, mas que podem ter o auxílio dela.

A necessidade de investigação destes crimes entrou em conflito com as barreiras impostas pelas ferramentas de privacidade nos telemóveis. Por isso, podemos dizer que, atualmente, nos encontramos diante de um embate entre os métodos de encriptação de telemóveis, que visam a proteção de dados dos usuários, e a necessidade de prevenir, investigar e reprimir a criminalidade, que muitas vezes parecem impor o acesso a tais dados.

Diante deste conflito, diversos métodos de aceder aos dados armazenados nos aparelhos foram criados, uns demandam um

investimento alto, outros implicam em uma grande vulnerabilidade dos sistemas operacionais. Assim, uma alternativa mais simples e efetiva surgiu: a desencriptação coativa de telemóveis.

Portanto, o objetivo deste estudo será apresentar em que consiste a desencriptação coativa de telemóveis, a possibilidade jurídica da sua aplicação em Portugal e as consequências dela. Optamos portanto por dividir a presente monografia em três partes.

Na primeira parte, iremos realizar uma análise acerca da criptografia, o seu surgimento e desenvolvimento até tornar-se altamente tecnológica nos dias atuais. Em seguida abordaremos como a criptografia passou a ser aplicada nos telemóveis, com suas vantagens de proteção de dados e suas desvantagens que emergem como uma grande ameaça em uma sociedade altamente tecnológica, a proteção de comportamentos ilícitos pela criptografia.

Na segunda, procederemos à análise da desencriptação coativa de telemóveis em outros ordenamentos jurídicos e a possibilidade da sua aplicação no ordenamento jurídico português, tendo por base o dever de cooperação do arguido. Por fim, abordaremos como os dados informáticos poderão ser utilizados no âmbito do processo penal como prova digital, a necessidade de regramento específico e especializado para fins de garantir a integridade da prova e sua confiabilidade.

Na terceira e final parte, procedemos com a análise das consequências jurídicas da desencriptação coativa, para tanto optaremos por dividir o capítulo em duas partes, nomeadamente as consequências para os direitos fundamentais do arguido e a segunda referente às consequências jurídico processuais desta prática.

CAPÍTULO I - A CRIPTOGRAFIA E SUAS REPERCUSSÕES

O assunto central do presente estudo é a criptografia como um obstáculo para a busca de dados informáticos para fins de persecução penal. Por este motivo, entendemos ser necessário realizar uma breve análise da criptografia, da sua história e de conceitos básicos relativos à ela para uma melhor compreensão da matéria e da profundidade dos temas abordados neste estudo. Contudo, ressaltamos que não iremos abordar a vertente técnica da criptografia tendo em vista que este não é o foco central do trabalho.

1. O conceito e funcionamento da criptografia

A criptografia pode ser definida como a ciência da escrita secreta, que tem como principal objetivo esconder o significado de uma mensagem[1]. Esta definição remonta às origens artesanais da criptografia, tendo em vista que este sistema existe há séculos[2] e foi muito utilizado em diversas alturas, por exemplo, por Julius Caesar, com o "*Caesar Cipher*". Nota-se, portanto, que a criptografia surgiu voltada às táticas militares.

O primeiro estudo acerca da criptografia surgiu durante a Idade Média e o primeiro impresso a respeito do tema intitulava-se "*Polygraphiae*" [3] e foi publicado em 1510 por um abade alemão chamado Johannes Trithemius[4], que até hoje é considerado o pai da criptografia moderna.

[1] PAAR, Christof e PELZL, Jan, *Understanding Cryptography: A textbook for Students and Practitioners*, Nova Iorque, Editora Springer, 2010, p. 03.
[2] Os primeiros recursos de proteção de dados surgiram em 700 a.C. na Grécia antiga através de uma ferramenta chamada de "Bastão de Licurgo", esta tecnologia evoluiu ao longo dos séculos.
[3] Como aponta Francisco de Paula Souza de Mendonça Júnior a obra possuía rodas circulares com ponteiros móveis, apresentando um alfabeto criptográfico com letras do alfabeto romano, permitindo realizar a tradução de um alfabeto para o outro. Vide *Artífice do Segredo: O Abade Johannes Trithemius (1462-1516) Entre o Magus e o Secretarium do Princeps*, Dissertação de Mestrado na Faculdade de Filosofia e Ciências Humanas da Universidade Federal de Minas Gerais, Belo Horizonte, 2009.
[4] Noel Brann sustenta que Trithemius obteve tamanho renome que atraiu estudantes, pesquisadores e sábios de toda a Europa que iam à Sponheim pesquisar s estudar na sua biblioteca ou aconselhar-se com o abade. Cf., BRANN, Noel L. *Trithemius and Magical Theology: A Chapter in the Controversy over Occult Studies in Early Modern Europe*, State University of New York Press, 1998.

A lógica rudimentar e militarizada perdurou até à Segunda Guerra Mundial, na qual a criptografia continuou a ser utilizada para transporte de táticas de guerra, contudo sofreu uma profunda modificação com a automatização com o auxílio de computadores. Os alemães criaram uma máquina eletromecânica conhecida como "Enigma", apontada por MANUEL JOSÉ LUCENA LÓPEZ como "o mais sofisticado engenho de codificação até então inventado"[5]. Com o auxílio do computador, os alemães garantiram vantagem militar no início conflito, o que mudou com a quebra do sistema por parte dos britânicos com o auxílio de Alan Turing[6], o que eventualmente contribuiu para o triunfo dos aliados[7].

O Enigma foi apenas o primeiro passo do futuro que se seguiu, com a criação e desenvolvimento dos novos computadores a capacidade de criptografar mensagens e de quebrá-las se desenvolveu muito. Por este motivo, como aponta AUGUSTO MARCACINI[8], atualmente a criptografia é considerada uma ramificação da criptologia[9]. O nível empregado de tecnologia e de sofisticação é muito maior que a criptografia antiga, o que fez com que a sua finalidade deixasse de ser apenas militar e passasse a ser comum em empresas e serviços[10], como por exemplo, em transações eletrónicas por meios de cartões de crédito, codificação de sinais de televisões por assinatura e principalmente, na internet.

Atualmente, a criptografia consiste na manipulação matemática das informações, que baralha um determinado conteúdo, tornando-o ininteligível. Para isso, o sistema utiliza de três algoritmos distintos, o primeiro usa o texto simples e aplica a chave de criptografia tornando o

[5] Cf.,LÓPEZ, Manuel José Lucena, *Criptografia y seguridad em computadores*, 3ª edição, Universidad de Jaén, 2001, p. 20.
[6] Alan Turing foi um matemático britânico, pioneiro na computação e considerado o pai da ciência computacional e da inteligência artificial.
[7] É possível assistir os esforços dos britânicos para decifrar o Enigma no Filme "The Imitation Game" de 2014.
[8] MARCACINI, Augusto Tavares Rosa, *Direito e Informática: uma abordagem jurídica sobre a criptografia*, São Paulo, 2010, p. 19.
[9] Criptologia trata tanto de métodos de proteger dados quanto de métodos de violar a criptografia.
[10] National Academies of Sciences, Engineering, and Medicine. *Decrypting the Encryption Debate: A Framework for Decision Makers*, National Academies Press, 2018, p. 18.

texto criptografado; o segundo, recebe o texto cifrado; e o terceiro é a chave que retorna o texto simples[11] [12].

Os métodos de encriptação evoluíram à medida que a tecnologia avançou. Nos anos 70, o método mais comum de encriptação era o *Secure Desk Telephone* – STU, que foi utilizado no âmbito governamental e posteriormente substituído pelo STU-II, em 1975, e, consequentemente, pelo STU-III, em 1977[13]. Com a invenção da internet e do telemóvel, a criptografia ganhou diferentes contornos. Desde então o método de encriptação mais utilizado tem sido o *Advanced Encryption Standard* – AES[14]. Esta popularização da criptografia é tamanha que por muitas vezes ela é utilizada sem que tenhamos consciência. Ela está presente em computadores, em aplicações de correio eletrónico e nos telemóveis, visando proteger a confidencialidade e a integridade das informações[15].

Como ressaltaremos por inúmeras vezes neste estudo, um dos principais componentes da criptografia é a chave. Sem a chave criptográfica não é possível quebrar a criptografia e decifrar o conteúdo criptografado. A respeito deste tema, a criptografia atual pode ser dividida em dois métodos, a criptografia simétrica e assimétrica.

Na criptografia simétrica a chave é a mesma para criptografar e decodificar a mensagem[16], por isto neste caso é necessário manter em sigilo esta chave tendo em vista que é ela que preserva a segurança da informação. Porém, como ressalta AUGUSTO TAVARES ROSA MARCACINI[17], o método simétrico tem limitações tendo em vista que as partes devem ter um segundo meio seguro de comunicação que permita combinar a chave secreta, além disso, caso seja necessário ter diversas

[11] Advanced Encryption Standard (AES): What It Is and How It Works, disponível em <https://securityboulevard.com/2020/04/advanced-encryption-standard-aes-what-it-is-and-how-it-works/ > Acesso em 10 de abril de 2021.
[12] National Academies of Sciences, Engineering, and Medicine. *Decrypting the Encryption Debate: A Framework for Decision Makers*, National Academies Press, 2018, p. 18.
[13] The History of Secure Phones, disponível em <https://www.mssdefence.com/blog/secure-phones-history/ > Acesso em 10 de abril de 2021.
[14] RIJMEN, Vincent, DAEMEN, Joan, *Advanced encryption standard. Proceedings of Federal Information Processing Standards Publications*, National Institute of Standards and Technology, 2001, pp. 19-22.
[15] *Idem*, Decrypting the Encryption Debate, p. 18
[16] OLIVEIRA, Ronielton Rezende, Criptografia simétrica e assimétrica: os principais algoritmos de cifragem, *Segurança Digital Revista Online*, n.º 31, pp. 11-15.
[17] *Ibidem* MARCACINI, 2010, p. 30.

conversas com diversas pessoas, serão necessárias chaves diferentes para cada uma.

A criptografia assimétrica por sua vez, é mais recente, teve desenvolvimento em 1976, por Whitfield Diffie e Martin Hellman[18]. Diferentemente da simétrica, a criptografia assimétrica é compostas de duas chaves, uma privada e outra pública: uma vez criptografada com a chave pública esta não poderá ser desencriptografada com a mesma chave e vice-versa[19]. Este método é considerado mais rápido e eficaz do que a criptografia simétrica, permitindo que a mensagem seja enviada a mais de um destinatário evitando diversas chaves públicas. É por este motivo que este método que é utilizado em operações bancárias e demais aplicações com o uso da internet.

Como ressaltamos anteriormente, o foco principal da criptografia está na chave que irá garantir a sua segurança e confiabilidade. Como bem explica AUGUSTO MARCACINI, uma chave com oito *bits* poderá representar um número entre 0 e 255, com dez *bits* representa um número entre 0 e 123. Atualmente, as chaves com 128 *bits* têm 39 algarismos e são consideradas seguras, segundo o autor caso seja necessário descobrir uma chave de 39 algarismos serão necessários 10.790.283.070 anos utilizando-se um bilião de computadores que trabalharão durante 24 horas[20]. MANUEL LUCENA LÓPEZ ainda sustenta que nesta hipótese não há energia disponível no universo para construir um computador capaz de decifrar estas combinações[21].

Nota-se, portanto, que toda a segurança da criptografia se resume na chave que irá decifrar a mensagem protegida. Quanto maior e mais complexa, mais difícil será decifra-la, uma vez descoberta a chave o método mais sofisticado de criptografia não é capaz de proteger a mensagem[22].

---

[18] DIFFIE, Whitfield e HELLMAN, Martin E., New Directions in Cryptography, IEEE Transactions on Information Theory, Vol. IT-22, n.º 6, November 1976. Disponível em: https://ee.stanford.edu/~hellman/publications/24.pdf

[19] MARCACINI, Augusto Tavares Rosa, O documento eletrônico como meio de prova, São Paulo, Novembro, 1999, Disponível em: https://simagestao.com.br/wp-content/uploads/2016/05/Odocumentoeletronicocomomeiodeprova.pdf

[20] *Ibidem,* MARCACINI, 2010, p. 48

[21] *Ibidem,* LÓPEZ, 2001, p. 22.

[22] Por isto, especialistas recomendam que as chaves criptográficas sejam longas e que não tenham relação com dados pessoais, nome do cônjuge ou dos filhos, número de documentos e afins. Especialistas recomendam que usem números, letras e símbolos.

Com os avanços tecnológicos a criptografia passou a ser adotada em aparelhos eletrónicos, como telemóveis, como método de proteção de dados que estejam armazenados, sob os quais este estudo pretende debruçar-se.

O telefone foi inventado em 1875 e logo foi considerado uma revolução e um sucesso na comunicação por voz, pese embora ninguém pudesse imaginar a transformação tecnológica e socioeconómica que este aparelho causaria 145 anos depois. Desde então, com o auxílio da tecnologia, o telefone sofreu profundas transformações, para fins deste estudo iremos apontar duas como principais: a criação do telemóvel em 1982 e a sua junção com a internet.

A criação do telemóvel retirou o caráter fixo do telefone e o tornou, como o próprio nome diz, *móvel*, possibilitando uma comunicação mais rápida e qualquer lugar do mundo. Posteriormente, com a abertura da internet para além dos muros académicos[23], a junção dos telemóveis com a internet criou o que chamamos de *smartphone*.

Os *smartphones* são minicomputadores capazes de concentrar uma enorme quantidade de tarefas em um pequeno aparelho: calculadora, câmara fotográfica, computador, rádio, correio eletrónico, telefone, entre outras ferramentas[24]. São aparelhos extremamente populares: em 2006 74,4% da população portuguesa declarou que tinha telemóvel, já em 2010 o número passou para 88,7%. Este número está distribuído em vários escalões etários, mantendo-se acima dos 85%, exceto com relação às faixas etárias acima dos 65 anos de idade[25]. Este número considerável de utilizadores tem como consequência uma transmissão e o armazenamento de dados constante, fazendo surgir a necessidade da proteção dos

[23] A primeira referência da internet ocorreu em 1965 no *Massachusetts Institute of Technology* – MIT, contudo muito rudimentar. O mecanismo foi sendo refinado e em 1969 a primeira mensagem foi enviada do *Standford Research Institute* (SRI) para o *Network Information Center* na University of California. Até este ponto a internet era fechada para as universidades, este paradigma mudou em 1972 sob o nome de "Internetting". A *Enthernet* foi desenvolvida por Bob Metcalfe na XEROX PARC em 1973 e a partir daí, passou a estar presente nos computadores da empresa. 1985 foi ano do crescimento exponencial da internet e da sua expansão, o que abriu caminho para deixar de ser um sistema livre para a sua comercialização que ganhou fôlego em 1989 e que mantém-se até hoje. Cf., LEINER, Barry M., *et al*. "A brief history of the Internet." *ACM SIGCOMM Computer Communication Review* 39.5 (2009): 22-31. https://dl.acm.org/doi/pdf/10.1145/1629607.1629613.

[24] A partir deste momento, passaremos a nos referir aos telemóveis inteligentes ou *smartphones* apenas por telemóveis.

[25] QUINTANILHA, Tiago Lima, CARDOSO, Gustavo, ESPANHA, Rita, A apropriação dos Telemóveis na Sociedade em Rede, *A Sociedade em Rede*, 2010, p. 06.

mesmos, sendo desta forma que a criptografia passou a ser utilizada nos telemóveis.

Existem diversos métodos criptográficos utilizados nos telemóveis, que variam a depender da marca e da tecnologia dos dispositivos, alguns abrangem todos os dados armazenados, chamados de *Full Disk Encryption*[26], outros apenas parte deles, a mesma lógica aplica-se para o nível de proteção conferido pela criptografia, alguns são mais sofisticados que outros.

Os aparelhos telemóveis chamados "Iphones" da marca Apple tem os seguintes métodos de criptografia: *" (...) hardware-and-software-based encryption of their password-protected contents. (...) These protections safeguard the encryption keys on the device with a passcode designated by the user during setup. This passcode immediately becomes entangled with the Iphone's Unique ID ("UID"), which is permanently assigned to that one device during the manufacturing process. The Iphone's UID is neither accessible to other parts of the operating system nor known to Apple"* [27]. Já os aparelhos que utilizam do sistema operacional Android utilizam a criptografia baseada em arquivo que permite que diferentes arquivos sejam criptografados com diferentes chaves que podem ser desbloqueadas independentemente[28].

O que nós utilizadores conseguimos "ver" da encriptação nos telemóveis é pouco. Quando ativamos o ecrã do aparelho, teremos algumas opções a depender do modelo: palavras-passe, gestos – normalmente ligação entre pontos – e a utilização de dados biométricos tais como impressão digital, íris, reconhecimento por voz e reconhecimento facial[29]. Estes gestos simples de desbloqueio de ecrã nada mais são do que a

[26] *Full Disk Encryption* – FDE, que significa que o disco do aparelho telemóvel é encriptado inteiramente. Entretanto, ainda há alguma diferença de utilização deste método de encriptação a depender da marca de telemóvel. Os aparelhos telemóveis da marca Apple que tenham o sistema operacional do iOS 8 em diante são dotados do sistema de FDE e são inacessíveis por terceiros. O sistema operacional Android não é centralizado, tendo em vista que é utilizado por aparelhos produzidos por marcas diversas, portanto apenas 10% dos aparelhos que utilizam Android tem FDE, contudo esta tendência tem vindo a espalhar-se.
[27] Segundo a própria empresa em manifestação no âmbito do processo Apple v. FBI, que será melhor abordado adiante: Disponível em: https://epic.org/amicus/crypto/apple/In-re-Apple-Motion-to-Vacate.pdf acesso em 21 de maio de 2021.
[28] Acerca da criptografia do sistema operacional Android Disponível em: https://source.android.com/security/encryption acesso em 21 de maio de 2021.
[29] CHOONG, Yee-Yin, FRANKLIN, Joshua M., GREENE, Kristen M., *Usability and Security Considerations for Public Safety Mobile Authentication, Maryland*, National Institute of Standards and Technology, 2016, p. 11.

inserção da chave criptográfica no aparelho, tornando os dados protegidos inteligíveis.

É importante ressaltar que, a depender do método utilizado, haverá uma camada de proteção mais sofisticada, portanto mais difícil de ser corrompida. Como ressaltamos anteriormente, quanto maior a palavra-passe, mais difícil será solucionar o enigma da encriptação e, consequentemente, aceder às informações. A mesma lógica é aplicável aos dados biométricos, que são dados biológicos únicos, como a leitura facial, impressão digital, voz e íris[30] que são armazenados e a partir deles é criada uma chave[31].

Além do sistema criptográfico do próprio aparelho telemóvel, existem camadas complementares de criptografia fornecidas pelas aplicações utilizadas pelos utilizadores. Muitos deles têm adotado um método de encriptação que se chama "encriptação de ponta a ponta" – em inglês *end to end encryption – E2E*. Este método de encriptação protege todos os pontos da troca de mensagens, sendo que as chaves de proteção da encriptação que integram o sistema estão restritas aos interlocutores, mudando a cada mensagem enviada e não com o servidor.

De acordo com o engenheiro cofundador do aplicativo "Whatsapp", não é possível desencriptar mensagens já transmitidas, tendo em vista que o servidor armazena as informações encriptadas e apenas os usuários têm as chaves. Isto posto, uma vez que seja necessário aceder às informações de alguma conversa de algum indivíduo em específico, é necessário aceder ao telemóvel ou retirar as chaves de todos os usuários do referido aplicativo para que a mensagem de um deles seja desencriptada[32].

Diante do exposto, podemos observar que a criptografia é de extrema importância na proteção de dados dos indivíduos, contudo é possível observar que esta mesma característica pode ser utilizada para outros fins

---

30 KEENAN, Thomas P., *Replacing Something Bad with Something Worse: Why Biometric Authentication Will Be So Creepy*, Canada, University of Calgary, 2016.

31 CAVOUKIAN, Ann, STOIANOV, Alex, Biometric Encryption. In: TILBORG Henk, JAJODIA, Suschil, *Encyclopedia of Cryptography and Security*, Springer, Boston, 2011.

32 AFFONSO, Filipe José Medon. A criptografia na era dos bloqueios do WhatsApp: uma análise segundo a metodologia civil-constitucional. *In* TEPEDINO, Gustavo et al. (Coord.). *Anais do VI Congresso do Instituto Brasileiro de Direito Civil.* Belo Horizonte, Editora Fórum, 2019. p. 299-324.

que não sejam a proteção de dados e sim como um escudo para comportamentos ilícitos.

1.1 Os crimes e a internet

A internet enfrentou profundas mudanças desde a sua popularização nos anos 1990 do século passado, passou de um espaço de divertimento e comunicação para um ambiente multifacetado com inúmeras possibilidades. Atualmente é possível apontar que a internet está tão infiltrada na vida dos indivíduos que é possível traçar um roteiro de um dia apenas se utilizando dos dados informáticos que deixam rastros dos passos de alguém[33].

MANUEL DA COSTA ANDRADE afirma que a evolução da sociedade está associada à evolução dos modelos de comunicação[34], e, de facto, é possível afirmar que a internet é considerada o catalisador da terceira revolução industrial[35] que vivemos. Ela foi capaz de interligar os computadores que se popularizaram na década de 90 através de uma rede criando novas formas de organização e estruturação nunca antes vistas, o que mudou as relações e os padrões de vida até então vigentes[36].

Por isso, alguns autores, como MARCO ANTONIO ZANELLATO[37], afirmam que não vivemos mais em uma sociedade moderna, mas sim em uma sociedade digital, também chamada de "Sociedade *bit*"[38]. ULRICH BECK, por sua vez, sustenta que vivemos em uma "Sociedade do Risco"[39] na qual a tecnologia é um dos riscos que estão ligados diretamente à

[33] COSTA, José de Faria, *As telecomunicações e a privacidade: o olhar (in)discreto de um penalista*, Coimbra, Coimbra Editora, 1999, p. 161.
[34] ANDRADE, Manuel da Costa, *Liberdade de Imprensa e Inviolabilidade Pessoal*, Coimbra, Coimbra Editora, 1996, p. 66-67.
[35] SMITH, Bradford, The third Industrial Revolution, *Policymaking and Technology Law Review*, n.º 3, 2000, p. 242.
[36] VATTIMO, Gianni, *A sociedade transparente*, Lisboa, Editora Relógio d'Água, 1992, p. 10-11.
[37] ZANELLATO, Marco Antonio, Condutas ilícitas na sociedade digital, Direito e Internet, *Caderno de Escola Superior do Ministério Público de São Paulo*, São Paulo, Ano II, n.º IV, p. 165-228.
[38] ALMEIDA, Reginaldo Rodrigues de, *Sociedade Bit: Da Sociedade da informação à Sociedade do Conhecimento*, Porto, Editora Quid Iuris, 2004, p. 10.
[39] Cf., A Sociedade do Risco aponta para uma sociedade que acumula riscos – ecológicos, financeiros, militares, terroristas, bioquímicos, informacionais – que tem uma presença esmagadora atualmente. *In* BECK, Ulrich, *Sociedade de risco*, São Paulo: Editora 34, 2010, pp. 49-53.

globalização e com a insegurança. As transformações desta sociedade podem ser vistas por todos nós no nosso dia a dia, temos ferramentas tecnológicas que há vinte anos seriam inimagináveis que atualmente são triviais e elas influenciam as nossas vidas também de forma inimaginável.

Neste contexto, à medida que a rede passou a permear muitos aspetos da vida de um indivíduo, a facilidade de tratamento, armazenamento, processamento e transferência de dados informáticos[40], juntamente com a popularização dos aparelhos informáticos fez com que a quantidade de dados informáticos gerados e armazenados crescesse exponencialmente. De acordo com um relatório produzido pela empresa DOMO de gestão de servidores em nuvem, todos os dias são criados 2.5 quintilhões de bytes de dados[41], sendo que 90% de todos os dados já gerados no mundo foram criados desde os anos de 2018 em diante, o que nos demonstra o avanço tecnológico em que vivemos.

Estas transformações não se resumem somente aos dados, como também impactam a ciência, a economia, a saúde, a educação e também o Direito, em especial no processo penal, especialmente em matéria de investigação criminal[42], como bem aponta MIREN JOSUNE PÉREZ ESTRADA[43] *"(...) no se puede cuestionar que la evolución tecnolólica há supuesto um incrementode la calidade de vida y um desarrollo em la estrutura social y económica. Se habla ya de uma nueva civilización caracterizada por la instantaneidade y la desaparicíon de las distancias, pero tambíen es evidente que este gran avance tecnológico perjudica, en ocasiones, los intereses ajenos. Aparecen nuevos medios para delinquir y ello conlleva la necesidad de investigar dichos delitos a través de los, tambíen, nuevos medios tecnológicos".*

Naturalmente a utilização da tecnologia e da internet também passou a ser utilizada para fins ilícitos, abrindo o caminho para um novo tipo de criminalidade, que se utiliza de aparelhos informáticos para o

[40] DEL CANTO, Enrique Rovira, Delincuencia informática y fraudes informáticos. Editorial Comares, 2002, 96-97.
[41] MARR, Berbard, How much data do we create very day? The mind-blowing stats everyone should read. Forbes Magazine, disponível em: shorturl.at/ahxKZ acesso em 06 de junho de 2021.
[42] RODRIGUES, Benjamim da Silva, *Da Prova Penal – Tomo IV: da prova eletrónico-digital e da criminalidade informático-digital,* Lisboa, Editora Rei dos Livros, 2008, p. 102.
[43] ESTRADA, Miren Josune Pérez, La investigacíon del delito a través de las nuevas tecnologías. Nuevos medios de investigacíon em el processo penal, *In* ARZAMENDI, José Luis de la Cuesta, *Derecho Penal Informático*, 1ª edición, Civitas, 2010, p. 306-307.

cometimento de crimes, como bem aponta CLAUDE DECHAMPS *"comme toute invention humaine porteuse de progrès, elle engendre dês comportements déviants et une nouvelle forme de délinquance: la cybercriminalité"*[44].

Esta nova categoria de crimes forçou uma adaptação do Direito Penal e Direito Processual Penal, demandando novas modalidades de crimes e novas formas de comissão, demandando a criação de tipos penais amplos e indefinidos, como aponta VERA MARQUES DIAS[45].

Foi neste contexto que surgiu a Lei da Criminalidade Informática – Lei n.º 109/91 de 17 de agosto –, que se limitava a prever tipos penais e suas respetivas penas. Contudo, desde a sua promulgação em 1991, a área tecnológica teve grandes avanços, o que fez com uma série de adaptações fossem realizadas para acomodar os novos factos jurídicos que passaram a surgir. Foi neste ponto que foi feita uma reforma ao Código de Processo Penal em 2007, que alargou a aplicação do artigo 190.º, que passou a determinar: "o disposto nos artigos 187.º, 188.º e 189.º é correspondentemente aplicável às conversações ou comunicações transmitidas por qualquer meio técnico diferente do telefone, designadamente correio electrónico ou outras formas de transmissão de dados por via telemática, bem como a interceção das comunicações entre presentes".

Contudo, esta reforma demonstrou-se inefetiva, pois aplicou um meio de obtenção de prova à um meio de prova completamente distinto ao que se propunha originalmente. MANUEL DA COSTA ANDRADE[46] conceituou esta reforma como uma "casa de horrores hermenêuticos", tendo em vista que englobou realidades distintas, causando incerteza e insegurança.

A verdadeira mudança somente ocorreu com a ratificação de Portugal à Convenção de Budapeste[47] a respeito da criminalidade

[44] DECHAMPS, Claude, *Cybercriminalité*, La Commission de la Defense Nationale et des Forces Armées, Avril 2005, p. 99.
[45] DIAS, Vera Elisa Marques, *A problemática da investigação do cibercrime*, Trabalho de conclusão do I Curso de ppós-graduação de aperfeiçoamento em direito da investigação criminal e da prova, Universidade de Lisboa, Faculdade de Direito, 2010, p. 32.
[46] COSTA ANDRADE, Manuel da, *Bruscamente no Verao Passado: a reforma de Processo Penal,* Coimbra, Coimbra Editora, 2006, p. 185.
[47] A Convenção sobre a Cibercriminalidade – também chamada de Cciber – foi assinada em Budapeste em 23 de Novembro de 2001 e teve por base a evolução das novas tecnologias da informação e a sua utilização para fins criminosos, o que se tornou um problema de difícil regulamentação em âmbito Europeu. A Convenção visou criar mecanismos para harmonizar elementos

informática, considerada "o primeiro e mais importante trabalho internacional de fundo sobre crime no ciberespaço"[48], que deu origem a Lei n.º 109/2009, de 15 de setembro.

A Lei n.º 109/2009, chamada de Lei do Cibercrime[49], como bem ressaltou o Tribunal da Relação de Lisboa no Acórdão do dia 22-01-2013 no Processo n.º 581/12.6PLSNT-A.L1-5[50], superou a Lei da Criminalidade Informática que estava em vigor até então, tendo em vista que esta não continha normas processuais que adequassem o regime processual às particularidades da investigação.

Na nova Lei do Cibercrime, novos tipos penais de cibercrimes[51] foram criados juntamente com novos meios de obtenção de prova adaptados para os meios de prova digital, ao mesmo tempo que revogou tacitamente parcelas do artigo 187.º a 190.º do Código de Processo Penal, como defendem PAULO DÁ MESQUITA[52] E RITA CASTANHEIRA NEVES,[53] bem como a jurisprudência no Acórdão do Tribunal da Relação de Évora de 20-01-2015[54].

Apesar do nome, a Lei do Cibercrime deixou de conceituar exatamente o que são os cibercrimes. Na doutrina, os crimes na internet ou que ocorrem com o auxílio dela assumem diversas nomenclaturas, como crime digital, crime informático, crime informático-digital, na língua inglesa *high technology crimes* ou *computer-related crime*[55]. Alguns conceitos são mais restritos que outros.

---

de direito penal material e disposições conexas em matéria de cibercriminalidade além de fornecer ferramentas e poderes necessários ao direito processual penal à instrução e perseguição de infrações cometidas por meio de um sistema informático ou em situações que existam provas sob forma eletrónica. Cf., *Ibidem,* RODRIGUES, 2008, p. 314-317.

[48] Cf., Exposição dos Motivos da Proposta de Lei n.º 289/X/4ª – Lei do Cibercrime.

[49] A Lei n.º 109/2009 – Lei do Cibercrime sucedeu a Lei da Criminalidade Informática n.º 109/91 de 17 de agosto. A Lei do Cibercrime foi resultado da ratificação de Portugal a Convenção sobre o Cibercrime, que visou uniformizar a previsão dos crimes cibernéticos e criar instrumentos processuais modernizados nos Estados-Parte, viabilizando a cooperação Estatal. Que além de criar novos tipos penais voltados à criminalidade informática, também criou novos meios de obtenção de prova, dentre eles a pesquisa de dados informáticos. Cf., VERDELHO, Pedro, A nova lei do Cibercrime, *Scientia Juridica*, LVIII, Braga, 2009, p. 258

[50] Acórdão do Tribunal da Relação de Lisboa, Processo n.º 581/12.6PLSNT-A.L1-5 de 22-01-2012, Disponível em shorturl.at/huzEZ acesso em 03 de abril de 2020.

[51] Cf., Entre os artigos 3.º e 8.º da Lei do Cibercrime, nomeadamente a falsidade informática, o dano relativo a programas ou dados informáticos, a sabotagem informática, o acesso legítimo, a interseção ilegítima e a reprodução ilegítima de programa protegido.

[52] *Ibidem* MESQUITA, 2010, p. 117.

[53] *Ibidem* NEVES, 2011, p. 280.

[54] Acórdão do Tribunal da Relação de Évora, Processo 648/14.6GCFAR-A.E1, de 20-01-2015, disponível em shorturl.at/gtBV4 acesso de 04 de junho de 2020.

[55] Optamos por adotar a nomenclatura "cibercrime" pois foi esta a opção do legislador. Contudo, adotaremos a sua conceção ampla.

Os cibercrimes em sentido estrito estão listados nos artigos 3.º à 10.º da Lei do Cibercrime e, segundo BENJAMIM SILVA RODRIGUES, são aqueles que consistem em condutas penalmente relevantes que são veiculados a partir de computadores, sistemas, redes informáticas e redes de comunicações eletrónicas[56]. Já PEDRO DIAS VENÂNCIO conceitua os cibercrimes em sentido amplo como toda atividade criminosa que possa ser levada a cabo por meios informáticos, ainda que estes não sejam mais que um instrumento para a prática criminosa, mas que não integre o tipo penal[57].

Como bem sustentou PEDRO VERDELHO, o conceito de cibercrime definido pela Lei do Cibercrime é pouco abrangente diante da realidade social que utiliza da internet para diferentes tipos de crimes, especialmente após a popularização das redes sociais e de aplicativos de mensagens como "WhatsApp" e "Telegram". Por isso, o autor aponta três tipos de cibercrimes: os que recorrem a meios informáticos, os crimes referentes à proteção de dados pessoais e os crimes informáticos propriamente ditos[58]. Este posicionamento também é adotado pela Comissão Europeia[59].

Levando em consideração a complexidade da relação entre a internet e o cometimento de crimes, optamos por adotar o conceito amplo de cibercrime defendido pelo autor Pedro Verdelho, tendo em vista a importância dos aparelhos eletrónicos na vida dos indivíduos e a permeabilidade da internet nas tarefas diárias. Compreendemos que um conceito jurídico demasiadamente restrito teria relevância direta na resposta penal[60] e ignoraria uma nova gama de tipos penais que cada vez se torna mais comum.

Apesar da tecnologia disponível atualmente, as autoridades ainda têm grandes dificuldades de investigar a criminalidade informático-digital em razão de alguns fatores: o alto grau de tecnicidade dos agressores que

---

[56] *Ibidem* SILVA RODRIGUES, 2009, p. 279.
[57] *Ibidem* VENÂNCIO, p. 17.
[58] VERDELHO, Pedro, Cibercrime *In Direito da Sociedade da Informação*, n.º IV, pp.347-348.
[59] European Union Legislation, Fight against organized crime *In* https://eur-lex.europa.eu/summary/chapter/2308.html acesso em 06 de setembro de 2021
[60] Cf., NUNES, Duarte Rodrigues, *Os Meios de Obtenção de Prova previstos na Lei do Cibercrime*, Coimbra, Editora Getlegal, 2018, p. 12.

se modifica com rapidez exponencial e a falta de meios disponíveis para os investigadores que estejam no mesmo patamar da tecnologia disponível para os agressores, por exemplo, a criptografia[61].

1.2 O uso da criptografia no acobertamento de crimes

A adoção da criptografia como um método de proteção de dados veio a calhar, tendo em vista que, ao mesmo tempo que é uma forma de proteção de dados, também se torna um escudo de dados informáticos que indiquem o cometimento de crimes e demais ilícitos, como bem aponta ORIN S. KERR[62]: *"Encryption is now everywhere. Most Americans carry an encrypted device with them, and all are free to use strong encryption to protect their data. As a result, technology has inserted a remarkably powerful password gate in the way of routine searches across a wide range of cases".*

Este tema também tem sido discutido no âmbito europeu, especialmente após ataques terroristas ocorridos entre os períodos de 2014 e 2016[63], desde então soluções de como ter acesso legítimo a evidências digitais tem sido discutidas. Em resposta, a Comissão propôs a realocação de fundos para dar suporte às forças investigativas e o âmbito judiciário. Com isso surgiu a plataforma de desencriptação promovida pelo *European Cybercrime Centre* (EC3) da Europol, inaugurada em 2016 e o permitiu o desenvolvimento de uma nova plataforma inaugurada em 2020 pela Europol em cooperação com o Centro Comum de Investigação da Comissão Europeia.

O crime de pornografia de menores, disposto no artigo 176.º do Código Penal, é composto de diversas ações relacionadas com materiais relativos a menores. Este crime encontrou solo fértil na internet devido à

[61] *Ibidem,* RODRIGUES, 2008, p. 460.
[62] KERR, Orin S., Compelled Decryption and the Privilege Against Self-Incrimination. *Texas Law Review,* n.º 97, 2018, pp. 767.
[63] Nomeadamente o tiroteio no Museu Judaico da Bélgica em maio de 2014, os ataques em novembro de 2015 em Paris e o ataque a um caminhão em Nice em julho de 2016, os atentados a bomba em Bruxelas em março de 2016 e o Ataque no Aeroporto Ataturk em junho de 2016.

facilidade de compartilhamento e a grande capacidade de armazenamento dos computadores. A criptografia tornou ainda mais difícil a investigação deste crime. Um estudo da Universidade de Portsmouth[64] apontou que *websites* de pornografia de menores somavam 83% do conteúdo da *dark net*[65]. Em razão disto, a Comissão Europeia criou recentemente um grupo de discussão de meios para combater a pornografia infantil[66] e apontou como um dos obstáculos a encriptação[67].

O tráfico de drogas, um ilícito penal que tradicionalmente não depende da tecnologia, também passou a adotá-la como auxílio na logística e na venda estupefacientes. Esse é um movimento que tem ocorrido em todos os níveis da cadeia de venda, desde o produtor até os grandes cartéis[68] mexicanos que se utilizam aplicações criptografadas como auxílio na comunicação dos grupos, algumas inclusive desenvolvidas pelos próprios cartéis. Traficantes de drogas de menor porte também encontraram nos aplicativos de comunicação como *Whatsapp* uma nova forma de realizar vendas e estarem mais próximos da clientela sem demandar uma exposição em via pública.

As comunicações criptografadas também são canais propícios para a realização de atos preparatórios de outros crimes. Foi possível observar isto claramente com o crescimento exponencial do DAESH também conhecido como "Estado Islâmico". O Estado Islâmico é uma organização jihadista de orientação salafita e wahabita que surgiu após a invasão do Iraque em 2003 e que desde então, tem se utilizado das tecnologias para expandir-se e recrutar membros de diversos países[69]. Estudos mostram

---

[64] OWEN, Gareth e SAVAGE, Nick,The Tor and Dark Net, *Global Comission on Internet Governance Paper Series* n.º 20, Setembro 2015, disponível em shorturl.at/rtFLR acesso em 14 de março 2021.

[65] A *dark net* é o nome dado às páginas da internet que não são facilmente encontradas pelos usuários comuns. Para acessá-los o indivíduo deverá se utilizar de um software especial que permite acesso à conexões criptografadas. Disponível em https://www.cigionline.org/sites/default/files/no20_0.pdf

[66] Neste contexto, a empresa Apple fabricante do telemóvel Iphone anunciou em Agosto de 2021 uma medida de Inteligência Artificial que visa realizar uma análise de fotos armazenadas no serviço de nuvem da empresa para detetar eventuais imagens de cunho de pornografia infantil. Contudo, a empresa deixou claro que tal medida apenas será aplicável às imagens da nuvem e não aquelas armazenadas nos aparelhos telemóveis. O que torna ainda mais complexa a questão da proteção criptográfica dos aparelhos. Vide shorturl.at/eqCPW acesso em 15 de agosto de 2021.

[67] European Commission, *Technical solutions to detect child sexual abuse in end-to-end encrypted communications*, Disponível em < shorturl.at/gvKSW > Acesso em 21 de Abril de 2021.

[68] O'NEILL, Patrick Howell, *How a drug cartel used encryption and a fake website to launder millions*. Disponível em <https://www.dailydot.com/debug/mexican-cartel-encryption/ > Acesso em 21 de Abril de 2021.

[69] IRSHAID, Faisal, Isis, Isil, IS or DAESH? One Group, many names disponível em https://www.bbc.com/news/world-middle-east-27994277 acesso em 13 de maio de 2020.

que os extremistas se utilizam de aplicativos de mensagens como "Telegram"[70] e "Whatsapp"[71] promovem os seus serviços como extremamente seguros de interações externas devido à sua tecnologia de encriptação de ponta a ponta.

A proteção da criptografia foi essencial e possibilitou o crescimento de células terroristas longe dos olhos de agências de inteligência, como aponta GEMA SÁNCHEZ MEDERO[72] *"No obstante, habría que mencionar que los grupos terrorista utilizan técnicas muy diversas para evitar la intercepción de sus mensajes, entre las que cabe destacar la encriptación (...)".* Portanto, a criptografia permite criar um espaço paralelo que permitia a livre associação de indivíduos ao mesmo tempo que protegia a identidade dos mesmos[73]. Um grande exemplo foi Abdelhamid Abaaoud, um extremista islâmico nascido na Bélgica que se utilizou da proteção conferida pela criptografia para treinar indivíduos e ensinar seus seguidores a encriptar os dados dos aparelhos telemóveis e computadores pessoais. Alternativamente, outro grupo extremista, a Al Qaeda, criou o seu próprio sistema de troca de mensagens encriptado chamado Amn al-Mujahideen[74].

Foi neste contexto que surgiu um precedente de extrema importância nos Estados Unidos da América, chamado *Apple v. FBI*[75]. O caso trata a respeito de Syed Fizwan Farook e Tashfeen Malik um casal que realizou um ataque terrorista inspirado no Estado Islâmico na cidade de San Bernardino, no estado da Califórnia. Durante as investigações do ocorrido, o telemóvel de Syed, um Apple Iphone 5C, foi recuperado, todavia os investigadores foram impedidos de aceder aos dados armazenados em

[70] Mary-Ann Russon & Jason Murdock, "Welcome to the Bizarre and Frightening World of Islamic State channels on Telegram," *IB Times*, June 2, 2016, disponível em shorturl.at/copDH, acesso em 6 de setembro de 2021.
[71] SHEHABAT, Ahamad, MITEW, Teodor & ALZOUBI, Yahia, Encrypted Jihad: Investigating the Role of Telegram App in Lone Wolf Attacks in the West, *Journal of Strategic Security,* n.º 10 (3), 2017, pp. 27–53
[72] MEDERO, GEMA SÁNCHEZ, Cibercrimen, Ciberterrorismo y Ciberguerra: Los Nuevos Desafíos Del S. XXI, *Revista Cenipec*, n.º 31, Enero-Diciembre, 2012, pp. 239-267.
[73] *Ibidem* SHEHABAT*et.al., pp.* 27-53.
[74] AHLBERG, Christopher, *How Al-Qaeda uses encryption post-Snowden* (Part 2) – New Analysis in Collaboration with ReveringLabs, Recorded Future, Disponível em shorturl.at/nJUZ8, acesso em 21 de Abril de 2021.
[75] Após o ataque terrorista perpetrado por Syed Rizwan Farook e sua mulher o FBI iniciou as investigações, obtendo ordem de busca e apreensão do veículo utilizado pelo casal, onde foi encontrado um telemóvel da marca Apple Iphone modelo 5C. Em sequencia, o FBI obteve autorização judicial para realizar uma busca no telemóvel apreendido, contudo o mesmo estava protegido por criptografia. O FBI enfrentou uma série de obstáculos na análise pericial do telemóvel em razão da criptografia e em razão disso, solicitou extrajudicialmente auxílio da empresa Apple para desencriptar o referido aparelho. Em um primeiro momento a empresa providenciou um auxílio limitado, que foi considerado incompleto em razão da negativa da empresa em remover o sistema de criptografia, dando início à disputa judicial. Vide ordem judicial que compelia a empresa à assistir a perícia < https://www.justice.gov/usao-cdca/file/826836/download >.

razão da encriptação[76] fornecida de fábrica. Extrajudicialmente, o Federal Bureau of Investigation (FBI) solicitou à empresa Apple que, criasse um novo sistema operacional que possibilitasse o acesso aos dados nestes casos específicos. O juiz da causa ordenou a criação de um novo sistema operacional no prazo de dez dias, a empresa recusou-se a cumprir a ordem judicial, sob a justificativa que isto possibilitaria ao governo aceder a qualquer aparelho telemóvel da marca não sendo assim uma decisão proporcional. Posteriormente, o Governo desistiu da ação intentada, tendo em vista que especialistas encontraram falhas no sistema operacional, o que possibilitou aos investigadores aceder aos dados armazenados e realizar a investigação.

Os atos preparatórios não se resumem aos extremistas islâmicos, em janeiro de 2021, um grupo político radicalizado invadiu o Capitólio dos Estados Unidos da América, ameaçou a vida de congressistas que estavam reunidos no seu interior e causou danos à propriedade pública. Durante a investigação do ocorrido, o *Federal Bureau of Investigation* alertou que extremistas políticos tenderão a se utilizar de métodos encriptados de comunicação para evitar futuras investigações[77] e apontou que foi através destes aplicativos que o grupo organizou o ataque[78].

Em março de 2021, autoridades de França, Bélgica e Países Baixos com o auxílio da Europol, através de uma operação conjunta, obtiveram sucesso em bloquear o uso de uma aplicação de encriptação chamada *Sky ECC*. A operação buscou evitar o uso ilegal de encriptação para fins de acobertamento de crimes[79].

Diante dos exemplos apontados, é possível afirmar já está instalado um conflito entre a proteção da criptografia e a sua utilização como escudo no cometimento de crimes. Este conflito já esteve mais velado, contudo

[76] BURUM, Sue, HOLMES, Georgia, Apple v. FBI: Privacy vs. Security?, *National Social Science*, Vol. 48, Number 02, 2016, p.09.
[77] FRIED, Ina, Feds warn threats are harder to track as extremists shift to encryption, disponível em shorturl.at/ehlCI acesso em 21 de Abril de 2021.
[78] "This is our house!" A preliminary assessment of the Capitol Hill Siege Participants, disponível em shorturl.at/xLMPY acesso em 20 de Agosto de 2021.
[79] Europol Press Release disponível em shorturl.at/ryTU7 acesso em 21 de Abril de 2021.

está lentamente a tornar-se o tema de discussões, tendo em vista a tendência de aumento nos últimos anos[80].

Todavia, não podemos deixar de lado o papel essencial da criptografia na proteção da privacidade dos usuários. Como apontamos inicialmente, cada vez mais ela tem se demonstrado essencial na defesa de direitos fundamentais de sujeitos ao proteger o direito à liberdade de expressão e privacidade, especialmente em países com regimes políticos totalitários, permitindo a organização e a livre manifestação de ativistas e defensores de direitos humanos.

Por outro lado, a utilização da criptografia como uma "tática" para o cometimento de crimes também deve ser levada em consideração, tendo em vista que a medida que vivemos em uma sociedade cada vez mais tecnológica e conectada este não é um tema que pode ser ignorado. Devemos discutir o tema e explorar alternativas sem que avanços como a criptografia se tornem o alvo de um problema mais profundo.

Neste contexto, algumas discussões já se iniciaram[81] com o intuito de propor possibilidades e alternativas de "desviar" da proteção concedida pela criptografia e possibilitar a investigação de crimes. Algumas soluções foram apontadas e dentre elas abordaremos as três principais: a quebra da criptografia por força bruta, a criação de *backdoors* e a decriptação coativa de telemóveis, objeto principal deste estudo.

A quebra da criptografia por força bruta dependerá necessariamente da segurança do método criptográfico empregado. Segundo KERR e SCHNEIER, as chaves criptográficas de 63 e 80 bits já são facilmente quebradas por computadores, contudo as chaves de 128 ou 256 bits ainda não são violáveis[82]. Desta forma, a tarefa que quebrar a criptografia

[80] Pese embora, em termos comparativos, o número de crimes protegidos pela encriptação seja pequeno com relação aos demais cometidos sem a proteção da encriptação, é sabido que, à medida que a internet e os aparelhos que utilizam FDE se popularizam, este número tenderá a crescer. Oficiais governamentais, especialmente dos Estados Unidos da América, têm apontado que há um medo geral de que a *Full Disk Encryption* retire as capacidades investigativas do Estado.

[81] Contudo, é importante ressaltar que esta discussão surgiu predominantemente nos Estados Unidos da América e na Europa, pelo fato de haver uma maior prevalência da utilização de sistemas operacionais que adotam *full disk encryption* – FDE. O Departamento de Polícia de Los Angeles nos Estados Unidos da América contabilizou 450 telemóveis inacessíveis em investigações em 2016, enquanto o Departamento de Polícia de Nova York contabilizou 423, totalizando 34% dos telemóveis apreendidos que são inacessíveis para fins investigativos. VIDE LEWIS, James A., ZHENG, Denise & CARTER, William A. *The effect of encryption on lawful access to communications and data*. CSIS Technology Policy Program, 2017, pp. 09 e 14.

[82] KERR, Orin S., & SCHNEIER, Bruce, Encryption workarounds. *Georgetown Law Journal,* 2018, pp. 989-1019.

empregada no telemóvel não é uma tarefa simples de ser empregada, especialmente no contexto no qual aparelhos telemóveis empregam métodos criptográficos modernos.

A segunda alternativa, as *backdoors* podem ser traduzidas como criações de "entradas alternativas" concebidas intencionalmente pelo criador da encriptação com o objetivo de deixar uma possibilidade para que investigadores possam aceder às informações por outro método que não seja a de desencriptação. Esta entrada alternativa seria inserida pelo desenvolvedor do sistema, seria, portanto, para todos os aparelhos, sendo este o ponto principal da polémica. O principal motivo pelo qual a criptografia é um sistema fidedigno é em razão da confiança depositada na proteção proporcionada por este sistema, uma vez que exista uma *brecha*, este sistema deixará de ser confiável.

Países como a Turquia já a adotaram a obrigatoriedade de criação de *backdoors* nos sistemas de encriptação utilizados no país, enquanto outros países, como os Países Baixos, são contrários, reforçando a importância de uma encriptação segura sem *backdoors*.[83] Nos Estados Unidos da América[84], ela já foi parte de uma proposta legislativa e também já figurou como uma das alternativas a serem discutidas na luta contra a pornografia de menores pela Comissão Europeia[85] [86].

Na opinião deste estudo, a criptografia já não pode mais ser considerada como uma tecnologia que visa unicamente proteção de dados, pelo contrário, deve ser considerada uma forma de proteção de dados que é essencial na proteção de direitos fundamentais e humanos em uma sociedade tecnológica e dependente do fluxo de informação. A criação de *backdoors* aplicáveis à todos sem distinção é, acima de tudo, uma medida desproporcional que coloca em risco todos os usuários da internet e de

[83] Dutch government says no to 'encryption backdoors', *BBC News*, 7 janeiro 2016, disponível em http://www.bbc.co.uk/news/technology-35251429.
[84] Senate of the United States of America, *A bill to improve the ability of law enforcement agencies to access encrypted data*, and for other purposes. Disponível em https://www.docdroid.net/lHilrMA/oll20597-pdf Acesso em 22 de Abril de 2021.
[85] Comissão Europeia, *Technical Solutions to detect child sexual abuse in end-to-end encrypted communications,* Disponível em < https://www.politico.eu/wp-content/uploads/2020/09/SKM_C45820090717470-1_new.pdf> Acesso em 22 de Abril de 2021.EN E-005255/2020 Answer given by Ms Johansson on behalf of the European Commission, Disponível em https://www.europarl.europa.eu/doceo/document/E-9-2020-005255-ASW_EN.pdf acesso em 07 de junho de 2021.
[86] VEEN, Jeroen, BOEKE, Sergei, No Backdoors: Investigating the Dutch Standpoint on Encryption. *Policy & Internet*, 2020, 12.4, pp. 503-524.

aparelhos telemóveis que em sua maioria não praticam atos ilícitos e utilizam da tecnologia para proteção de dados pessoais.

Quando falamos a respeito da inserção de uma *backdoor* no contexto de uma investigação criminal, o conceito se torna ainda mais problemático, seria como fosse possível autorizar a interceptação telefónica de todos os habitantes de uma cidade, sob o pretexto de investigar apenas um indivíduo. Seria justificável aceitarmos uma medida tão radical, amplo e desproporcional? Na opinião deste estudo, não.

Além disso, na opinião deste estudo, o foco único e exclusivo na criptografia com vista a enfraquecê-la demonstra que Estados e investigadores optaram pelo caminho "mais fácil" que é atacar o elo entre o sujeito e a informação visada. Ao enfraquecer o elo dispensa-se um trabalho investigativo mais profundo, penoso e muitas vezes dispendioso de engenharia social.

Muitos autores sustentam que, quando a tecnologia das escutas telefónicas emergiu, ela tornou-se extremamente popular, sendo muitas vezes tratada como a rainha das provas[87], tornando a devassa na vida privada dos indivíduos um método corriqueiro de investigação. Compreendemos que a desencriptação coativa de telemóveis tem o potencial de tomar o mesmo caminho, com um potencial violador ainda mais grave de direitos fundamentais.

Ao mesmo tempo que temos conhecimento que situações extremas tenderão a acontecer com cada vez mais frequência, tendo em vista o potencial de maior utilização da criptografia nos telemóveis. Contudo, compreendemos que a temática é delicada e perigosa e que deve ser abordada com precaução.

A possibilidade da adoção da desencriptação coativa de telemóveis no ordenamento jurídico português e de outros países será melhor abordada no capítulo seguinte.

[87] *In* JÚDICE, Dr. José Miguel, Escutas telefónicas: a tortura do Século XXI?, *Revista da Ordem dos Advogados*, Ano 64, Vol. I/II, Nov. 2004 disponível em shorturl.at/bdxLP acesso em 06 de setembro 2021.

CAPÍTULO II - A DESENCRIPTAÇÃO COATIVA

1. A desencriptação coativa de telemóveis nos demais ordenamentos jurídicos

Uma das soluções apresentadas para o conflito entre a criptografia e a necessidade de acesso aos dados informáticos armazenados nos telemóveis é a desencriptação coativa, que aparenta ser uma alternativa plausível com relação aos *backdoors,* tendo em vista que é concentrada em um indivíduo em questão que terá no telemóvel os dados informáticos buscados.

A desencriptação coativa de telemóveis nada mais seria que o ato de coagir o arguido a ceder acesso ao telemóvel protegido por um sistema criptográfico, para que os dados informáticos sejam acessíveis.

É importante ressaltar que a forma da decriptação coativa dependerá do ordenamento jurídico em que ela estará inserida: no ordenamento jurídico português não há, até o momento, dispositivo expresso que trate a respeito dela. Contudo, em alguns ordenamentos jurídicos ela já existe e está em prática.

Segundo o terceiro informativo sobre a criptografia realizado pela Europol em conjunto com a Eurojust[88], até julho 2018, 19 Estados-Membros e a Suíça tinham editado alguma legislação relativa à criptografia, contudo na maioria destes países o dispositivo legal era geral. Desde então, apenas os Países Baixos e a Suécia realizaram modificações legais acerca do tema.

A França tem uma legislação extensa e detalhada a respeito da criptografia. Segundo o informativo conjunto, o artigo 434-15-2 do Código

[88] *Third Report of the Observatory Function on Encryption, Joint Report Europol & Eurojus Information*, June 2021. Disponível em: https://www.europol.europa.eu/publications-documents/third-report-of-observatory-function-encryption acesso em 06 de setembro 2021

Penal[89] permite que ferramentas técnicas sejam utilizadas para quebrar proteções criptográficas e utilizar os dados informáticos apreendidos como prova. Os mesmos artigos determinam uma pena de três anos de prisão e multa para quem detenha chave de desencriptação de uma mensagem que tenha sido utilizada para preparar, facilitar ou cometer um crime e se recuse a cumprir ordem judicial e cedê-la para fins investigativos[90].

A Bélgica, por sua vez, determina no artigo 88, 4.º do Código de Processo Penal belga[91] o dever de cooperação dos indivíduos que tenham especial conhecimento do sistema informático e que podem ceder acesso a eles[92]. A Irlanda explicita na sessão 48, n.º 5, b), do Código Penal que as autoridades investigativas podem, com base em um mandado judicial, determinar que qualquer pessoa que possa ter acesso aos dados armazenados nos aparelhos telemóveis seja compelida a ceder a palavra-chave, permitindo assim acesso pela autoridade competente[93].

Os Países Baixos realizaram profundas modificações no tema da criptografia, em março de 2019 o chamado "Computer Crime Act III" entrou em vigor com o objetivo de aperfeiçoar os poderes investigativos de cibercrimes[94], incluindo novos métodos ocultos de investigação na secção 126nba DCCP. Contudo, o Supremo Tribunal dos Países Baixos decidiu, no acórdão n.º 19/05471 CW de 09 de fevereiro de 2021[95], que o arguido deverá colaborar nas medidas investigativas, autorizando, caso haja recusa, a utilização de algemas para facilitar o uso das impressões digitais

---

89 *"A penalty of three years' imprisonment and a fine of €45,000 are incurred by anyone who, having the key to decipher an encrypted message which may have been used to prepare, facilitate or commit a felony or a misdemeanour, refuses to disclose that key to the judicial authorities or to operate it following instructions issued by the judicial authorities under of title II and III of Book I of the Code of Criminal Procedure".* Disponível em https://www.legal-tools.org/doc/418004/pdf/ acesso em 15 de Abril de 2021.

90 O referido artigo teve a sua constitucionalidade questionada, contudo a Corte Constitucional francesa, ao aplicar um entendimento restrito do direito à não autoincriminação como mero direito ao silêncio, entendeu que não há violação do direito à não autoincriminação, tendo em vista que o referido artigo não exige confissão do arguido e sim apenas exige uma entrega de uma chave. *In* Eurojust, Cybercrime Judicial Monitor.

91 Code D'Instruction Criminelle, 17 Novembre 1808, shorturl.at/rHLRV.

92 Pese embora o Código de Processo Penal Belga mencione que tal determinação não poderá recair sobre o arguido, em fevereiro de 2020 a Corte de apelações Belga decidiu que tal artigo pode ser aplicado a arguidos com a justificativa que o direito à não autoincriminação não é um direito absoluto, que deverá ser ponderado com os demais direitos afetados. Ao mesmo tempo, a Corte aplicou o mesmo entendimento dado ao ADN pela Tribunal Europeu de Direitos do Homem, ao entender que a palavra-chave existe independentemente da vontade do arguido. *In* KU Kleven CiTiP. Disponível em https://www.law.kuleuven.be/citip/blog/you-have-the-right-to-remain-silent-until-we-want-your-smartphone-password/ Acesso em 18 de maio de 2021.

93 Section 48 Criminal Justice Theft and Fraud Offences Act 2001; Section 7 Criminal Justice Offences Relating to Information Systems Act 2017.

94 Third Report of the Observatory Function on Encryption, Joint Report Europol & Eurojus Information, June 2021. Disponível em: https://www.europol.europa.eu/publications-documents/third-report-of-observatory-function-encryption

95 HR, 09-02-2021, n.º 19/05471 Disponível em shorturl.at/nsMVW acesso em 06 de setembro 2021.

no ato de desencriptação do aparelho telemóvel. A Suprema Corte decidiu que não há violação do direito à não autoincriminação do arguido na hipótese de este ser colocado em algemas e coagido a utilizar a sua impressão digital para desbloquear o *smartphone* no âmbito de investigações criminais, tendo em vista que a impressão digital bem como o reconhecimento facial existem independentemente da vontade do arguido, diferentemente das palavras-passe e códigos de acesso, sendo possível, portanto, exigir a colaboração do arguido nas medidas investigativas.

Vai no mesmo sentido a decisão exarada pelo Tribunal Internacional de Justiça no caso 09/818727-17 da data de 12 de Março de 2018, que determinou que não há tortura ou violação do direito à um julgamento justo ou direito à privacidade. O Tribunal compreendeu que o acusado não cooperou com a investigação na localização de duas crianças desaparecidas, portanto justificando as medidas coativas aplicadas[96].

O informativo também ressalta que, em razão da ausência de legislação específica que trate a respeito da criptografia, há uma insegurança jurídica acerca da admissibilidade das provas recolhidas. Além disso, apontamos que como é possível observar, a utilização da desencriptação coativa é apenas um entendimento jurisprudencial e não legal, o que nos aponta para o caminho que a maioria dos países está a tomar, que ao nosso ver não é um caminho desejável.

1.1 A desencriptação coativa de telemóveis em Portugal

Em Portugal, no entendimento de CONDE CORREIA[97], há uma omissão legislativa que não deixou qualquer norma habilitante a respeito da possibilidade ou não de notificar os possuidores de aparelhos

[96] EuroJust Cybercrime Judicial Monitor, Issue 4f
[97] *Ibidem* CORREIA, p. 29–59.

eletrónicos a fim que estes permitam o acesso ao conteúdo armazenado. Esta omissão legislativa abre espaço a interpretações tanto no sentido de não ser possível esta coação, opinião com a qual simpatizamos com melhor análise posterior, como no sentido de encontrar brechas legislativas que permitam tal ato.

Ao observarmos os exemplos da aplicação da desencriptação em outros ordenamentos jurídicos é possível realizarmos um paralelo com a realidade portuguesa e apresentar uma base jurídica para a sua ocorrência, vejamos assim a ordem dos acontecimentos

Primeiramente, haverá uma *notitia criminis*[98] acerca de um cibercrime ou um crime comum e assim dará início a uma investigação acerca do facto. Em seguida, caso um indivíduo seja considerado suspeito do cometimento de tal ilícito, irá assumir a qualidade de investigado ou arguido nos termos do artigo 57.º do CPP[99]. A partir deste ponto as diligências necessárias à investigação serão realizadas e a autoridade policial poderá sentir necessidade de realizar a análise e investigação dos dados informáticos armazenados no telemóvel do arguido.

Irá iniciar-se então a investigação do ocorrido através da atividade probatória que é dividida em dois pontos: os meios de obtenção de prova e os meios de prova. Os meios de prova são, segundo PAULO DE SOUSA MENDES[100], o esforço metódico através da qual serão demonstrados os factos relevantes para a existência do crime, a punibilidade do arguido e a determinação da pena ou da medida de segurança aplicável. Já os meios de obtenção de prova são, segundo GERMANO MARQUES DA SILVA[101], os instrumentos de que servem as autoridades judiciárias para investigar e recolher os meios de prova.

Ao longo da investigação, a pessoa que adquirir a qualidade de arguido terá direitos[102] e deveres, que estão dispostos no artigo 61.º, n.º 5,

---

[98] A *notitia criminis* é o conhecimento da ocorrência de uma infração penal que dá início às investigações com a instauração do inquérito policial conforme disposto no artigo 262.º, n.º 2 do Código de Processo Penal.

[99] "A definição de arguido tem interesse para a determinação do momento em que a instrução de deve considerar iniciada. Cf., DOS SANTOS, Gil Moreira, *Princípios e Prática Processual Penal*, Coimbra, Coimbra Editora, 2014, p. 140.

[100] MENDES, Paulo de Sousa, em *Jornadas de Direito Processual Penal e Direitos Fundamentais*, Almedina, 2004, p. 132.

[101] *In* MARQUES DA SILVA, Germano, *Curso de Processo Penal*, III Volume, Editorial Verbo, 2000, p. 68.

[102] Cf., artigo 61.º, n.º 1 - O arguido goza, em especial, em qualquer fase do processo e salvas as exceções da lei, dos direitos de: a) Estar presente aos atos processuais que diretamente lhe disserem respeito; b) Ser ouvido pelo tribunal ou pelo juiz de

nas alíneas a) a d) do Código de Processo Penal, sendo eles nomeadamente: o dever de comparecer perante o juiz, Ministério Público ou órgãos de polícia criminal quando a lei o exigir e quando tenha sido convocado; o dever de responder com verdade às perguntas a respeito da sua identidade; e, por fim, o dever de sujeitar-se a diligências de prova e a medidas de coação e garantia patrimonial especificadas em lei e ordenadas por autoridade competente[103].

Este dispositivo aponta uma *colaboração* do arguido[104] na busca pela verdade material, garantindo a participação deste na realização dos atos mencionados. Este é o entendimento de MANUEL DA COSTA ANDRADE, em seus estudos a respeito das proibições de prova, que afirma que o arguido está submetido pelo dever geral de cooperação a exames e perícias, através de ordem judicial fundamentada[105] e caso necessário o eventual uso da força[106].

Inclusive, a discussão acerca do direito ao silêncio do arguido quando este está em conflito com o dever de cooperação no âmbito do artigo 61.º, n.º 6, do CPP é pertinente, e será realizada em momento posterior no Capítulo III que tratará acerca das consequências da desencriptação coativa de telemóveis.

Desta forma, se ao longo da investigação for considerado indispensável aceder aos dados informáticos armazenados no aparelho

---

instrução sempre que eles devam tomar qualquer decisão que pessoalmente o afete; c) Ser informado dos factos que lhe são imputados antes de prestar declarações perante qualquer entidade; d) Não responder a perguntas feitas, por qualquer entidade, sobre os factos que lhe forem imputados e sobre o conteúdo das declarações que acerca deles prestar; e) Constituir advogado ou solicitar a nomeação de um defensor; f) Ser assistido por defensor em todos os atos processuais em que participar e, quando detido, comunicar, mesmo em privado, com ele; g) Intervir no inquérito e na instrução, oferecendo provas e requerendo as diligências que se lhe afigurarem necessárias; h) Ser informado, pela autoridade judiciária ou pelo órgão de polícia criminal perante os quais seja obrigado a comparecer, dos direitos que lhe assistem; i) Ser acompanhado, caso seja menor, durante as diligências processuais a que compareça, pelos titulares das responsabilidades parentais, pelo representante legal ou por pessoa que tiver a sua guarda de facto ou, na impossibilidade de contactar estas pessoas, ou quando circunstâncias especiais fundadas no seu interesse ou as necessidades do processo o imponham, e apenas enquanto essas circunstâncias persistirem, por outra pessoa idónea por si indicada e aceite pela autoridade judiciária competente; j) Recorrer, nos termos da lei, das decisões que lhe forem desfavoráveis.

[103] Paulo Pinto Albuquerque aponta que o arguido tem a obrigação de participar da acareação, mas não tem a obrigação de depor sobre os factos. O mesmo o autor aponta a respeito das fotografias, ao afirmar que o arguido está sujeito, por força do seu estatuto, à recolha de provas dactiloscópicas e fotográficas e de outra natureza independentemente do seu consentimento. *In* ALBUQUERQUE, Paulo Sérgio Pinto de, *Comentário do Código de Processo Penal: à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem*, 4ª ed. Lisboa, Universidade Católica Editora, 2011, p. 420 e 427.

[104] Pese embora alguns autores apontem como uma "cláusula geral do dever de sujeição do arguido" *In* PINTO, Lara Sofia, 2010, p. 100.

[105] Vide nº 1 do art. 8º ,da Lei 05/2008 de 12 de fevereiro que aduz: "1 - A recolha de amostra em arguido em processo criminal pendente, com vista à interconexão a que se refere o n.º 2 do artigo 19.º-A, é realizada a pedido ou com consentimento do arguido ou ordenada, oficiosamente ou a requerimento escrito, por despacho do juiz, que pondera a necessidade da sua realização, tendo em conta o direito à integridade pessoal e à reserva da intimidade do visado" (grifo nosso).

[106] COSTA ANDRADE, *Sobre as Proibições de Prova em Processo Penal*, Coimbra, Coimbra Editora, 2006. p. 121.

telemóvel do arguido, a autoridade judiciária competente, seja o juiz de instrução criminal seja o Ministério Público[107], irá determinar a pesquisa de dados informáticos[108].

A pesquisa de dados informáticos, prevista no artigo 19.º da Convenção do Cibercrime e no artigo 15.º da Lei do Cibercrime, foi elaborada para ser uma forma digital do sistema de busca e apreensões, ressalvando as diferenças fundamentais entre os dados informáticos e as demais provas[109].

Como é possível observar, o artigo 15.º da Lei do Cibercrime é sucinto, e por isso aplicar-se-á subsidiariamente o regime das buscas e apreensões dispostos nos artigos 174.º e 177.º do CPP[110].

De acordo com FRANCISCO MARCOLINO DE JESUS, as buscas são meios de obtenção de prova levadas a cabo em um lugar reservado ou não livremente acessível ao público, quando houver indícios de que nesses locais se encontram quaisquer objetos relacionados com um crime ou que possam servir de prova no processo em curso[111].

Contudo, é preciso ressaltar as diferenças essenciais entre as buscas tradicionais e a pesquisa de dados informáticos. Como SUSAN BRENNER E BARBARA FREDERIKSEN[112] bem apontam, as buscas tradicionais

---

[107] Na doutrina, há uma discussão a respeito de qual seria a autoridade judicial competente para determinar a pesquisa de dados informáticos, tendo em vista que poderão ser encontrados dados informáticos sensíveis, que coloquem em causa o direito à privacidade do arguido. Neste contexto, a opinião maioritária da doutrina é que o magistrado do Ministério Público detém a competência para determinar a pesquisa, ao passo que a opinião minoritária defende que deveria ser o juiz de instrução a determinar a pesquisa, justamente por se tratar de um conteúdo potencialmente violador de direitos fundamentais[107].

[108] Cumpre ressaltar de forma complementar que, em razão do novo regime da Lei do Cibercrime, o artigo 189.º do CPP é aplicável a interceptação das comunicações entre presentes e outros meios à distância que não constituam comunicações eletrónicas ou transmissões de dados informáticos. *In Ibidem* MESQUITA, Paulo Dá, *Processo Penal, Prova e Sistema Judiciário*, Coimbra, Coimbra Editora, 2010, p. 103.

[109] Vide Ponto 184 do Relatório Explicativo da Convenção do Cibercrime "O presente artigo visa a modernização e a harmonização das legislações nacionais relativamente à busca e apreensão de dados informatizados armazenados, para fins de obtenção de provas relacionadas com investigações criminais ou ações penais específicas. Qualquer legislação interna em matéria de direito processual penal, contempla os poderes relativos à busca e apreensão de objetos tangíveis. Contudo, em muitos Estados ou jurisdições, os dados informatizados armazenados, por si só, não serão considerados como algo tangível pelo que não poderão ser adquiridos a título de investigações criminais e ações penais da mesma forma que os bens corpóreos, a não ser através da obtenção do suporte no qual se encontram armazenados os dados. O objetivo do Artigo 19.º da presente Convenção é o de estabelecer um poder equivalente relativo aos dados armazenados". Disponível em shorturl.at/vwGHW acesso em 6 de setembro de 2021

[110] Como ressaltou Benjamim Silva Rodrigues, as buscas e apreensões informáticas pouco tem a ver com as tradicionais do meio físico, o que por si só já pode levantar questionamentos à necessidade de aplicação das normas gerais à pesquisa e recolha de dados informáticos presente na Lei do Cibercrime. Rodrigues ressalta que no âmbito informático as buscas têm duas fases distintas, a primeira consiste em descobrir e identificar o repositório eletrónico no qual se situa a prova digital e em seguida deverá se identificar a informação digital ali contida. *In* RODRIGUES, 2008, p. 534.

[111] MARCOLINO DE JESUS, Francisco, *Os Meios de Obtenção da Prova em Processo Penal*, 2ª edição, Coimbra, Editora Almedina, 2019, p. 226.

[112] *"In conventional searches and seizures, the execution of a warrant typically involves two stages: a 'search' for evidence that is followed by the 'seizure' of evidence once it has been found… In off-site computer searches, the execution of a warrant involves four stages, not two: a search designed to locate computer equipment; the seizure of that equipment and its removal to another location; a thorough search of*

consistem em um passo que é a recolha do objeto da busca, contudo as buscas relacionadas com computadores – no ordenamento português chamadas de pesquisa de dados informáticos – são essencialmente diferentes tendo em vista que será necessário realizar a busca do aparelho eletrónico e depois realizar a pesquisa de dados informáticos em um ambiente específico para tal[113].

Ressaltamos que alguns pontos da pesquisa de dados informáticos poderão ser de facto similares às buscas tradicionais, sempre, entretanto, deverão ser respeitadas as particularidades da pesquisa de dados informáticos. Contudo, a ausência de uma maior profundidade do legislador, ao nosso ver, deixa uma lacuna prejudicial na matéria.

Desta forma, diante da ausência de disposições legais específicas voltadas à pesquisa de dados informáticos, ela terá de ser levada a cabo pela autoridade judiciária competente, por ordem ou autorização desta mediante decisão judicial na qual é demonstrada a necessidade da medida para o processo. Como é possível observar em análise do artigo 15.º, não há prazo especificado para realização da pesquisa, por isso, compreende-se que deverá ser realizada no prazo máximo de 30 dias, presidida pela autoridade judiciária sempre que possível.

Aqui também é necessário levantar a questão de saber se o prazo de 30 dias é compatível com o procedimento da pesquisa de dados informáticos. Como será possível melhor observar adiante neste estudo, a pesquisa de dados informáticos envolve tarefas altamente especializadas de recolha de dados informáticos. Este processo poderá fácil ou dispendioso, necessitando contudo, de pessoal e aparelho especializado. Portanto, também levantamos o questionamento a respeito da possível incompatibilidade do prazo das tradicionais buscas e apreensões.

Isto posto, uma vez realizada a pesquisa de dados informáticos deverá ser elaborado um relatório, tendo em vista o cumprimento do artigo

the contents of the equipment which is conducted at a location; and a seizure of relevant evidence located in the course of that search" BRENNER, Susan W., FREDERIKSEN, Barbara A., Computer Searches and Seizures: Some Unresolved Issues, 8 Mich. Telecomm. & Tech. Law Review, n.º 39, 82, 2002.

[113] Os detalhes técnicos da recolha dos dados informáticos será melhor abordada na secção a respeito dos dados informáticos como prova digital.

253.º do Código de Processo Penal, que será dirigido à autoridade judicial competente.

Como iremos ressaltar na subsecção seguinte, a respeito do uso dos dados informáticos como prova digital, as provas digitais têm características específicas que impõem que a sua recolha e análise deverão ser feitas por quem tenha conhecimentos técnicos específicos para tanto. Por isso, afirma JOÃO CONDE CORREIA[114], que em determinadas circunstâncias poderá ser necessário proceder a uma perícia informática nos dados informáticos alvo da pesquisa.

Com relação a este tema, ALBERTO GIL LIMA CANCELA aponta que há uma articulação entre o artigo 15.º da Lei do Cibercrime com os artigos 151.º e seguintes bem como com o artigo 171.º do Código de Processo Penal pese embora não esteja disposto explicitamente, tendo em vista as disposições da Lei do Cibercrime não invalidam as disposições gerais do Código de Processo Penal[115]. PEDRO VERDELHO concorda com esta afirmação ao apontar que a pesquisa de dados informáticos não é um substituto para os exames periciais[116].

Uma vez iniciada a pesquisa de dados informáticos, surgem duas possibilidades: a primeira é a pesquisa ocorrer de forma bem-sucedida e realizar-se a apreensão de dados informáticos conforme disposto no artigo 16.º da Lei do Cibercrime, já a segunda possibilidade é o caso de a pesquisa ser obstada pela criptografia do aparelho, objeto deste estudo[117].

Neste caso, defendemos primeiramente que a autoridade judicial competente deverá consultar o arguido acerca da possibilidade de o mesmo consentir para a pesquisa de dados informáticos[118]. Compreendemos que uma medida drástica como a desencriptação coativa

---

[114] CORREIA, João Conde, Prova digital: as leis que temos e a lei que devíamos ter. *Revista do Ministério Público n.º 139*, 2014, pp. 29–59.

[115] CANCELA, Alberto Gil Lima, *A prova Digital: Os meios de obtenção de prova na Lei do Cibercrime* em dissertação apresentada à Faculdade de Direito da Universidade de Coimbra no âmbito do 2.º Ciclo de Estudos em Direito, na área de especialização em ciências jurídico-forenses sob orientação da Professora Doutora Sónia Mariza Florêncio Fidalgo em 2016. Disponível em https://estudogeral.sib.uc.pt/bitstream/10316/31398/1/A%20prova%20digital.pdf acesso em 10 de setembro de 2021.

[116] *Ibidem* VERDELHO, 2009, p. 740.

[117] Ressaltamos aqui a importância de que não haja possibilidade de aceder aos dados informáticos de nenhuma outra forma apenas através do telemóvel.

[118] Em respeito ao princípio do contraditório presente no n.º 5, do artigo 32.º da Constituição da República bem como ao disposto no artigo 174.º, n.º 5 alínea b) do Código de Processo Penal.

deve ser feita respeito o contraditório prévio, dando ao arguido a chance de manifestar-se previamente.

Caso o arguido recuse ceder acesso ao telemóvel alvo da pesquisa, surge a questão da revelação coativa da *password* do telemóvel, ou como optamos por chamar de desencriptação coativa de telemóveis[119].

1.2 O procedimento da desencriptação coativa

Ao observarmos a Lei do Cibercrime, em especial no artigo referente à pesquisa de dados informáticos, não há disposição alguma sobre como proceder no caso de o arguido recusar-se a colaborar e autorizar a pesquisa. Como bem aponta CONDE CORREIA, há uma verdadeira omissão legislativa acerca do tema[120].

Primeiramente, a doutrina se divide na consequência jurídica da recusa. DUARTE ALBERTO RODRIGUES NUNES[121] aponta que não há possibilidade de aplicar ao arguido ou suspeito o crime de desobediência, tendo em vista que o legislador português não previu qualquer dever de cooperação na Lei do Cibercrime, o que, por consequência, configuraria uma lesão do *nemo tenetur se ipsum accusare.* Já, no entendimento de ANA PAULA GUIMARÃES[122], com relação à recolha coativa de sangue para fins de análise de ADN, há a possibilidade de imputar ao arguido o crime de desobediência, previsto no artigo 348.º, n.º 1, alínea b), do Código Penal, punível com pena de prisão de até um ano ou pena de multa até 120 dias, além disso, caso haja fundada razão para crer que o arguido não se apresentará voluntariamente, o mesmo poderá ser detido para comparência nos termos dos artigos 254.º, n.º 1, alínea b), e 257.º, n.º 1, alínea a), do Código de Processo Penal.

---

119 Optamos por esta nomenclatura em detrimento da "revelação coativa da password", porque os telemóveis não são protegidos apenas por palavras-passe, pelo contrário, cada vez mais surgem novos métodos criptográficos, muitos com o uso de dados biométricos como camada extra de segurança.
120 *Idem* CONDE CORREIA, 2014, p.29-59.
121 *Ibidem* RODRIGUES NUNES, 2018, p. 90.
122 GUIMARÃES, Ana Paula, *A Pessoa como objecto de prova em Processo Penal: Exames, Perícias e Perfis de ADN – Reflexões à luz da dignidade humana*, Editora Nova Causa, 2016, p. 118.

Em seguida, independentemente de se imputar ou não ao arguido o crime de desobediência, será a partir da negativa do arguido que se dará início a desencriptação coativa.

Neste ponto, optamos por realizar um paralelo com a decisão do Tribunal Constitucional exarada no acórdão 155/2007[123]. Nesta ocasião, o entendimento firmado pelo Tribunal foi que o arguido poderá ser coagido a realizar a recolha de material biológico sob justificativa do artigo 61.º, n.º 3, alínea d), do Código de Processo Penal, desde que se respeite a adequação ao fim visado, exigibilidade e proporcionalidade sem violar os direitos fundamentais do arguido ao mesmo tempo que visa a verdade material[124]. Ao longo do acórdão, os autores COSTA ANDRADE e GOMES CANOTILHO são citados para firmar o entendimento que os avanços tecnológicos não podem ser ignorados na busca pela verdade material no processo penal, e que a sujeição coativa à colheita de saliva está formalmente suportada pelo dever de cooperação do arguido previamente mencionado.

Assim, da mesma forma que o Tribunal Constitucional compreendeu ser possível coagir o arguido a sujeitar-se a meio de obtenção de prova, baseado no dever de cooperação do arguido na busca pela verdade material, compreendemos ser possível realizarmos a mesma interpretação com relação à desencriptação coativa de telemóveis.

Este entendimento baseia-se também no caso *Sauders v. Reino Unido*, julgado em 1996 pelo Tribunal Europeu dos Direitos do Homem - TEDH. Nele, o TEDH compreendeu que o direito à não autoincriminação se refere ao respeito pela vontade do arguido em não emitir declarações, na sua vertente, portanto, do direito ao silêncio clássico. Entretanto, não inclui no âmbito da não autoincriminação os dados obtidos por meio coercitivos que

[123] Nesta decisão, o Tribunal Constitucional julgou inconstitucional o artigo 172.º, n.º 1 do Código de Processo Penal quando interpretada no sentido de dispensar a autorização do juiz no ato de colheita coativa de vestígios biológicos de um arguido para a determinação do seu perfil genético quando este tenha manifestado a recusa em colaborar ou permitir a colheita. Julgamento disponível em: https://dre.pt/home/-/dre/2068880/details/maximized>

[124] Compreendemos que para que um sistema jurídico seja exequível, os direitos fundamentais não podem e não devem ser ilimitados. Neste contexto, haverá sempre a necessidade de *ponderação* dos mesmos em situações de aparente conflito. Contudo, na opinião deste estudo, o caso abordado no acórdão 155/2007 do Tribunal Constitucional não se encaixa nesta hipótese, pelo contrário, se trata de uma decisão que considera constitucional, sob autorização judicial, uma ação coativa que fere de morte a dignidade da pessoa humana ao submeter o arguido à realização de ações que ferem a sua dignidade e integridade física e moral sob a justificativa da busca pela verdade material.

não dependam da declaração do arguido, como por exemplo, colheita de sangue.

Desta forma, o arguido ao recusar cooperar com a investigação, dando acesso ao telemóvel, poderá ser compelido a fazê-lo com base nos deveres do arguido na busca pela verdade material, desde que este ato coercitivo respeite a adequação ao fim visado, exigibilidade e proporcionalidade[125].

Por isso, uma vez determinada a pesquisa de dados informáticos, sendo esta obstaculizada pela criptografia do aparelho e registada a recusa do arguido em dar acesso ao telemóvel, é necessário assim, um segundo despacho a ordenar a desencriptação coativa que deverá cumprir alguns requisitos.

Primeiramente, a autoridade judicial competente, ao solicitar o despacho coator, deverá comprovar que o arguido se recusou a cooperar cedendo acesso ao aparelho telemóvel. ORIN KERR E BRUCE SCHNEIER[126] ressaltam que esta comprovação poderá ser dificultosa tendo em vista que o arguido poderá argumentar que esqueceu a palavra passe ou que nunca a soube.

Uma vez recebido o pedido, o despacho deverá levar em consideração o princípio da proibição de excesso, concretizado pela necessidade e proporcionalidade da medida conforme disposto no artigo 18.º, n.º 2, da Constituição[127], que determina que qualquer restrição a direitos fundamentais deverá cingir-se ao mínimo necessário, o que significa que a medida de desencriptação coativa deverá ser apontada como o único meio disponível para aceder aos dados informáticos considerados essenciais na busca pela verdade. Além disso, o despacho deverá determinar que a coação deverá ser feita do modo menos penoso para os direitos do arguido.

---

[125] A proporcionalidade está consagrada como princípio da necessidade ou adequação no n.º 2 do artigo 18.º da Constituição, sendo um limite material constitucional de toda a intervenção político-criminal que afete direitos fundamentais. *In* GUIMARÃES, 2016, p. 69.

[126] *Idem* Kerr & Schneier, 2017, pp. 989.

[127] Artigo 18.º, n.º 2 da CRP que dispõe: "A lei só pode restringir os direitos, liberdades e garantias nos casos expressamente previstos na Constituição, devendo as restrições limitar-se ao necessário para salvaguardar outros direitos ou interesses constitucionalmente protegidos".

A partir deste ponto temos algumas observações relevantes acerca dos procedimentos que devem ser adotados. Primeiramente, defendemos que em razão da desencriptação coativa de telemóveis ser uma medida de extrema gravidade, esta deverá ser determinada pelo juiz de instrução, traçando um paralelo com a recolha coativa de ADN, a qual deverá ser determinada pelo juiz de instrução e não pelo magistrado do Ministério Público, como apontado no Acórdão n.º 155/2007 do Tribunal Constitucional[128].

A necessidade de respeito à proporcionalidade da medida também nos leva à discussão a respeito da possibilidade de restrição da medida ao mínimo de casos possível. Uma opção seria a criação de um catálogo de crimes[129] a que esta medida seria aplicável, como o adotado na intervenção nas comunicações escritas, postais e telegráficas que são aplicáveis apenas aos crimes graves como disposto no artigo 179.º, n.1º, alínea b), do CPP.

Porém, não há catálogo de crimes estipulado pela Lei do Cibercrime com relação à pesquisa de dados informáticos, o que nos leva a entender que este meio de obtenção de prova pode ser aplicado a um universo de crimes aberto[130]. PAULO DÁ MESQUITA aponta que as regras de direito probatório criadas pela Lei do Cibercrime não versam apenas sobre cibercrimes mas correspondem a um regime amplo de prova eletrónica em processo penal, aplicável portanto a qualquer crime[131].

Contudo, é possível observar o catálogo de crimes presente no artigo 15.º, n.º 3, alínea b), que aponta a hipótese da autoridade policial poderá realizar a pesquisa de dados informáticos "nos casos de terrorismo, criminalidade violenta ou altamente organizada, quando haja fundados indícios da prática iminente de crime que ponha em grave risco a vida ou a integridade de qualquer pessoa". Em razão de ser uma situação extrema,

---

128 *"Por outras palavras e no concreto caso, o n.º 4 do artigo 32.º da CRP prossegue a tutela de defesa dos direitos do cidadão no processo criminal e, nessa exata medida, determina o monopólio pelo juiz da instrução, juiz-garante dos direitos fundamentais dos cidadãos ("reserva do juiz")."* *In* Acórdão do Tribunal Constitucional n.º 155/2007 disponível em https://www.tribunalconstitucional.pt/tc/acordaos/20070155.html

129 É em razão ao princípio da proporcionalidade que levou o legislador a consagrar os chamados "crimes de catálogo". *In* DOS SANTOS, Gil Moreira, Princípios e Prática Processual Penal, Coimbra, Coimbra Editora, 2014, p. 249.

130 *Ibidem* RODRIGUES NUNES, 2018, p. 96.

131 *Ibidem* MESQUITA, 2010, p. 98.

o catálogo de crimes apontado é uma alternativa possível de ser utilizada na desencriptação coativa de telemóveis.

Apesar da hipótese de o catálogo de crimes ser da nossa preferência, em razão da gravidade da medida, entendemos que ela não é atrativa de modo geral. Conforme referimos no primeiro capítulo deste estudo, a utilização dos telemóveis para a prática de ilícitos não é restrita apenas aos cibercrimes, e a sua tendência será ampliar-se cada vez mais. Deste modo, a criação de um catálogo seria demasiadamente dificultosa, pois deveria incluir crimes comuns.

Alternativamente, propomos a adoção de uma análise, caso a caso, da necessidade da aplicação da medida, levando em consideração a importância dos dados eventualmente coletados para o processo em questão, nos moldes do disposto no artigo 15.º da Lei do Cibercrime que aduz*:* "Quando no decurso do processo se tornar necessário à produção de prova, tendo em vista a descoberta da verdade, obter dados informáticos específicos e determinados (...)".

O despacho também deverá individualizar os indícios e o crime, quais dados informáticos estão a ser buscados[132], a individualização[133] do aparelho telemóvel alvo da desencriptação coativa para fins de respeito ao princípio da especialidade. Desta forma, não é possível e nem aceitável que uma pesquisa de dados informáticos e também uma desencriptação coativa seja decretada a nível de investigações preliminares, prospectivas ou seletivas. Como bem ressalta RODRÍGUEZ LAINZ, ao apontar que o princípio da especialidade marca as pautas de atuação agressiva ao direito do segredo das comunicações[134].

Ultrapassada a fase do despacho judicial, se iniciará a fase da desencriptação coativa em si, que dependerá do método de criptografia

---

[132] "This term refers to inspections conducted without factual or legal basis – they are driven merely by an unsubstantiated suspicion of a potential infringement. Fishing expeditions are prohibited since they constitute an abuse of public powers by a competition authority" *In* MICHALEK, Marta, Fishing Expeditions and Subsequent Electronic Searches in the Light of the Principle of Proportionality of Inspections in Competition Law Cases in Europe, *Yearbook of Antitrust and Regulatory Studies*, Vol. 2014, 7 (10), pp. 129-157. Disponível em shorturl.at/htyP4

[133] A individualização do aparelho poderá ser feita através da especificação do número IMEI. O IMEI é um número de 15 dígitos que identifica cada um dos dispositivos existentes. O número além de vir na embalagem do aparelho, também pode ser encontrado na entrada do SIM. *In Associação Portuguesa de Apoio à Vítima – APAV, Folha Informativa: Segurança de telemóveis*, disponível em: https://apav.pt/apav_v3/images/folhas_informativas/fi_seguranca_dispositivos_moveis.pdf

[134] RODRÍGUEZ LAINZ, José Luiz, *La intervención judicial de las comunicaciones del concursado*, Editorial Bosch, S.A, 2004, p. 217

adotado pelo aparelho telemóvel alvo da pesquisa. Conforme apresentamos no primeiro capítulo, a criptografia é uma tecnologia que tem se desenvolvido rapidamente nos últimos anos, especialmente depois que foi aplicada aos telemóveis. Atualmente, muitos aparelhos conjugam um ou mais métodos de encriptação distintos, um que consiste em uma palavra-passe e o outro uma encriptação que usa dados biométricos, que podem ser reconhecimento facial ou leitura de digital.

No caso dos dados biométricos, o ato de desencriptação é mais simples e consistirá no ato de aplicar a digital do arguido no telemóvel ou utilizar o reconhecimento facial. Neste caso, como bem sustenta ANA PAULA GUIMARÃES a recolha de um dado biométrico[135] não pressupõe uma manifestação de vontade do visado e a sua recusa não afasta a realização coativa, como também sustenta ORIN KERR E BRUCE SCHNEIER[136] *"Because biometric access ordinarily does not require testimony, the government can force a phone's owner to press their fingers onto a fingerprint reader (...)".*

Defendemos, contudo, caso este entendimento seja adotado, que o método menos invasivo possível seja empregado, de modo que a integridade física e moral do arguido seja respeitada[137].

Contudo, com relação da palavra-passe a situação altera-se. A palavra-passe por poder ser formada de números é considerado um "veículo verbal e o veículo da escrita pressupõem sempre um ato livre de vontade do próprio arguido" [138], ou seja, uma declaração que terá de ser feita pelo arguido. Desta forma compreendemos que não seja possível nem legalmente aceitável coagir o arguido a realizar qualquer tipo de declaração sob pena de violação do direito à não autoincriminação na sua vertente do direito ao silêncio. ORIN KERR E BRUCE SCHNEIER[139] vão no mesmo

[135] Dados biométricos são características individuais únicas que podem ser utilizadas para fins de identificação e/ou autenticação. Os dados biométricos são elementos essenciais da ciência forense e um elemento precioso em controlo de acessos. Definição em Parecer 3/2012 sobre a evolução das tecnologias biométricas. Emitido pelo Grupo de Proteção de Dados do Artigo 29.º, Adotado em 27 de abril de 2012. Disponível em https://www.gpdp.gov.mo/uploadfile/others/wp193_pt.pdf acesso em 04 de setembro de 2021.
[136] *Idem* KERR & SCHNEIER, 2017, pp. 989.
[137] Inspirado nos termos do art. 10.º da Lei 5/2008 de 12 de fevereiro que trata acerca da Base de dados perfis de ADN.
[138] *Ibidem* GUIMARÃES, 2016, p. 118-123.
[139] *Idem* KERR & SCHNEIER, 2017, pp. 989.

sentido ao apontarem que *"(...) The government can force a target to use a biometric indicator, physically placing his finger on the reader. But the government has no way to actually force a suspect to disclose a key or decrypt a device (...)".*

Por isso, concluímos que na hipótese de a desencriptação coativa de telemóveis ser compreendida possível, não seria aplicável no caso da utilização da palavra-passe, tendo em vista não ser possível coagir um indivíduo a realizar uma declaração. Nota-se assim uma restrição considerável à desencriptação coativa de telemóveis.

Concluída a desencriptação coativa, será possível proceder com a pesquisa de dados informáticos e eventualmente a recolha dos mesmos, realizando-se a perícia dos mesmos, seguindo a determinação do artigo 151.º do Código de Processo Penal que aduz que a prova pericial terá lugar quando os factos exigirem conhecimentos técnicos, científicos e artísticos.

1.3 Considerações acerca da desencriptação coativa

Como é possível observar, diante das disposições legais e o atual entendimento jurisprudencial, que a desencriptação coativa de telemóveis é possível, porém não é imune a críticas.

As nossas críticas iniciam-se o já mencionado artigo 61.º, n.º 3, alínea d), do Código de Processo Penal, que determina que o arguido tem o dever de sujeitar-se a diligências de prova. No nosso entendimento, este dispositivo não é compatível com os direitos, liberdades e garantias protegidos pela Constituição e com os princípios constitucionais e do processo penal[140].

[140] O Direito Processual Penal tem princípios próprios e constitucionais que o enformam. Podemos apontar alguns princípios constitucionais como o princípio geral do Estado de Direito Democrático, bem como o da necessidade e proporcionalidade dispostos no art. 18.º, n.º 2 da Constituição. Já com relação aos princípios próprios do Processo Penal, estes são inúmeros, como o do juiz natural, o da estrutura acusatória do processo, o da celeridade, o do direito à assistência jurídica dentre outros, como muito bem aponta DIAS, José Figueiredo, *Direito Processual Penal*, I Vol, Coimbra, Coimbra Editora, 1974, pp. 80-112.

Compreendemos que o arguido não deve ser compelido a cooperar na busca pela verdade material do processo, pelo contrário, firmamos o entendimento que o objetivo do arguido no âmbito do Processo Penal deverá unicamente garantir a sua própria defesa. A busca pela verdade material deve ser um objetivo a ser perseguido pela acusação e será esta que deverá buscar as evidências que sustentem os seus argumentos, sem necessidade de participação do arguido para tanto.

Ressaltamos a diferença entre o dever de colaboração do arguido e a necessidade de este curvar-se à determinadas situações, como por exemplo, o dever de submeter-se a uma prisão preventiva caso esta seja considerada necessária. Neste caso não há uma colaboração do arguido na busca pela verdade, apenas a submissão do arguido à uma decisão judicial.

Também ressaltamos que, em razão dos avanços tecnológicos, dados biométricos têm cada vez mais sido adotados como uma forma segura de confiança de dados, como por exemplo, em forma de chave criptográfica. Portanto, a tendência será que as diligências de prova serão cada vez mais intrusivas e com um potencial cada vez mais violador de direitos, como RENATO LOPES MILITÃO[141] ressalta "amplificar, facilitar e agilizar medidas de investigação criminal no domínio da obtenção da prova digital torna-se ainda mais agressivo, intrusivo, desleal e perigoso do que fazê-lo em relação as 'provas tradicionais'".

Por isso, defendemos que em razão da gravidade da desencriptação coativa, ela não deve ser fruto de uma interpretação legislativa, e sim deve estar expressa em uma norma habilitante que trate do tema de forma completa e exaustiva, em respeito pelo princípio da legalidade, presente nos artigos 48.º a 51.º, 53.º e 283.º do Código de Processo Penal que determina a estrita vinculação à lei[142]. LARA SOFIA PINTO tem o mesmo entendimento ao compreender que deve haver uma tipicidade dos casos de colaboração do arguido em lei expressa, adequada e proporcional em respeito ao artigo 18.º, n.º 2 da Constituição[143].

---

[141] MILITÃO, Renato Lopes, A propósito da prova digital no Processo Penal. *Revista da Ordem dos Advogados*, 2012, p. 247–281.
[142] Cf., DIAS, José Figueiredo, *Direito Processual Penal*, I Vol., Coimbra, Coimbra Editora, 1974, p. 125-136.
[143] PINTO, Lara Sofia, Privilégio contra a auto-incriminação versus colaboração do arguido. In: *Prova Criminal e Direito de Defesa*. Coimbra, Almedina, 2010, p. 25.

Em conclusão, nos utilizamos do entendimento do Tribunal Constitucional no Acórdão n.º 183/2008 publicado no Diário da República de 22 de Abril de 2008, para afirmar que, mesmo em face das exigências comunitárias que visam pressionar um poder cada vez mais punitivo por parte do Estado, a liberdade pessoal e as garantias do cidadão sempre terão um especial valor. E que os direitos fundamentais do cidadão deverão ser sempre a lanterna que nos guia em um caminho escuro, mesmo diante de desafios inéditos, como os apresentados pela tecnologia.

Uma vez apresentada a possibilidade jurídica da desencriptação coativa e a nossa crítica a respeito dela, avançamos para a análise dos dados informáticos como o meio de prova alvo da pesquisa de dados informáticos e como ponto essencial para uma análise completa das consequências jurídicas da desencriptação coativa de telemóveis.

2. Dados informáticos como prova

O amplo uso da internet e de aparelhos telemóveis é um desafio a ser enfrentado pelo direito diante do seu potencial de modificar a prática de ilícitos e alterar a forma de investigação de crimes. A Lei do Cibercrime se propôs a solucionar alguns impasses já existentes, apresentando meios de obtenção de prova relacionados às provas digitais, como a pesquisa de dados e recolha de informáticos. Como abordamos, muitas vezes os dados informáticos são protegidos pela criptografia, o que impossibilita a realização de meios de obtenção de prova, sendo que uma das saídas para este obstáculo é a desencriptação coativa de telemóveis.

Uma vez que a desencriptação coativa de telemóveis seja bem sucedida, eventualmente a pesquisa e a recolha de dados informáticos ocorrerá e os dados informáticos poderão ser utilizados como prova. Os dados informáticos foram definidos pelo artigo 2.º, alínea b), da Lei do Cibercrime, como representações de factos, informações ou conceitos sob

uma forma suscetível de processamento num sistema informático, incluindo os programas aptos a fazerem um sistema informático executar uma função[144]. Neste contexto, os dados informáticos podem ser considerados meios de prova digitais.

Diante disso, para realizarmos uma análise completa das consequências jurídicas da desencriptação coativa, nos propomos abordar como os dados informáticos poderão ser utilizados como prova no Processo Penal tendo em vista as suas repercussões nos direitos fundamentais do arguido.

O Direito Processual Penal, segundo MANUEL DA COSTA ANDRADE[145] é uma província do direito constitucional, o verdadeiro direito constitucional aplicado, sendo a Constituição a sua principal fonte, que visa proteger bens jurídicos reafirmar a validade das normas e reforçar a confiança na sua vigência, restabelecer a paz jurídica e prosseguir a verdade preordenada à realização da justiça material.

A realização da justiça material passa indubitavelmente pela atividade probatória, que pode ocorrer tanto no âmbito do inquérito[146] quanto ao longo do processo a depender da necessidade, versando sobre factos controversos do processo e com objetivo de gerar convicção no julgador[147] [148]. De forma simplificada, parafraseando GIL MOREIRA DOS SANTOS, a prova começa onde se perde, subjetivamente, a consciência da probabilidade[149].

A prova[150], segundo PAULO SOUSA MENDES, que parafraseia o artigo 124.º do Código de Processo Penal, é o esforço metódico através do qual são demonstrados os factos relevantes para a existência do crime, a

---

144 Ao contrário do que podemos imaginar, eles não consistem apenas de códigos, pelo contrário, eles podem ter diversos formatos, como textos, imagens, vídeos, músicas ou aplicações e/ou programas, que podem ser encontrados em sistemas de armazenamento de dados em nuvem, em discos externos, em pen-drives, e até mesmo no próprio disco interno de aparelho de eletrónico, como um telemóvel.

145 *Ibidem* COSTA ANDRADE, 2006, p. 72.

146 "O inquérito compreende o conjunto de diligências que visam investigar a existência de um crime, determinar os seus agentes e a responsabilidade deles e descobrir e recolher as provas, em ordem à decisão sobre a acusação". *In* MARQUES DA SILVA, 2000, p. 68.

147 GONÇALVES, Manuel, Recolha de amostras de ADN para fins de investigação criminal Suspeito. *Revista do Ministério Público,* n.º 136, p. 199–222, 2013.

148 DE JESUS, Francisco Marcolino. *Os Meios de Obtenção da Prova em Processo Penal.* 2ª. Edição. Almedina, 2019, p. 33/84.

149 *Ibidem* MOREIRA DOS SANTOS p. 207.

150 Também disposta no artigo 341.º do Código Civil que aduz: "As provas têm por função a demonstração da realidade dos factos".

punibilidade do arguido e a determinação da pena ou medida de segurança aplicáveis[151]. Além de ser um direito que advém do direito de ação e defesa previstos na Constituição conforme apontam GOMES CANOTILHO E VITAL MOREIRA[152].

O tema das provas não está restrito unicamente ao Código de Processo Penal, pelo contrário, está também disposto no Código Civil e de Processo Civil, como no artigo 341.º do Código Civil, que pode ser considerado também como fonte da doutrina sobre prova no direito processual penal, pois dispõe acerca da finalidade da prova – demonstrar a realidade dos factos[153]. Com relação ao Código de Processo Penal, o legislador dedicou à matéria todo um livro, que vai do artigo 327.º ao 374.º, onde se reúnem todas as disposições fundamentais acerca da matéria, sendo a *lex generalis* a respeito da prova, pese embora a legislação avulsa também tenha peso na matéria.[154]

O Código de Processo penal optou por adotar uma liberdade às provas, como observamos no artigo 125.º do CPP, onde é disposto que todos os meios de prova poderão ser utilizados, desde que ela própria não proíba. A leitura deste artigo deve ser cautelosa, como bem ressalta BENJAMIM SILVA RODRIGUES, tendo em vista que a cláusula deste artigo poderá fechar-se no caso de o novo meio de prova ou meio de obtenção de prova ofender, em grau insuportável um direito fundamental[155]. Entretanto, apesar das limitações, é possível extrair o entendimento de que há um espaço para novos meios de prova, que inclui as resultantes dos avanços tecnológicos, como as provas digitais.

Em Portugal, a prova digital está regulamentada em três diplomas legais nomeadamente, o Código de Processo Penal, a Lei n.º 32/2008, de 17 de julho - que regula a conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas -, e a Lei do

151 *Ibidem* SOUSA MENDES, 2004, p. 132.
152 CANOTILHO, J.J Gomes e MOREIRA, Vital, *Constituição da República Portuguesa Anotada*, Vol. I, 4.º, Ed. Revista, Coimbra, Coimbra Editora, 2007, p. 410.
153 VALENTE, Manuel Monteiro Guedes, *Cadeia de Custódia da Prova*, Coimbra, Editora Almedina, 2019, p. 24.
154 SILVA, Sandra Oliveira e. Legalidade da prova e provas proibidas. *Revista Portuguesa de Ciência Criminal,* Ano 21, n. 4, p. 545–591, 2011.
155 RODRIGUES, Benjamim Silva, *Da Prova Penal, Tomo VI: Novos métodos "Científicos" de investigação Criminal nas Fronteiras das Nossas Crenças*, 1ª Ed., Editora Rei dos Livros, 2011, p. 34.

Cibercrime, sendo esta a sua pedra angular segundo aponta CONDE CORREIA[156].

Apesar da panóplia legislativa, o legislador optou por não definir a prova digital, abrindo espaço para que a doutrina e a jurisprudência a conceituasse. Na doutrina, JOÃO GAMA GONÇALVES as define como quaisquer informações que tenham valor probatório e que estejam armazenadas digitalmente ou que sejam transmitidas através de sistema e redes informáticas ou de comunicações tanto públicas como eletrónicas. BENJAMIM DA SILVA RODRIGUES por sua vez conceitua as provas digitais como qualquer fluxo informacional ou comunicacional digital, que, estaticamente, se encontre armazenado, tratado ou processado, ou, pelo contrário, dinamicamente, seja transmitido, veiculado ou não por meio das redes informáticas ou de serviços e comunicações eletrónicas, quer ao nível de um ciclo informacional e comunicacional fechado ou aberto, privado ou público[157]. Já a Convenção de Budapeste define as provas digitais como qualquer evidência passível de ser coletada na forma eletrónica.[158] E por fim, o departamento de justiça dos Estados Unidos da América optou por as definir como informações transmitidas e armazenadas de forma binária que poderá ser utilizada nos tribunais.[159]

Ressalte-se que, por muitas vezes, há uma confusão entre os conceitos de prova eletrónica e prova digital. Contudo, DAVID SILVA RAMALHO aponta que se tratam de conceitos diferentes. A prova eletrónica compreende todos os tipos de dados seja analógico ou digital que possam estar em conteúdo digital, já a prova digital é uma subespécie da prova eletrónica que abrange apenas as provas em formato digital, associados à lógica binária[160]. No presente estudo, optamos por adotar o termo da prova

---

156 *Idem* CONDE CORREIA, 2014, p. 29–59.

157 *Ibidem* RODRIGUES, 2008, p. 534.

158 European Union Agency for Cybersecurity, *Eletronic evidence – a basic guide for First Responders*. Disponível em < https://www.enisa.europa.eu/publications/electronic-evidence-a-basic-guide-for-first-responders > Acesso em 24 de abril de 2021.

159 U.S. Department of Justice, Office of Justice Programs, National Institute of Justice, *Forensic Examination of Digital Evidence: A Guide for Law Enforcement*, 1st ed, 2014 p. 46. Disponível em <https://www.ncjrs.gov/pdffiles1/nij/199408.pdf > Acesso em 24 de abril de 2021.

160 *Bit*, é a menor unidade de informação ser armazenada ou transmitida na comunicação de dados. Os computadores possuem comandos que testam e manipulam bits. O valor de um bit é armazenado como uma carga elétrica dentro de um dispositivo de memória, mas também podem ser representados fisicamente por vários meios, como pela eletricidade, através de fibras óticas, ou em leitores e gravadores de discos, por ondas eletromagnéticas, como nas redes wireless. Disponível em: < https://www.significados.com.br/bits/ >

digital e não eletrónica, tendo em vista que a desencriptação coativa de telemóveis visa a busca por dados informáticos que são essencialmente imateriais.

As provas digitais podem estar presentes em diversos tipos de aparelhos eletrónicos como computadores, *tablets,* armazenamento USB, e telemóveis[161], dentro destes aparelhos é possível encontrar diversas categorias de provas digitais, como por exemplo, fotos, músicas, vídeos, mensagens e logs de ligações[162]. Contudo, existem características comuns a todos os tipos de provas digitais, que melhor analisaremos a seguir.

Primeiramente, acima de tudo, a prova digital deverá ser consistente com o sistema legal probatório do processo penal português, como ressalta ALBERTO GIL LIMA CANCELA[163], ao dizer que esta deverá apresentar-se em uma linguagem simples de modo que possa ser aplicada pela generalidade dos operadores judiciários

Primeiramente, por existir em um ambiente altamente tecnológico, a prova digital é considerada complexa, tendo em vista que não é qualquer utilizador que é capaz de realizar a sua recolha. Por isso, compreende-se que não poderão ser utilizados os mesmos investigadores que seriam utilizados em uma investigação que não se utilize de provas digitais[164].

Surgem assim as polícias científicas, que são voltadas exclusivamente para a recolha e análise das provas digitais, com conhecimentos forenses elevados e materiais adequados para a realização de investigações.

As investigações também não poderão ser conduzidas da forma "tradicional", pelo contrário, as medidas deverão ser criadas sob medida para a realidade das provas digitais[165]. Sendo esta a razão pela qual surgiu

[161] *Idem* CONSELHO DA EUROPA, pp. 16-31.
[162] Os logs de ligações são um registo de todas as ligações realizadas e recebidas por aquele aparelho telemóvel.
[163] *Ibidem* CANCELA, 2016.
[164] RAMALHO, David Silva, *Métodos Ocultos de Investigação Criminal em Ambiente Digital*, Coimbra, Coimbra Editora, 2017, p. 103.
[165] Como aponta Orin S. Kerr ao ressaltar que a prova digital não pode ser considerada como uma derivação da prova física, pois são realidades distintas que devem ser objeto de diferentes enquadramentos jurídicos, livre de amarras da analogia e de subsidiariedade de sistemas criados para provas físicas. O autor também defende o mínimo de remissões, apenas em caráter formal. *In* KERR, Orin S., Search Warrants in na Era of Digital Evidence, *Mississipi Law Journal*, Vol. 75 (2005), p.. 92-97.

a ciência forense digital ou em inglês *digital forensic*[166], que visa orientar a investigação criminal desenvolvendo regras predeterminadas acerca da preservação, recolha, gravação, validação, identificação, análise, interpretação, documentação e apresentação das provas digitais.

Existem diversos modelos de Ciência Forense Digital, foram aos poucos desenvolvidos por diferentes países[167] para adaptarem-se aos respetivos sistemas judiciais, uns mais complexos que outros[168]. Em Portugal não há diploma no regime processual penal que trate especificamente das provas digitais, como bem ressalta JOÃO CONDE CORREIA[169], ao afirmar que o legislador escolheu a via incerta da pluralidade e da complexidade, criando um sistema não oferece bússola para encontrar o caminho mais seguro. Porém, compreendemos que a Lei do Cibercrime juntamente com disposições do CPP nos dão uma base legal para prosseguir com a ciência forense digital tendo em vista que trata a respeito das perícias forenses no artigo 159.º.

Com relação às perícias forenses voltadas especificamente para os telemóveis, estas destacam-se por alguns motivos específicos que iremos abordar. Primeiramente, como ressaltam NENA LIM e ANNE KHOO, os telemóveis, diferentemente dos computadores pessoais, são desenvolvidos para algumas tarefas específicas e portanto, tem um sistema mais limitado que os computadores, pese embora tenham cada vez mais ferramentas[170].

Além disso, estes aparelhos podem ser considerados o grande exemplo de avanço tecnológico, tendo em vista que se modificam e ganham novas ferramentas todos os anos o que faz com que a ciência forense digital voltada à estes aparelhos também tenha que se desenvolver na mesma velocidade, o que nem sempre ocorre, como aponta MARK TAYLOR et al.

---

166 Inicialmente chamada de Computer Forensic Science que em razão da evolução tecnológica passou a ser chamada de Ciência Forense Computacional e Ciência Forense Digital em razão da maior amplitude do termo, que inclui as ativiades de identificação, recolha e análise da prova digital. *In* RAMALHO, David Silva, 2017, p. 110-111.

167 Por exemplo, Austrália adota as *Guidelines for the Management of IT Evidence* (2003), o Reino Unido utiliza o *Good Practice for Computer based Electronic Evidence,* da *Association of Chief Police Officers. In* MASON, Stephen e SHELDON, Andrew, *Proof: The investigation, collection and examination of digital evidence in Evidence*, University of London Press, Institute of Advanced Studies, 2017, p. 73-75.

168 *Ibidem* RODRIGUES, 2008, p. 536.

169 *Idem* CONDE CORREIA, 2014.

170 LIM, Nena, & KHOO, Anne, "Forensics of computers and handheld devices: identical or fraternal twins?." *Communications of the ACM* 52, nº. 6, 2009, pp. 132-135

"New mobile telephones are constantly being developed, requiring forensic software tool manufacturers to update their tools continually to keep coverage current. The growing number and variety of mobile telephones makes it difficult to develop a single process or forensic software tool to address all eventualities"[171].

Por este motivo, é sabido que a brecha de segurança encontrada pelos investigadores ao longo do caso *Apple v. FBI* vai até alguns modelos já datados de Iphones, nomeadamente os 5C. Após a adoção da leitura de biometria digital, a tecnologia implementada pela empresa modificou-se, impossibilitando novamente que estes aparelhos sejam acedidos[172].

Contudo, independentemente do modelo de ciência forense adotada, existem etapas básicas que serão seguidas por todos eles, sendo elas: a identificação, preservação, recolha, exame, análise, apresentação e decisão[173], o método adotado que poderá modificar-se e também atualizar-se a medida do tempo[174] [175]. Independentemente do método adotado, em nome da transparência do procedimento, este deverá ser conduzido com proximidade entre o especialista forense, a autoridade judiciária e o órgão de polícia criminal[176].

Outra característica das provas digitais que merece atenção é a imaterialidade, tendo em vista que apenas existem em *bits*. Neste contexto, EOGHAN CASEY ressalta que o que vemos em um telemóvel é uma ilusão

---

[171] MARK, Taylor, *et.al* Digital evidence from mobile telephone applications. *Computer Law & Security Review* 28, n.º 3, 2012, pp. 335-339

[172] A respeito do assunto *In* SKOROBOGATOV, Sergei, The bumpy road towards Iphone 5C NAND mirroring, Disponível em https://arxiv.org/abs/1609.04327

[173] PALMER, Gary, A Road Map for Digital Forensic Research, *DFRWS Technical Report, Report from the First Digital Forensic Research Workshop*, 6 de Novembro de 2001, disponível em https://dfrws.org/wpcontent/uploads/2019/06/2001_USA_a_road_map_for_digital_forensic_research.pdf acesso em 13 de abril de 2020

[174] Há atualmente um grande debate a respeito do uso da tecnologia *blockchain* para garantir a integralidade da evidência digital o que seria um avanço tecnológico. Blockchain é uma espécie de banco de dados que visa utilizar da descentralização como medida de segurança para garantir a integralidade de uma determinada informação. *In* TIAN, Zhihong, *et al.* Block-DEF: A secure digital evidence framework using blockchain."*Information Sciences* 491 (2019): 151-165. Disponível em < shorturl.at/bmLPX>

[175] Este tema torna-se mais complexo quando analisamos o panorama europeu que permite um rápido fluxo informacional entre diferentes países, dificultando a investigação e a persecução penal em cibercrimes ou delitos que tenham provas digitais em países diversos. Em razão disso, foi proposta uma Ordem Europeia de Preservação de provas eletrónicas que, semelhante a um mandado de detenção europeu, que permitiria a uma autoridade judiciária de um Estado-Membro solicitar a um prestador de serviço ou ao seu representante legal em outro Estado-Membro, que preserve determinados dados. Em seguida, haveria um pedido subsequente de auxílio judiciário para que a autoridade judiciária do outro Estado-Membro obtenha a prova do prestador de serviço através de uma ordem de investigação ou de uma ordem europeia de produção de prova. Isto posto, é necessário que haja uma padronização do modelo de ciência forense adotado, sob pena de tornar a Ordem Europeia de Preservação de Provas uma autêntica Torre de Babel. Vide a Proposta de Regulamento do Parlamento Europeu e do Conselho relativo às ordens europeias de entrega ou conservação de provas eletrónicas em matéria penal. Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A52018PC0225

[176] *Ibidem* RAMALHO, David Silva, 2017, p. 117.

que nos permite instruir o sistema informático a realizar uma tarefa, sem ela, apenas especialistas compreenderiam os códigos complexos e necessários para que uma tarefa seja ordenada[177]. Por isso, compreende-se que as provas digitais precisam de um mediador[178], também chamado de transportador, que faz com que ela seja representada[179] nos aparelhos eletrónicos, por exemplo, uma imagem será representada através de mediadores diferentes em um telemóvel e em um computador[180], muitas vezes o aparelho eletrónico não tem capacidade de mediar um ficheiro, pela ausência de mediador.

Em razão da imaterialidade, as provas digitais são consideradas voláteis ou instáveis, tendo em vista que ela estão sujeitas a mudanças rápidas e irreversíveis.[181] Elas podem ser facilmente alteradas e até mesmo perdidas caso manipuladas de forma descuidada ou intencionalmente modificadas[182] ou destruídas[183]. Isto poderá ocorrer por diversos motivos, por exemplo, danificações no servidor ou aparelho onde estão armazenadas, como, por exemplo, a falta de energia, a corrupção de ficheiros, a humidade ou campos magnéticos que afetam a memória de computadores[184].

A modificação ou ocultação das provas digitais também poderá ocorrer de forma intencional, com o objetivo de dificultar a análise das provas no âmbito de uma investigação. Como ocorre por exemplo com a anonimização[185] das provas digitais, que são métodos que visam impedir que o investigador criminal consiga associar uma conduta ao seu autor

---

177 CASEY, Eoghan, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*, 3ª ed., Academic Press/Elsevier, 2011, p. 25.
178 WEIR, George R.S & MASON, Stephen, *Electronic Evidence*, Londres, LexisNexis Butterwoths, 2012, p. 31
179 JONES, Nigel*, et. al.* Vic CyberCrime@IPA, European Union and Council of Europe, Joint Project on Regional Cooperation against Cybercrime, *Electronic evidence guide - A basic guide for police officers, prosecutors and judges,* Version 2.0, 2020. Disponível em shorturl.at/cdP06 acesso em 24 de Abril de 2021.
180 *Ibidem* DEL CANTO, 2002, p. 83-84
181 *Ibidem* RODRIGUES, 2009, p. 514.
182 "(...) quando são utilizados programas para alterar o *metadata* de certos ficheiros. Destaca-se, nesta matéria, o programa *Times-tomp,* cuja principal função é alterar o *metadata* que regista a data de criação e de alteração de ficheiros informáticos. Assim, se um investigador eleger como um dos parâmetros de pesquisa e triagem da informação recolhida a data de criação ou de alteração dos documentos dos documentos visados, o resultado obtido poderá excluir a prova verdadeiramente pretendida, por a mesma ter tido estas propriedades previamente alteradas". *In* RAMALHO, 2017, p. 172.
183 PALACIOS, Fernando Pinto, CAPILLA, Purificación Pujol. *La prueba en la era digital* Madrid, Wolters Kluwer, 2017, p. 28.
184 *Idem* JONES, Nigel, et. al. 2020.
185 O dado anônimo é aquele que não pode ser identificado com um indivíduo ou computador. O vinculo entre os dados e os titulares pode ser quebrado através de diversos métodos, como supressão, generalização, randomização e pseudoanonimização. *In* BIONI, Bruno. "Compreendendo o conceito de anonimização e dado anonimizado." *Cadernos Jurídicos. São Paulo, ano* 21, 2020, pp. 191-201.

ocultando a sua origem ou protegendo-se através de sistemas como a criptografia, como ressaltamos no primeiro capítulo do presente estudo. Por isso, a investigação das provas digitais deverá ser técnica, célere e adaptada às suas peculiaridades, como forma de garantir a confiabilidade e preservar a cadeia de custódia das provas digitais, que é um tema de extrema relevância, especialmente quando tratamos das provas.

A cadeia de custódia, segundo MANUEL MONTEIRO GUEDES VALENTE, é uma garantia formal e material da tutela da prova tendo em vista a sua função de formar convicção no julgador em sede de processo crime. O principal objetivo dela é evitar que quaisquer indícios ou vestígios probatórios sejam alterados, ao mesmo tempo que visa garantir o princípio da confiança e da boa fé[186] na relação entre o Estado e de seus operadores com a sociedade e o cidadão indiciado ou acusado[187]. Assim, o único modo de garantir a confiança nos meios de prova é garantir a integridade e autenticidade das mesmas através do respeito às regras.

Este tema é de extrema relevância quando tratamos das provas digitais, tendo em vista que, além de ser um novo meio de prova, em razão das suas características apontadas anteriormente são suscetíveis a modificação com extrema facilidade, por isso ressaltamos o tema da cadeia de custódia.

MANUEL MONTEIRO GUEDES VALENTE considera a cadeia de custódia uma técnica jurídico-processual que visa garantir a identidade e a autenticidade da prova, desde o meio de obtenção de prova até a sua apreciação pelo Tribunal[188].

É importante ressaltar que a cadeia de custódia tem uma relação íntima com os princípios fundantes do processo penal e os demais direitos fundamentais protegidos constitucionalmente tendo em vista que eles são vinculativos de todo o ordenamento jurídico[189]. Ressaltamos o devido

[186] O princípio da boa fé é um princípio geral do Direito entranhado na materialidade constitucional dos Estados democráticos constitucionais, sendo a essência medular de uma sociedade republicana e democrática. *In* VALENTE, Manuel Monteiro Guedes, *Cadeia de Custódia da Prova*, Coimbra, Editora Almedina, 2019, p. 34
[187] *Ibidem* VALENTE, 2019, p. 33-34.
[188] *Ibidem* VALENTE, 2019, p. 45
[189] ROXIN, Claus, *Introdução ao Direito Penal e ao Direito Processual Penal*, Belo Horizonte, Del Rey Editora, 2007, p. 154-155.

processo legal[190], o princípio da legalidade[191], o princípio da jurisdicionalidade[192], o princípio da prossecução do interesse público[193], o princípio da boa-fé[194] e o princípio da transparência[195].

Em razão das especificidades das provas digitais, que acabaram por gerar a ciência forense digital e pressionar pela especialização dos atores judiciais, MANUEL MONTEIRO GUEDES VALENTE aponta que haverá violação da cadeia de custódia caso não haja respeito pelo princípio da indisponibilidade das competências[196], ou seja, existem indivíduos especializados com competências específicas para apurar, adquirir, recolher, coletar, apreender e conservar a prova, o desrespeito desta competência coloca todos os atos do processo sob questionamento em razão do risco de contaminação ou modificação irreparável[197].

Além disso, qualquer falta de controlo e verificação da cadeia de custódia irá, na opinião de CLAUS ROXIN, causar a inadmissibilidade da prova, e caso esta seja submetida a julgamento a sua inadmissibilidade de valoração[198] [199], posicionamento também adotado por MANUEL MONTEIRO GUEDES VALENTE[200], o que demonstra o peso e a importância da matéria no âmbito do Processo Penal[201].

Além disso, a potencial ideia de a sociedade não poder confiar inteiramente na imparcialidade do Estado para seguir os padrões necessários de recolha e manipulação de evidências cria um ambiente de desconfiança geral que não é benéfico ao Processo Penal, afetando a

190 Vide n.º4 do artigo 20.º da Constituição
191 Vide Artigo 2.º do Código de Processo Penal
192 Vide artigos 27.º, n.º 2 e 32.º, n.º 4 ambos da Constituição
193 Vide artigo 266.º da Constituição
194 "O princípio da boa fé não é um mero princípio de intenção moral, mas um verdadeiro princípio legitimador da atividade da administração da justiça por parte do Estado, sendo de grande relevância muito em especial para a atuação da polícia criminal. *In* VALENTE, 2019, p. 58
195 Vide Artigo 86.º do Código de Processo Penal
196 Presente nos artigos 272.º, n.º 3 e 202.º, n.º 3 da Constituição e dos artigos 1.º alíneas c) e d), 9.º, 55.º, 263.º, 288.º e 290.º todos do Código de Processo Penal.
197 *Ibidem* VALENTE, 2019, p. 49
198 ROXIN, Claus E SCHÜNEMANN, Bernd, *Derecho Procesal Penal,* 29.ª Edição de Darío Rolón e Mario Amoretti, Buenos Aires, Editora Didot, p. 190-194.
199 "A conduta ilícita do operador judiciário implica uma dupla consequência: a proibição de toda a dimensão da prova – inadmissibilidade da prova no processo-crime e, quando esta não ocorra, inadmissibilidade de valoração, impondo-se o respetivo desentranhamento da mesma fazendo assim retroagir a inadmissibilidade da prova –;" *In* VALENTE, 2019, p. 80
200 *Ibidem* VALENTE, 2019, p. 85.
201 A temática das proibições de prova irá ser abordada de forma mais completa no Capítulo III do presente estudo.

confiança, a credibilidade e a segurança jurídica necessária que o processo penal requer[202].

Uma vez superado os detalhes técnicos da recolha da prova digital, temos que nos atentar aos princípios que estas deverão respeitar quando utilizadas no processo. Como os demais meios de prova, as provas digitais seguem os mesmos princípios gerais das provas[203], porém em razão da sua peculiaridade, elas também têm princípios próprios. Semelhantemente como ocorre com o conceito, os princípios próprios das provas digitais ainda não são unanimidade, em razão disso, optamos por apontar os princípios desenvolvidos pela União Europeia e pelo Conselho da Europa.

O primeiro princípio e a base dos demais será a necessidade da manipulação das provas digitais por especialistas, o que é crucial para a utilização das provas digitais, pois, devido às características anteriormente citadas, correm o risco de serem modificadas não intencionalmente, o que poderá eventualmente causar a invalidação das provas em âmbito processual.[204] Em Portugal, a entidade especializada responsável pela perícia forense digital é a polícia judiciária através da Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica – UNC3T[205].

ANA RAQUEL LEITE ressalta a importância do caráter especial da investigação tendo em vista que, segundo a autora, a utilização de meios tradicionais já disponíveis do Processo Penal violariam o princípio constitucional da igualdade, que determina que seja tratado igualmente o que seja igual e diferente o que é diferente[206]. Inclusive, ROGÉRIO BRAVO sustenta que a norma penal tradicional é ineficaz com relação aos avanços tecnológicos, ressaltando que a norma penal deve ser adaptada ao ambiente tecnológico levando em consideração o tempo, a natureza do

[202] *Ibidem* VALENTE, 2019, p. 41
[203] Os principais princípios relativos à prova são: o princípio da legalidade, o princípio da livre apreciação da prova, princípio da oralidade, princípio da imediação, princípio da concentração, princípio da investigação ou verdade material, princípio da presunção de inocência, princípio do in dubio pro reo e o princípio do contraditório.
[204] *Idem* JONES, 2020.
[205] Unidade operacional especializada em resposta preventiva e repressiva aos crimes previstos na Lei do Cibercrime e crimes praticados com recurso ou por meio de tecnologias ou de meios informáticos. https://www.policiajudiciaria.pt/unc3t/
[206] LEITE, Ana Raquel Gomes, *Criminalidade Informática: Investigação e Meios de Obtenção de Prova*, Dissertação apresentada no âmbito do 2.º Ciclo de Estudos em Direito, Faculdade de Direito da Universidade de Coimbra, com especialização em Ciências Jurídico-Forenses, sob orientação da Professora Doutora Helena Moniz, Coimbra, 2013, p. 17.

espaço virtual e as relações deste com outros espaços de existência humana[207].

O segundo princípio é o da não alteração da prova, que visa garantir a integridade da prova nos atos de recolha, tratamento e armazenamento. Para que ele se efetive, os investigadores deverão excluir qualquer tipo de atuação que possa contaminar os dados pesquisados e eventualmente armazenados.[208]

Para que a cadeia de custódia se mantenha íntegra, todas as atividades relativas à prova digital deverão ser documentadas, seguindo o princípio da garantia de documentação em todas as fases processuais, tendo em vista que esta é a única forma de visibilidade da cadeia de custódia[209] e de que estas provas tenham seu uso admitido como evidência processual. Além disso, a documentação possibilita que as provas sejam auditadas posteriormente[210] e que também sejam repetidas caso necessário[211]. É importante ressaltar que as provas digitais evoluem à medida que a tecnologia evolui, em uma alta velocidade, sendo necessário que as técnicas de recolha, tratamento e utilização das provas digitais evoluam na mesma velocidade.[212]

Por fim, há o princípio da responsabilização compartilhada dos vários intervenientes na produção das provas digitais, que determina que todos os agentes forenses responsáveis por este meio de prova são responsáveis pela sua integridade e não modificação. Portanto, para que sejam utilizadas em âmbito processual, as provas digitais deverão ser autênticas, íntegras, não enviesadas e confiáveis.[213]

Diante do exposto, no presente capítulo foi possível observar a urgência da discussão a respeito da desencriptação coativa de telemóveis diante dos avanços tecnológicos que cada vez mais avançam e exigem do direito respostas à altura dos desafios.

---

[207] BRAVO, Rogério, *As tecnologias de Informação e a Compressão dos Direitos, Liberdades e Garantias – os efeitos das regras "10/10" e "1/1"*, Lisboa, 2012, p.1
[208] *Ibidem* RODRIGUES, 2009, p. 726
[209] *Ibidem* RODRIGUES, 2009, p. 728
[210] *Idem* JONES, 2020.
[211] *Ibidem* RODRIGUES, 2009, p. 728
[212] *Idem* JONES, 2020.
[213] *Idem* JONES, 2020.

Pudemos apresentar as bases jurídicas sob as quais alguns países europeus justificaram a desencriptação coativa nos seus próprios ordenamentos jurídicos e também realizar uma análise interpretativa do ordenamento jurídico português a fim de compreendermos ser possível, através da analogia, a aplicação da desencriptação coativa de telemóveis como um dever do arguido fundado no artigo 61.º do Código de Processo Penal, pese embora as críticas devidamente levantadas.

Uma vez apresentada a possibilidade jurídica, avançamos para como a desencriptação se daria, através de um despacho da autoridade judicial competente, que deverá ser fundamentado e deverá levar em consideração a necessidade extrema dos dados informáticos para a busca pela verdade material.

Nesta toada, realizamos uma análise dos dados informáticos como prova digital no processo penal, tendo em vista que esta é uma matéria recente e ainda pouco abordada. Mencionamos o surgimento da ciência forense digital e da importância da existência de profissionais especializados na área tendo em vista as características da prova digital.

Desta forma, no terceiro capítulo que se seguirá, munidos do panorama apresentado, iremos abordar as consequências jurídicas da desencriptação coativa.

CAPÍTULO III - CONSEQUÊNCIAS JURÍDICAS DA DESENCRIPTAÇÃO COATIVA

Até este ponto, o presente estudo buscou apresentar como a criptografia, uma ferramenta criada para a proteção da privacidade dos usuários, pode se tornar um obstáculo na investigação de crimes, tendo em vista que obsta o acesso ao aparelho e a aplicação de meios de obtenção de prova. Observamos também, como os dados informáticos, uma vez pesquisados e recolhidos, podem ser considerados meios de prova, em razão da atual importância e das diversas informações que podem carregar.

Isto posto, no presente capítulo visamos realizar uma análise das consequências jurídicas da adoção da desencriptação coativa de telemóveis. Para fins didáticos, esta análise será realizada em duas partes, a primeira abordará as consequências para os direitos fundamentais do arguido e a segunda tratará a respeito das consequências jurídico processuais.

1. Consequências para os direitos fundamentais do arguido

FIGUEIREDO DIAS aponta que o Direito Processual Penal sendo direito constitucional aplicado, se utiliza da Constituição como fundamento e auxílio para a resolução do conflito penal[214], desta forma haverá uma densidade de normas inscritas na Constituição que têm alcance diretamente jurídico-penal como bem ressalta MANUEL DA COSTA ANDRADE[215].

[214] DE FIGUEIREDO DIAS, Jorge, 1974, Prefácil.
[215] COSTA ANDRADE, Manuel da, *Constituição e direito penal in A justiça nos dois lados do Atlântico*, Lisboa, Fundação Luso-Americana para o desenvolvimento, 1998, p. 198.

Por esta razão, do mesmo modo que as normas constitucionais permeiam todas as etapas do processo penal, todas as ações ao longo do mesmo irão gerar consequências para os direitos fundamentais do arguido, sejam elas positivas no através da sua proteção ou negativas através de eventuais violações.

Para um perfeito e estável funcionamento, a Constituição concebeu direitos fundamentais que visam proteger um núcleo de bens essenciais aos indivíduos, contudo eles não são absolutos e ilimitados[216], há neste caso uma possibilidade de limitação prevista na própria Constituição no artigo 18.º, n.º 2 o qual dispõe que eventuais restrições deverão limitar-se ao necessário na medida em que salvaguarda outros direitos ou interesses constitucionalmente protegidos[217], por isso, dizemos que há um limite na busca pela verdade.

A respeito da verdade, é necessário ressaltarmos alguns pontos. A "verdade" é um conceito complexo, que pode ser dividido em três principais categorias, a humana, a absoluta e a material. A verdade humana é aquela que cada um de nós forma a respeito dos acontecimentos, com uma percepção do mundo com base nos nossos conhecimentos e vivências, o que varia de pessoa para pessoa.[218] Já a verdade absoluta coincide com os factos ocorridos na realidade, livre de qualquer viés imposto pela verdade humana, sendo esta um ideal a ser perseguido mas que nunca será alcançado.[219] Por fim, há a verdade material, também chamada de verdade processual que, segundo PAULO DÁ MESQUITA[220], é aquela que é considerada a verdade processualmente válida, distinta da realidade passada dos eventos do mundo exterior, obtida através de um processo

[216] Vide Artigo 18.º, n.º 2: "A lei só pode restringir os direitos, liberdades e garantias nos casos expressamente previstos na Constituição, devendo as restrições limitar-se ao necessário para salvaguardar outros direitos ou interesses constitucionalmente protegidos".
[217] MIRANDA, Jorge, *Manual de Direito Constitucional. Direitos Fundamentais*, Tomo IV, 5.ª edição, Coimbra, Coimbra Editora, 2012, p. 134.
[218] LOPES JR, Aury, O problema da "verdade" no Processo Penal em Verdade e Prova no Processo Penal *In Estudos em homenagem ao professor Michele Taruffo*, Editora Gazeta Jurídica, São Paulo, p. 79.
[219] Como bem ressalta Manuel Monteiro Guedes Valente "A verdade real não existe em um processo-crime. No mundo físico a verdade real esgota-se em cada milésimo de segundo e jamais pode ser reposta ou reedificada por meio de um processo reconstrutivo. *In* VALENTE, 2019, p. 19.
[220] DÁ MESQUITA, Paulo, *A prova do Crime e o que se disse antes do julgamento*. Coimbra, Coimbra Editora, 2011, p. 264.

dialético probatório, com respeito ao contraditório e aos direitos fundamentais[221].

Em razão disso, a busca pela verdade material ao longo do processo deverá respeitar regras e balizas impostas pela lei, respeitando acima de tudo, os direitos fundamentais do arguido, o que significa que não se poderá utilizar meios de obtenção de prova abusivos. Isto posto, nesta subsecção iremos realizar uma análise das consequências negativas da desencriptação coativa aos direitos fundamentais do arguido, iniciando-se pela dignidade da pessoa humana.

1.1 A dignidade da pessoa humana

A dignidade é um conceito que já utilizado na Roma Antiga[222], muito embora com outra conotação[223], porém foi apenas com o fim da Segunda Guerra Mundial[224] que o conceito de Estado Democrático de Direito, conforme o entendemos hoje, surgiu. Com isso, a dignidade da pessoa humana foi adotada nos termos e com a amplitude que a conhecemos e passou a constar em diversas Constituições, tanto explícita quanto implicitamente.[225]

É possível definir a dignidade da pessoa humana como um princípio e direito que existe apenas pelo facto de sermos humanos, o que significa que qualquer indivíduo tem dignidade e deve ser tratado como um fim em si mesmo e não como um objeto para atingir outros fins. ANA PAULA GUIMARÃES conceitua a dignidade como uma força espiritual galvanizadora dos demais princípios e normas constitucionais, sendo intrínseca ao homem que já nasce com ela, portanto não lhe é dada, cedida

[221] *Ibidem* VALENTE, 2019, p. 20.
[222] Cícero assinalava a diferença entre os seres humanos e os restantes seres, afirmando a superioridade do ser humano por ser portador de uma alma criada por Deus e da lei emergia a liberdade. *In* GUIMARÃES, 2016, p. 56.
[223] "Na roma antiga, da valoração positiva do atributo da dignitas decorria a necessidade de dar àquele a quem se reconhecia ou que tinha dignitas um tratamento privilegiado e distinto do que era conferido à generalidade dos indivíduos" *In* NOVAIS, Jorge Reis, *A dignidade da pessoa humana*, Coimbra, Editora Almedina, 2015, p. 34.
[224] Presente no preâmbulo da Carta das Nações Unidas, da Declaração Universal dos Direitos do Homem, da Constituição Francesa de 1946 e no artigo 1.º da Constituição Alemã de 1949.
[225] *Ibidem* NOVAIS, 2015, p. 09.

ou transmitida, faz parte do ser pessoa humana[226]. JORGE REIS NOVAIS, por sua vez, conceitua a dignidade da pessoa humana como um estatuto universal reconhecido a todas as pessoas pelo facto de o serem[227]. Por fim, JOSÉ CARLOS VIEIRA DE ANDRADE define o conceito de dignidade humana como a afirmação da ideia de uma dignidade-valor reconhecida a cada individuo pelo facto de ser pessoa.[228]

Nota-se portanto que a dignidade da pessoa humana, apesar de estar presente no ordenamento jurídico, prescinde de estar, em razão de seu peso como afirma JOSÉ AFONSO DA SILVA, ao dizer que a dignidade independe de criação constitucional, pois é um conceito *a priori*, que preexiste toda experiência vinculativa[229], por isso é possível afirmar que os ordenamentos não concedem dignidade, apenas a reconhecem como dado essencial daquele ordenamento jurídico[230] [231]

No ordenamento português, a Constituição de 1976 foi a primeira[232] que concedeu à dignidade o *status* de arcabouço principal da República, ao mesmo tempo que a estabeleceu como um limite aos poderes do Estado.[233] Esta foi uma verdadeira mudança de paradigma com relação às Constituições anteriores, tendo em vista que instituiu uma nova "ordem de valores",[234] em que o indivíduo foi posto em primeiro lugar, em primazia com relação ao Estado, que tem o dever de o respeitar acima de tudo.[235] A dignidade está consagrada no artigo 1.º da Constituição, apontando este princípio como o princípio fundamental da Constituição, o pilar sobre o qual se assenta a república como afirma JORGE REIS NOVAIS, que afeta

[226] *Ibidem* GUIMARÃES, 2016, p. 55-61.
[227] *Ibidem* NOVAIS, 2015, p. 37.
[228] DE ANDRADE, José Carlos Vieira, *Dos Direitos Fundamentais na Constituição Portuguesa de 1976*, 6ª Edição, Coimbra, Editora Almedina, 2019, p. 90.
[229] SILVA, José Afonso da, A dignidade da pessoa humana como valor supremo da democracia. *Revista de Direito Administrativo*, v. 212, abr./jun. 1998, p. 84-94.
[230] SARLET, Ingo Wolfgang. A dignidade da pessoa humana, *Revista de Direito Administrativo* n.º 212, 1998, pp. 84-94.
[231] "A Constituição portuguesa não reivindica para si as prerrogativas de *criador* dos direitos fundamentais, não concebe estes como meros produtos da sua vontade constituinte. Parece, pelo contrário, admitir, mais modestamente, que, no seu núcleo essencial, se limitou a *reconhecer* os direitos fundamentais, que existem para além do catálogo que formulou e que não estão sujeitos aos seus poderes de livre disposição." *In* DE ANDRADE, 2019, p. 44.
[232] MIRANDA, Jorge, *Escritos Vários sobre Direitos Fundamentais.* Estoril, Principia, 2006, p. 469.
[233] NOVAIS, Jorge Reis, *Os princípios Constitucionais Estruturantes da República Portuguesa,* 1ª Edição, Coimbra, Almedina, 2011, p. 51.
[234] Termo utilizado em NOVAIS, 2015, p. 72.
[235] *Ibidem* NOVAIS, 2015, p. 55.

todo o ordenamento – em especial o Direito Processual Penal[236] – e os poderes de Estado que ficam vinculados a respeitar, proteger e promover a dignidade da pessoa humana[237].

Em razão da sua característica fundante, a dignidade irá afetar o ordenamento jurídico de dois três modos diferentes, nomeadamente como fundamento de regras e princípios gerando novas normas[238] [239]– função normogenética dos princípios e normas[240] –, como critério de interpretação ou de integração[241] [242] [243], como é o caso de enunciados dúbios ou vagos[244] e outras vezes, como regra ou princípio, como defende ROBERT ALEXY[245]. O Tribunal Constitucional compartilha do mesmo entendimento ao ressaltar nos Acórdãos n.º 16/84[246] e n.º 43/86[247] a influência da dignidade da pessoa humana na proibição de penas de caráter difamante.

Como ressalta JORGE MIRANDA[248], a raiz de todos os direitos fundamentais reside na dignidade da pessoa humana, tendo em vista que sem considerarmos que todos os indivíduos devem ser respeitados em razão de serem humanos, não é possível considerar a existência de qualquer outro direito fundamental. Isto posto, direitos liberdades e garantias bem como os demais direitos sociais são fundados na dignidade da pessoa humana, além de atribuir a outros direitos o caráter de direito fundamental, como ressalta o Tribunal Constitucional no Acórdão n.º 6/84[249] ao considerar que o direito geral de personalidade pese embora

---

[236] "O sistema processual penal português tem um compromisso inalienável com a dignidade da pessoa humana por ser o fundamento último da Constituição e do princípio estruturante do Estado de direito democrático. Constitui o centro nevrálgico da matéria relativa aos direitos fundamentais que limita o poder" *In* GUIMARÃES, 2016, p. 56.
[237] *Ibidem* NOVAIS, 2015, p. 09-18.
[238] CANOTILHO, José Joaquim Gomes, *Direito Constitucional e Teoria da Constituição*, Coimbra, Editora Almedina, 4ª edição, 2000, p. 1125.
[239] *Ibidem* DE ANDRADE, 2019, p. 94.
[240] Função "normogenética" *In* CRORIE, Benedita Mac, O Recurso ao Princípio da Dignidade da Pessoa Humana na Jurisprudência do Tribunal Constitucional. Em Separata - *Estudos em Comemoração ao 10 Aniversário da Licenciatura em Direito da Universidade do Minho*. Coimbra, Almedina, 2003.
[241] ALEXANDRINO, José De Melo, *A Estruturação do Sistema de Direitos, Liberdades e Garantias na Constituição Portuguesa*, Volume II. Coimbra, Editora Almedina, 2006, p. 323-324.
[242] *Ibidem* CRORIE, 2003, p. 152.
[243] CANOTILHO, José Joaquim Gomes, *Direito Constitucional e Teoria da Constituição*, Coimbra, Editora Almedina, 4ª edição, 2000, p. 1137-1139.
[244] *Ibidem* MIRANDA, p. 227.
[245] ALEXY, Robert, *Teoria de los derechos fundamentales*, Centro de Estudios Constitutionales, Madrid, 1993, p. 106.
[246] Publicado no Diário da República 2ª série, de 12 de maio de 1984.
[247] Publicado no Diário da República 2ª série, n.º 111, de 15 de maio de 1986.
[248] *Ibidem* MIRANDA, p. 348.
[249] Publicado no Diário da República, 2ª série, de 2 de maio de 1984.

não expresso na Constituição está fundado na dignidade da pessoa humana.

Quando se trata do direito processual penal, o princípio da dignidade da pessoa humana toma contornos ainda mais importantes tendo em vista que como bem ressalta o Tribunal Constitucional no Acórdão n.º 1/2001, os fins das penas articulam-se com a dignidade da pessoa humana e com o princípio do Estado de direito,[250] a medida que, como bem ressalta BENEDITRA MAC CRORIE, visa garantir a defesa de bens jurídicos essenciais para que seja possível a vida em sociedade[251].

Além disso, a dignidade é fundamento de interpretação dos demais princípios normativos, criando um sistema unificado de direitos fundamentais[252] como ressalta o Tribunal Constitucional no Acórdão n.º 25/84[253] ao sustentar que a dignidade é princípio interpretativo e instrumento metódico de resolução de conflitos.

Neste ponto, após a análise do conceito e da influência da dignidade da pessoa humana é possível compreender que a desencriptação coativa de telemóveis é violadora da dignidade da pessoa humana, tanto como regra e princípio autônomo quanto como base dos demais direitos fundamentais do ordenamento jurídico, fundamentamos este posicionamento ao ponderarmos dois pontos.

No primeiro, ressaltamos que ao longo do processo penal ocorrerão atos e factos que não são do interesse e da vontade do arguido, aos quais este deverá se submeter mesmo contra a sua própria vontade. Um exemplo é a prisão preventiva, disposta no artigo 202 do Código de Processo Penal[254], que apesar de ser uma medida grave, é considerada aceitável em situações específicas e justificáveis.

---

250 Publicado no Diário da República n.º 33/2001, Série II de 2001-02-08, disponível em https://dre.pt/home/-/dre/1696349/details/maximized.
251 *Ibidem* CRORIE, 2003, p. 160.
252 *Ibidem* MIRANDA, 2013, p. 180.
253 Publicado no Diário da República, 2ª série, de 2 de maio de 1984.
254 A prisão preventiva está prevista na alíena b) do n.º 3 do artigo 27.º da Constituição que determina que a privação de liberdade deverá ser pelo tempo e nas condições que a lei determinar. E como bem ressaltam J.J Canotilho e Vital Moreira é uma medida excepcional, precária, fundamentada e temporalmente limitada. *In* CANOTILHO, José Joaquim Gomes, MOREIRA, Vital Martins, *Constituição da República Portuguesa Anotada*, Vol. I, Coimbra, Coimbra Editora, 2007, p. 488.

Contudo, devemos levar sempre em conta que no Processo Penal o ónus da prova reside na acusação,[255] que deverá provar que o arguido cometeu ou não o crime ao qual este é acusado. Desta forma não é aceitável exigir do arguido um auxílio na sua própria acusação e na busca pela verdade material. Vai neste sentido o posicionamento de FIGUEIREDO DIAS, que ressalta que o facto do arguido ser sujeito processual não exclui a possibilidade do mesmo ser um meio de prova, contudo aponta que o indivíduo tem uma posição jurídica que lhe permita participar no caso concreto[256].

Desta forma, é possível chegar a conclusão que o Estado não poderá, ao basear-se em um dever de cooperação do arguido, reduzi-lo à objeto de prova, submetendo-o a coações e determinações que violem a sua dignidade na busca por meios de prova para facilitar em uma acusação. Portanto, discordamos do posicionamento adotado por CANOTILHO e VITAL MOREIRA[257] que sustentam a existência de deveres públicos dos cidadãos que autorizem intervenções no corpo humano em caso de recusa na realização de exames. Compreendemos que tal entendimento é incompatível com um sistema jurídico que adota a dignidade da pessoa humana como base fundante do Estado e com um Processo Penal que é baseado no sistema acusatório[258].

Além disso, defendemos que a discussão acerca da gravidade da medida da desencriptação coativa de telemóveis – como a feita no caso da recolha de ADN pela zaragatoa bucal – não é cabível. Primeiramente porque a dignidade compreende a violação física e moral de um indivíduo, não sendo possível assim, mensurar a sua violação[259]. Além disso, entendemos que a dignidade não é um princípio ou direito passível de flexibilização,

---

[255] Como bem aponta Gil Moreira dos Santos "Em processo penal, não há ónus de alegação nem ónus de contraprova, relativamente ao arguido; e quanto a qualquer das "partes", só se pode falar em ónus de alegação até ao despacho de pronúncia. Isto o que resulta dos artigos 267.º, n.º1, 299.º, 340.º, n.º 1 e 2, 303.º, n.º 1 e 3 e 359.º do Código de Processo Penal" (...) "E relativamente ao Ministério Público, porque a averiguação da verdade material é, mais que um imperativo hipotético, um imperativo categórico, um dever – artigo 53.º, n.º 1 –, não se pode falar em ónus mas em encargo".. *In* DOS SANTOS, Gil Moreira, Princípios e Prática Processual Penal, Coimbra, Coimbra Editora, 2014, p. 208/209.

[256] FIGUEIREDO DIAS, Jorge de, *Direito Processual Penal*, Coimbra, Coimbra Editora, reimpressão, 2004, pp. 429-430.

[257] GOMES CANOTILHO, J.J., MOREIRA, Vital, *Constituição da República Portuguesa Anotada*, vol. I, 4ª ed. revista, Coimbra, Coimbra Editora, 2007, p. 456.

[258] Como bem aponta Gil Moreira dos Santos: "A estrutura acusatória pressupõe que os sujeitos formais do processo tenham papel constitutivo, nenhum deles figurando como mero objecto. *In* DOS SANTOS, 2014, p. 49.

[259] MIRANDA, Jorge, MEDEIROS, Rui, *Constituição Portuguesa Anotada*, Tomo I, Coimbra, Coimbra Editora, 2005, p. 268/269.

como defende JORGE REIS NOVAIS ao sustentar que a dignidade da pessoa humana é um *knock-down argument*, ou seja, um argumento-trunfo, que por si só basta para tornar um ato ilegal [260].

Desta forma, a dignidade é passível de ser violada como princípio autónomo, mas também como fundo principiológico de outros direitos fundamentais, que devemos a seguir.

1.2 A presunção de inocência

A presunção de inocência é um princípio e um direito fundamental que determina que o arguido será considerado inocente, até o trânsito em julgado da sentença penal condenatória. A palavra "presunção" vem do latim *praesumptio*, *onis*, cujo verbo é *praesumere*, que significa antecipar, prever, imaginar antes. Já o termo "inocência" vem do termo latino "*innocentia, ae"* significando pureza e ingenuidade, tendo um sentido religioso que significa isento de pecados[261].

Este direito teve surgimento no movimento Iluminista, após a passagem do modelo de processo inquisitório para o modelo acusatório[262], onde foi criada uma nova concepção de indivíduo no âmbito do processo penal, com respeito a liberdade do cidadão[263]. A criação deste princípio foi uma mudança de paradigma, tendo em vista que, com a sua adoção, o arguido não teria de provar a sua inocência – através de uma prova negativa, uma prova diabólica –, devendo antes a acusação provar a sua culpabilidade.[264]

[260] NOVAIS, 2015, p. 147.
[261] MORAES, Maurício Zanoide de, *Presunção de inocência no processo penal brasileiro: análise de sua estrutura normativa para a elaboração legislativa e para a sua decisão judicial*. Rio de Janeiro, Lumen Juris, 2010, p. 83-86.
[262] Cf., FIGUEIREDO DIAS, 1974, p. 41.
[263] *Ibidem* GUIMARÃES, 2016, p. 75.
[264] BARBAGALO, Fernando Brandini. *Presunção de inocência e recursos criminais excepcionais: em busca da racionalidade no sistema processual penal brasileiro*, Editora TJDFT, 2015, p. 39

No sistema jurídico português, a presunção de inocência está disposta no artigo 32.º, n.º 2 da Constituição[265]. FIGUEIREDO DIAS, ressalta que a presunção de inocência além de ser um princípio constitucional e do processo penal, é um princípio do Estado de Direito Democrático, que se estende a todo o estatuto do arguido, devendo ser levado em consideração aquando da determinação de medidas de coação, da recolha de prova e até mesmo na duração processo penal que não poderá ser eterno.[266] Para SOUTO MOURA, a presunção de inocência também tem repercussões extraprocessuais, pois até que o arguido seja considerado culpado de forma definitiva, deverá ter tratamento igualitário aos demais cidadãos.[267] A presunção de inocência também é dirigida ao legislador, tendo em vista que este não poderá consagrar presunções de culpa na lei, como muito bem aponta HELENA MAGALHÃES BOLINA[268].

Desta forma, a presunção de inocência tem alcance multidimensional, pois não é considerado apenas um princípio, mas também uma regra interpretativa de valoração de prova e critério que impõe limite do poder legislativo na formulação de normas.[269] Ela irá operar em todo o processo[270], até o trânsito em julgado da sentença condenatória e influenciará o processo através das suas ramificações, como por exemplo, o *in dubio pro reo*[271], que influencia diretamente a matéria probatória[272].

Tamanha é sua importância, que a presunção de inocência está presente em diversos documentos internacionais de direitos humanos, como por exemplo, no artigo 9.º da Declaração dos Direitos do Homem e

---

265 "Todo o arguido se presume inocente até ao trânsito em julgado da sentença de condenação, devendo ser julgado no mais curto prazo compatível com as garantias de defesa".
266 DIAS, Jorge Figueiredo, *Direito Processual Penal*. Coimbra, Coimbra Editora, 1974, p. 213
267 MOURA, José Souto de "A *Questão da Presunção de Inocência do Arguido*". RMP. Lisboa, Sindicato dos Magistrados do Ministério Público, Ano 11, no 42, pp. 31-47.
268 BOLINA, Helena Magalhães, Razão de ser, significado e consequências do princípio da presunção de inocência (art. 32.º, n.º 2 da CRP), *Boletim da Faculdade de Direito de Coimbra*, Vol. IXX (Separata), Estudos nos Cursos de Mestrado, 1994, p. 453
269 *Ibidem* GUIMARÃES, 2016, p. 80.
270 "Do princípio da presunção de inocência decorre, por exemplo, que as fases processuais anteriores ao julgamento não possam prolongar-se além do que já não possa ser razoavelmente considerado compatível com a presunção de inocência do arguido, num exercício de ponderação das finalidades que são apontadas ao processo penal de um Estado de direito democrático". Em ANTUNES, Maria João, Direito Processual Penal, Coimbra, Editora Almedina, 2016, p. 41.
271 O *in dúbio pro reo* é um princípio específico relativo a prova que cria uma regra interpretativa das provas, ligado à presunção de inocência na sua dimensão de valoração de prova. Vide MARQUES DA SILVA, Germano, Curso de Processo Penal, Vol. II, Lisboa, Editora Verbo, 4.ª edição, 2008, p. 126.
272 *Ibidem* BOLINA, 1994, p. 433-461.

do Cidadão de 1789[273], no artigo 14.º do Pacto Internacional sobre Direitos Civis e Políticos[274], no artigo 6.º da Convenção Europeia de Direitos do Homem[275], e no artigo 48.º da Carta dos Direitos Fundamentais da União Europeia[276].

A presença da presunção de inocência tanto na Constituição quanto em diplomas internacionais de direitos humanos aponta como o processo penal deve ser compreendido e interpretado dentro de uma perspectiva constitucional e humanitária como ressalta JORGE DE FIGUEIREDO DIAS[277].

Ressaltamos contudo, que ela não impedirá que algumas medidas de coação sejam aplicadas ao longo do processo, como ressalta JORGE FIGUEIREDO DIAS ao apontar que o estado de inocência não é absoluto, admitindo restrições em favor de outros valores assegurados constitucionalmente[278]. Porém, até as restrições à presunção de inocência não permitem violações, devendo sempre respeitar a proporcionalidade e o devido processo legal, como bem aponta GERALDO PRADO, ao sustentar que um Processo Penal efetivo exige o respeito aos direitos fundamentais e à capacidade de punir em atenção ao devido processo penal, e um Estado que pretende legitimar a punição daqueles que violam a lei, não pode, para punir, violar seus próprios comandos legais[279].

Com estas ressalvas, defendemos que a desencriptação coativa de telemóveis viola a presunção de inocência, pois funda-se no pressuposto que para a acusação ser bem sucedida é necessário que o arguido colabore submetendo-se à coações e agindo contra a sua vontade o que vai no sentido oposto da lógica do Processo Penal. O que vai no sentido oposto

---

273 "Todo o acusado se presume inocente até ser declarado culpado e, se se julgar indispensável prendê-lo, todo o rigor não necessário à guarda da sua pessoa, deverá ser severamente reprimido pela Lei".
274 "Qualquer pessoa acusada de um delito tem direito a que se presuma a sua inocência até que se prove a sua culpa conforme a lei".
275 "Qualquer pessoa acusada de uma infração presume-se inocente enquanto a sua culpabilidade não tiver sido legalmente provada".
276 "Todo o arguido se presume inocente enquanto não tiver sido legalmente provada a sua culpa."
277 FIGUEIREDO DIAS, Jorge de, *Direito Processual Penal*, 1ª edição reimpressão, Coimbra, Coimbra Editora, 2004, p. 74 e ss.
278 "A via para um correto equacionamento da evolução do processo penal nos quadros do Estado de Direito material deve, em meu entender, partir do reconhecimento e aceitação da tensão dialética ente tutela dos interesses do arguido e tutela dos interesses da sociedade representados pelo poder democrático do Estado (...)" em DIAS, Jorge de Figueiredo, Para uma nova justiça penal, Coimbra, Editora Almedina, 1996, p. 206.
279 PRADO, Geraldo; CASARA, Rubens R. R. Eficientismo Repressivo e Garantismo Penal: dois exemplos de ingenuidade na seara epistemológica. *In* BATISTA, Vera Malaguti (coord.). *Discursos Sediciosos*: *crime, direito e sociedade.* Rio de Janeiro: Editora Revan, p. 67-74, ano 17, n. 19/20, p. 1o e 2o semestres de 2012, p. 71.

do que aponta GIUSEPPE DI CHIARA e outros ao afirmarem que não cabe ao imputado provar a sua inocência, mas antes a acusação provar a sua culpabilidade[280].

Ressaltamos ainda que não encontramos compatibilidade entre ambos os institutos, tendo em vista a violência empregada pela desencriptação na esfera dos direitos do arguido. Por isso, sustentamos que a busca pela verdade só é possível e aceitável com um desenvolvimento regular do processo e de todos os procedimentos que fazem parte dele, sempre respeitando os direitos fundamentais do arguido. Vai neste sentido o entendimento do Tribunal Constitucional que aponta a presunção de inocência como princípio fundamental da plenitude das garantias de defesa proibindo a inversão do ónus da prova em detrimento do arguido[281].

Neste contexto, também podemos observar repercussões em outros direitos que são considerados ramificações da presunção de inocência, como por exemplo, a igualdade de armas.

1.3 A igualdade de armas

A igualdade de armas pode ser conceituada como o equilíbrio entre as partes ao longo do processo, assegurando que as partes terão as mesmas possibilidades para fazer valer suas posições processuais perante o tribunal como bem aponta FIGUEIREDO DIAS[282]. Segundo o Supremo Tribunal de Justiça, a igualdade de armas determina que cada uma das partes processuais, quais sejam o arguido e a acusação, possa sustentar a sua posição de modo que não coloque a outra parte em desvantagem, portanto, segundo o entendimento do Tribunal, haverá desigualdade

[280] SIRACUSANO, Fabrizio, GALATI, Antonino, TRANCHINA, Giovanni, ZAPPALA, Vicenzo, DI CHIARA, Giuseppe, *Diritto Processuale Penale*, volume primo, Giuffrè Editore, 2004, p. 173 ss.
[281] Acórdão Tribunal Constitucional n.º 155/2007, 3ª secção, disponível em https://www.tribunalconstitucional.pt/tc/acordaos/20070155.htm.
[282] *Ibidem* FIGUEIREDO DIAS, 1974, p. 274.

processual toda vez que uma das partes tenha uma desvantagem processual em detrimento da outra[283].

No ordenamento jurídico português, a igualdade de armas está disposta no artigo 20.º da Constituição, contudo é densificado através de diversas normas em outros âmbitos do direito, como no direito administrativo, direito civil e direito penal. No processo penal, ela pode ser vista de diversas formas, como na exigência de um juízo imparcial – na existência de sistema de sorteios, no padrão ético dos magistrados, no dever de fundamentar – e na organização processual – nos prazos processuais, direito das partes.

O Processo Penal português pode ser considerado um processo acusatório misto[284], que ainda conserva alguns pontos do processo inquisitório, nomeadamente na fase preliminar ou pré-acusatória[285] [286]. Em razão disso, GERMANO MARQUES DA SILVA sustenta que a igualdade de armas só vigora nas fases jurisdicionais do processo e em especial da fase de julgamento, tendo em vista que na fase pré- acusatória a entidade competente para realizar as investigações dispõe de poderes que o arguido ou suspeito não tem[287], como também afirma LOPES DO REGO, a igualdade de armas não dá estatutos idênticos às partes processuais, mas garante que o arguido não tenha menos direitos que a acusação[288].

Isto posto, afirmamos que vemos a prática da desencriptação coativa de telemóveis como uma ofensa à paridade de armas tendo em vista que vai além de uma desigualdade formal das partes devido à organização do

---

283 Acórdão do Supremo Tribunal de Justiça n.º 251/15.3GDCTX.L2.S1 disponível em shorturl.at/hstN7.

284 "Este sistema fundeia-se na relação dialética decorrente da necessidade sentida pela comunidade de perseguir os culpados pelos crimes cometidos - incumbindo ao Estado a tarefa pública de exercer o seu *ius puniendi* - mas, em cada caso concreto, assegura-se ao arguido a possibilidade de exercer os seus direitos de defesa, evitando-se os perigos decorrentes de uma real aniquilação da condição humana (do arguido) em prol da busca, levada ao extremo no sistema inquisitório, da descoberta da verdade material" Em NEVES, Rosa Vieira, *A Livre Apreciação da Prova e a Obrigação de Fundamentação da Convicção (na Decisão Final Penal)*, Coimbra, Coimbra Editora, 2011, p. 58-65.

285 SILVA, Germano Marques, *Do Processo Penal Preliminar*, Editorial Minerva, 1990, p. 72.

286 "Tendo em vista que o Tribunal poderá, caso entenda ser necessário, ordenar oficiosamente todos os meios de prova cujo conhecimento lhe afigure necessário à descoberta da verdade e à boa decisão da causa". (...) "Não há paridade entre o MP e o arguido dado que durante a fase preliminar do processo, o MP tem ao seu dispor meios humanos (os órgãos de polícia criminal) e meios técnicos e tecnológicos para investigar que o arguido não tem". *In* RIBEIRO, Maria da Conceição Fernandes, Dissertação de mestrado apresentada para a obtenção do grau de Mestre em Ciências Jurídico-Forenses sob a orientação da Professora Doutora Cristiane Reis e da Co-Orientadora Mestre Sara Moreira no Instituto Superior Bissaya Barreto em 2015, p. 41.

287 *Ibidem* SILVA, 1990, p. 69.

288 LOPES DO REGO, Carlos, Acesso ao direito e aos tribunais, *Estudos sobre a jurisprudência do Tribunal Constitucional*, Aequitas/Editorial de Notícias, 1993, p. 76-70.

processo, ela submete o arguido a uma verdade obtida a todo o preço[289], que não deve confundir-se com dever de cooperação, tendo em vista que coloca o arguido em uma posição de inferioridade com relação à acusação, como subserviente de submeter-se à diligências as quais se recusou a cumprir e como objeto em busca de uma verdade material.

Por fim, defendemos que cabe ao Ministério Público elaborar uma acusação sólida e robusta que não dependa de violações de direitos fundamentais do arguido. Por isso, neste contexto, compreendemos ser o momento propício deste estudo para tratarmos a respeito de um dos direitos que consideramos essenciais no Direito Processual Penal, o direito à não autoincriminação.

1.4 O direito à não autoincriminação

Também refletido na fórmula latina *nemo tenetur se ipsum accusare*[290] ou *nemo tenetur se ipsum detegere,*[291] o direito à não autoincriminação, pese embora seja comumente referido como direito ao silêncio[292] [293], é um direito complexo que compreende a liberdade de não confessar, testemunhar e não declarar culpabilidade contra si próprio[294]. Este direito tem diversas ramificações[295], que podem ser considerados círculos independentes que se intersectam em alguns pontos[296] [297].

[289] FIGUEIREDO DIAS, 1974, p. 43.
[290] Traduz-se "Ninguém é obrigado a acusar-se".
[291] Traduz-se "Ninguém é obrigado a manifestar-se".
[292] Como bem refere Ana Paula Guimarães, o silêncio é apenas um dos modos possíveis do exercício do direito de defesa do arguido e é um evidente obstáculo à procura indistinta e incessante dos factos que se pretende apurar no âmbito da investigação. *In* GUIMARÃES, 2016, p. 127.
[293] Vânia Costa Ramos aponta que continua a fazer-se uso da expressão direito ao silêncio em homenagem ao seu aparecimento e evolução históricas. In RAMOS, Vânia Costa, Corpus Iuris 2000 – Imposição ao arguido de entrega de documentos para prova e *nemo tenetur se ipsum accusare*" (Parte I), *Revista do Ministério Público*, n.º 108, Out-Dez-, 2006, pp. 132-133.
[294] *Ibidem* GUIMARÃES, 2016, p. 127.
[295] Como o direito ao silêncio corporal dentre outros *In* BRAVO, Jorge Dos Reis - Tetis Contra Se - A possibilidade de um Direito ao Silêncio Corporal. *Revista do CEJ, 2018 - I*. Lisboa. 2018, pp. 151–194.
[296] *"One might be tempted by rather loose terminology into assuming that the right to silence and the privilege against self-incrimination are one and the same thing. However, the two guarantees must be seen as being represented by two partly overlapping circles".* Em TRECHSEL, Stefan - *Human Rights in Criminal Proceedings*. Oxford, Oxford University Press, 2005, p. 342.
[297] Para os fins deste trabalho, usaremos a terminologia do direito à não autoincriminação, tendo em vista que este conceito é o mais aplicável ao tema discutido.

O direito à não autoincriminação nem sempre foi a regra no direito processual penal. Durante séculos o sistema processual inquisitório vigorou na Europa, tendo como principal característica o tratamento do indivíduo como um objeto do processo, o que fazia com que o Estado se utilizasse de toda a sua força, muitas vezes utilizando métodos de tortura em busca de uma confissão[298].

Foi apenas com a influência dos ideais do Iluminismo que diversas práticas medievais foram abandonadas, de entre elas a legitimação da tortura na obtenção das confissões[299]. Em consequência disso, houve uma profunda modificação no sistema processual, com a mudança do sistema inquisitório para o sistema acusatório, com a reformulação do modelo de julgamento e a introdução da defesa técnica por advogados, o que possibilitou ao acusado ser defendido ao mesmo tempo que mantinha o silêncio[300].

Assim, o *nemo tenetur* foi um resultado da mudança da conceção de indivíduo perante o poder Estatal, que passou a ser considerado uma parte processual com direitos que devem ser respeitados e não apenas um objeto utilizado na obtenção da verdade material. Contudo, a maior influência no tema foi o direito norte americano, que inseriu o "*privilege against self-incrimination"* na V Emenda à Constituição norte americana e influenciou constituições no mundo todo[301] [302].

No ordenamento jurídico português, o direito ao silêncio apareceu pela primeira vez no Decreto de 28 de dezembro de 1910, no qual se estabeleceu que o réu não poderia ser obrigado a responder em audiência de julgamento, exceto a respeito da sua própria identidade.[303] Atualmente,

---

[298] RIBEIRO, Telma Sofia Martins, *A "intercomunicabilidade probatória" entre o procedimento de inspeção tributária e o processo penal*. Dissertação do Mestrado em Direito Judiciário, Escola de Direito, Universidade do Minho. Braga, 2017 p. 27-28.

[299] Vide o artigo 9.º da Declaração dos Direitos do Homem e do Cidadão.

[300] OLIVEIRA E SILVA, Sandra, *O Arguido como meio de prova contra si mesmo: Considerações em torno do princípio nemo tenetur se ipsum accusare*. Coimbra, Editora Almedina, 2019, p. 101.

[301] *"No person (...) nor shall be compelled in any criminal case to be a witness against himself (...)".*

[302] Também dos Estados Unidos da América vem o conhecido caso *Miranda vs. Estado do Arizona* julgado em 1966, no qual Ernesto Miranda foi preso por um crime de roubo em razão do qual foi preso. Nas instalações da autoridade policial, Miranda assinou uma declaração de confissão de um crime de violação, que foi determinante para a sua condenação. Este alegou que desconhecia ter direito a ser assistido por advogado e de permanecer em silêncio. O Tribunal pronunciou-se no sentido de que não há processo equitativo se o arguido não for devidamente informado dos direitos que lhe assistem. Tal decisão criou o "Miranda Rights" uma declaração de leitura obrigatória no momento da realização de uma prisão. *In* MESQUITA, Paulo Dá, 2011, p. 224.

[303] *Ibidem* RIBEIRO, 2017 p. 31

está previsto no art. 32.º da Constituição e nos arts. 61.º, n.º 1, al. c), 343.º, n.º 1, e 345.º, n.º 1, do CPP [304], além de estar reconhecido e declarado pela jurisprudência[305].

Com relação ao fundamento do direito à não autoincriminação há uma divergência na doutrina portuguesa nomeadamente: a corrente substantivista e a corrente processualista. A substantivista, considerada uma opinião minoritária, inspirada na corrente substantiva alemã,[306] aponta a estreita ligação do *nemo tenetur* com os direitos fundamentais[307]. Já segunda corrente, maioritária, liga o direito à um fundamento processual, assinalando o direito de defesa, processo equitativo e presunção de inocência[308].

Ambos os posicionamentos têm razão de ser, a ligação do direito ao silêncio à dignidade da pessoa humana cria um escudo e previne que o individuo torne-se um objeto durante o processo, o que ocorria com frequência no processo inquisitório, conforme ressaltado. Por outro lado, também é possível traçar tranquilamente uma ligação entre a não autoincriminação e os princípios o direito a defesa, processo equitativo, também previamente abordados neste estudo. Esses princípios formam um arcabouço de garantias que protegem o arguido.

Como bem ressaltou LARA SOFIA PINTO, a escolha entre uma ou outra corrente tem consequências diretas na possibilidade ou não de introduzir restrições ao referido princípio, havendo mais espaço para flexibilização caso seja de natureza processual do que constitucional[309]. Exatamente por esta razão nos posicionamos a favor da primeira corrente, justamente por compreendemos que ao ligamos o direito à não autoincriminação ao principio da dignidade da pessoa humana e a demais

---

304 Vide Diretiva (EU) 2016/343 do Parlamento Europeu e Conselho de 9 de março de 2016, disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016L0343

305 "O princípio *nemo tenetur se ipsum* accusare, não se encontrando expressa e diretamente consagrado no texto constitucional, constitui um corolário da tutela de valores ou direitos fundamentais com directa consagração constitucional, que a doutrina vem referindo como correspondendo à dignidade humana, à liberdade de ação e à presunção de inocência". Vide Acórdão do Tribunal Constitucional n.º 418/2013, relativo ao Processo n.º 120/2011, de 15/07/2013 disponível em http://www.tribunalconstitucional.pt/tc/acordaos/20130418.html

306 Vide a decisão sobre a insolvência do Tribunal Constitucional Alemão de 1981, na qual o Tribunal afirmou que o direito ao silêncio é uma manifestação inequívoca da proteção à dignidade da pessoa humana. *In* OLIVEIRA E SILVA, 2019, p. 149

307 Posicionamento também adotado pelo Tribunal de Justiça da União Europeia no caso *Orkem v. Comissão* de 18 de outubro de 1989.

308 RIBEIRO, 2017 p. 42-43

309 *Ibidem,* PINTO, 2010, p. 23

direitos fundamentais, que são cláusulas inegociáveis de um estado de direito democrático, constatamos que o *nemo tenetur* não é apenas[310] uma garantia processual, e sim uma garantia básica de fundo constitucional, o que dá muito mais força e peso ao conceito, dificultando a sua ponderação para outros fins, como a desencriptação coativa de telemóveis.

Ao mesmo tempo compreendemos que nenhum direito fundamental é absoluto, todos até mesmo a vida, são passíveis de ponderação a depender da situação em questão. O próprio Tribunal Constitucional já se manifestou no Acórdão n.º 254/99[311] a respeito do tema ao apontar que a Constituição autoriza, tendo em vista a prossecução das finalidades próprias do processo penal, a restrição dos direitos fundamentais à integridade pessoal, à liberdade geral de atuação, à reserva da vida privada ou à autodeterminação informacional.

Neste contexto, devemos apontar o artigo 61.º do Código de Processo Penal, que densifica de modo claro tais restrições ao determinar que o arguido deverá cumprir uma série de ações como, comparecer ao tribunal e não afastar-se da sala da audiência, responder com verdade às questões relativas à sua identidade civil e especialmente, o dever de sujeitar-se a diligências de prova, medidas de coação e de garantia patrimonial na estrita medida que estas sejam necessárias.

Ao mesmo tempo, PAULO PINTO ALBUQUERQUE[312] afirma que o arguido não tem o dever de colaboração com o tribunal e com o Ministério Público na busca pela verdade material em razão do direito à não autoincriminação. A respeito do tema, o autor cita a decisão do caso *Kelly v. Jamaica*[313] para sustentar que a acusação deverá se abster de qualquer pressão direta ou indireta, física ou psicológica sob o arguido.

Diante dos argumentos apresentados, defendemos que muito embora a doutrina seja firme no entendimento de que o arguido tem

---

310 Ressaltamos que compreendemos a importância das normas processuais, pese embora defendamos a compreensão do Direito Processual Penal como Direito Constitucional aplicado.

311 Acórdão n.º 254/99 do Tribunal Constitucional, Processo n.º 456/97, Disponível em shorturl.at/doyE0

312 ALBUQUERQUE, Paulo Sérgio Pinto de, *Comentário do Código de Processo Penal: à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem*, 4ª ed. Lisboa, Universidade Católica Editora, 2011, p. 56

313 *Kelly v Jamaica*, Merits, Communication No 253/1987, UN Doc CCPR/C/41/D/253/1987, IHRL 2403 (UNHRC 1991), 8th April 1991, United Nations [UN]; Human Rights Committee [CCPR]

deveres a cumprir no âmbito do processo, a desencriptação coativa não está dentre deles. Sustentamos que a desencriptação fere de forma profunda o direito a não autoincriminação, tendo em vista que a ideia fundante da medida surge do facto de que o arguido é *coagido* a desencriptar o aparelho telemóvel quando o mesmo expressou previamente a recusa de fazê-lo.

Compreendemos portanto, que uma vez que o arguido expressou a recusa em cooperar com a acusação na realização de qualquer medida requisitada por esta que possa ferir a sua autoincriminação, este não poderá ser coagido a realizá-la. ADRIANA DIAS PAES RISTORI[314] segue o mesmo entendimento, ao afirmar que a coação constitui um ataque a liberdade do individuo, ocasionando na perda da do domínio, fazendo que as suas ações e declarações não sejam fruto da sua livre determinação.

Podemos ir além e realizarmos uma breve análise do ato de desencriptação do telemóvel. O método de criptografia do telemóvel poderá ser feita de diversas formas, por exemplo, reconhecimento facial ou leitura de digital e palavras-passe. Neste contexto, a depender do método adotado haverá ou não uma conduta ativa do arguido, no caso da palavra-passe, o arguido terá de escrevê-la, inseri-la ou dita-la. No caso da leitura de digital, deverá inserir o dedo no leitor ou deverá aceitar que o façam.

Neste ponto, é possível perceber que o arguido terá que ir além de *suportar* alguma ação infringida sob o seu corpo, e como WOLFSLAST[315] ressalta *"não se é apenas instrumento da própria condenação quando se colabora mediante uma conduta ativa, querida e livre, mas também quando contra a vontade, uma pessoa tem de tolerar que o próprio corpo seja utilizado como meio de prova"*[316]. Desta forma, compreendemos que esta ação ultrapassa o tolerável para as medidas coativas aplicáveis na atividade probatória, não sendo aceitável e nem tolerável.

[314] RISTORI, Adriana Dias Paes, Sobre o silêncio do arguido no interrogatório no processo penal português, Editora Almedina, Coimbra, 2007, p. 140.
[315] Inclusive, o autor destoa da doutrina alemã tradicional ao compreender que a colaboração tanto ativa quanto passiva tem potencial violador da dignidade do arguido. Vide PINTO, 2010, p. 20.
[316] WOLFLAST, G, Beweisführung durch heimliche Tonbandayfzeichnung, NStZ 1987, p. 103 ss.

Ressaltamos que não poderemos esquecer as finalidades do processo penal que são a realização da justiça, a descoberta da verdade, o restabelecimento da paz jurídica em conjunto com a defesa e a garantia dos direitos fundamentais[317]. Portanto, o arguido deverá sujeitar-se ao processo, participar dele tendo seus direitos respeitados, e eventualmente, após respeitado o devido processo legal e seus direitos fundamentais, curvar-se à sentença penal condenatória transitada em julgado, porém em nenhum destes pontos deverá haver desrespeito de direitos fundamentais do arguido.

1.5 Direito à privacidade

Por fim, mas não menos importante, apontamos a possível violação do direito à privacidade do arguido. Muito embora o conceito de privacidade exista desde a Grécia antiga, foi com o surgimento do Iluminismo que ela passou a ser conexa com o conceito de personalidade e com a liberdade do indivíduo de ter um espaço próprio onde possa desenvolver a própria personalidade.[318] Esta conexão influenciou a criação do direito à privacidade, sendo a razão pela qual este é um dos direitos que compõem os direitos de personalidade e uma das expressões do valor da dignidade humana[319].

No direito norte-americano, tido como percursor no tema, a privacidade como um direito ganhou novos contornos com um artigo escrito pelos advogados Samuel Warren e Louis Brandeis[320], entitulado *"The Right to Privacy",* em 1890.[321] Neste artigo, os autores se inspiraram no valor da privacidade trazido à América do Norte pelos peregrinos ingleses[322] e defenderam a necessidade de proteção da esfera privada dos

317 VALENTE, Manuel Monteiro Guedes, *Cadeia de Custódia da Prova*, Coimbra, Editora Almedina, 2019, p. 21
318 FUSTER, Gloria González - *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Editora Springer, 2014, p. 23
319 DRUMMOND, Victor, *Internet, Privacidade e Dados Pessoais*. Rio de Janeiro: Lumen Iuris, 2003, p. 16
320 CORREIA, Victor, *Sobre a Privacidade.* Lisboa: Sinapis Editores, 2014, p. 64.
321 WARREN, Samuel D, BRANDEIS, Louis D, *The Right to Privacy,* Harvard Law Review, Vol. 4, Nº 5, Dez. 1890 pp.193-220.
322 PINHEIRO, Alexandre Sousa, *Privacy e Protecção de Dados Pessoais: A Construção Dogmática do Direito à Identidade Informacional*. Lisboa: AAFDL, 2015, p. 273.

indivíduos de agressões externas, como da imprensa.[323] [324] Para isso, criaram um conceito até hoje utilizado chamado de *"right to be alone"*, livremente traduzido como o "direito de não ser incomodado".[325]

Internacionalmente, o direito à privacidade é previsto em diversos instrumentos como a Declaração Universal de Direitos Humanos,[326] o Pacto Internacional sobre Direitos Civis e Políticos,[327] a Convenção Europeia dos Direitos do Homem,[328] a Carta dos Direitos Fundamentais da União Europeia,[329] a Convenção Americana de Direitos Humanos,[330] a Convenção das Nações Unidas sobre os Direitos da Criança[331] e, por fim, a Convenção Internacional de Proteção dos Direitos de todos os Trabalhadores Migrantes e dos Membros das suas Famílias.[332]

No direito português, o direito à privacidade está disposto nos artigos 26.º, n.os 1 e 2, 34.º e 35.º da CRP, além de outros pontos do ordenamento jurídico. O direito à reserva da intimidade da vida privada e familiar tem a proteção mais ampla concedida pela Constituição, em razão de fazer parte do rol de direitos, liberdades e garantias. Na jurisprudência, o Tribunal Constitucional português foi pioneiro ao equiparar o direito à privacidade ao *privacy* americano e, posteriormente, criar a ramificação decisional da privacidade, amplificando o conceito para abarcar o direito

323 *Ibidem* PINHEIRO, 2015, p. 286.
324 Cumpre informar que no artigo original, Warren e Brandeis visam a proteção do indivíduo de agressões de particulares, desta forma, não abrangem a proteção do indivíduo de agressões do Estado.
325 *Ibidem* PINHEIRO, 2015, p. 294.
326 Artigo 12.ºNinguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a protecção da lei.
327 Artigo 17º Ninguém será objeto de ingerências arbitrárias ou ilegais na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem de ataques ilegais à sua honra e reputaçãoo. Toda a pessoa tem direito a proteção da lei contra essas ingerêcias ou esses ataques.
328 ARTIGO 8° 1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência. 2. Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem-estar económico do país, a defesa da ordem e a prevenção das infrações penais, a proteção da saúde ou da moral, ou a proteção dos direitos e das liberdades de terceiros.
329 Artigo 7º Todas as pessoas têm direito ao respeito pela sua vida privada e familiar, pelo seu domicilio e pelas suas comunicações.
330 Artigo 11º 2. Ninguém pode ser objeto de ingerências arbitrárias ou abusivas em sua vida privada, na de sua família, e m seu domicílio ou em sua correspondência, nem de ofensas ilegais à sua honra ou reputação. 3. Toda pessoa tem direito à proteção da lei contra tais ingerências ou tais ofensas.
331 Artigo 16º 1. Nenhuma criança pode ser sujeita a intromissões arbitrárias ou ilegais na sua vida privada, na sua família, no seu domicilio ou correspondência, nem a ofensas ilegais à sua honra e reputação. 2. A criança tem direito à proteção da lei contra tais intromissões ou ofensas.
332 Artigo 14º Nenhum trabalhador migrante ou membro da sua família será sujeito a intromissões arbitrarias ou ilegais na sua vida privada, na sua família, no seu domicilio, na sua correspondência ou outras comunicações, nem a ofensas ilegais à sua honra e reputação. Os trabalhadores migrantes e membros da sua família têm direito à proteção da lei contra tais intromissões ou ofensas.

de o indivíduo regular a esfera da intimidade, tendo em vista o caráter íntimo e privado de certas informações[333] [334] [335].

Como já foi possível observar, o presente estudo está centrado na questão da necessidade e da possibilidade da desencriptação coativa de telemóveis, por isso, compreendemos ser importante ressaltar a importância deste aparelho na vida dos indivíduos.

Atualmente, os aparelhos eletrónicos e a internet tornaram-se parte essencial da vida dos indivíduos. Chegamos ao ponto de que caso um individuo opte por evitar tais tecnologias ele estará de certo modo ilhado em um mundo que já não é mais completo, diante da exigência de integração das tecnologias.

Além da importância no contexto da sociedade, os aparelhos telemóveis também têm uma grande relevância na esfera individual, proporcionando uma série de ferramentas facilitadoras do dia a dia, temos à distância de um toque, ter uma agenda, serviço de correio eletrónico, câmara fotográfica, telefone e acesso à internet. Todas estas ferramentas geram e armazenam dados informáticos que são armazenados nestes aparelhos.

Quando os dados informáticos podem ser objeto de interesse por parte de investigações no âmbito do direito processual penal, temos que levar em conta que muitas vezes, ousamos dizer na maioria delas, estes dados estão armazenados juntamente com dados de uso pessoal do arguido. Isto porque, são poucas as situações que o indivíduo utiliza o aparelho telemóvel única e exclusivamente para o cometimento de delitos, na maioria das vezes o indivíduo irá utilizar o aparelho telemóvel para o

---

333 TEIXEIRA, Maria Leonor - Proteção de dados e big data - Os desafios líquidos do pós-panoptismo. *Revista do Ministério Público n. 159*, Lisboa, 2019, pp. 197-245

334 PALMA, Maria Fernanda, Tutela da Vida Privada e Processo Penal: Realidades e Perspetivas Constitucionais em *VIII Conferencia Trilateral – A proteção da vida privada na jurisprudência do Tribunal Constitucional*, 2-3 de outubro 2006, Lisboa. 2006, p. 09

335 "No Acórdão nº 128/92 (publicado no Diário da República II Série, de 24 de Julho de 1992), considerou-se estar em causa "o direito de cada um ver protegido o espaço interior ou familiar da pessoa ou do seu lar contra intromissões alheias. É a privacy do direito anglo-saxónico. (...) Neste âmbito privado ou de intimidade está englobada a vida pessoal, a vida familiar, a relação com outras esferas de privacidade (v.g. a amizade), o lugar próprio da vida pessoal e familiar (o lar ou o domicílio), e bem assim os meios de expressão e comunicação privados (a correspondência, o telefone, as conversas orais, etc.). em Acórdão Tribunal Constitucional nº 607/2003 Processo nº 594/03 2ª Secção Conselheiro Benjamin Rodrigues.

uso pessoal e cotidiano, e poderá eventualmente, utilizá-lo como auxílio ou no cometimento de crimes.

Em razão disso, quando a desencriptação coativa de telemóveis é aplicada, há também um grande risco de violação do direito a privacidade, tendo em vista este *nó* de dados informáticos de diversas naturezas e propósitos armazenados nos telemóveis. Aqui cumpre realizarmos neste ponto um paralelo com as interceptações telefónicas, No caso das interceptações telefónicas, há um recorte temporal e específico de conversas que possam ser de interesse da investigação, diferentemente da pesquisa e recolha de dados informáticos, tendo em vista que neste ponto não é possível realizar um recorte temporal de dados, sendo possível realizar um recorte apenas funcional, voltado a uma aplicação ou função específica.

Em conclusão, compreendemos que pese embora a importância dos dados informáticos no contexto atual, é papel das normas jurídicas e do interprete do Direito, manejar a relação estatal com o individuo, visando a proteção da dignidade humana, da liberdade, da igualdade, da segurança. Sem considerá-los direitos estanques e rígidos, mas também sem flexibilizá-los a ponto de permitir a sua ruptura. Entendemos que a desencriptação coativa de telemóveis, seja resultado da interpretação analógica ou de uma norma permissiva, tem potencial violador de direitos que repercutem também no andamento processual, como veremos na seguinte secção.

2. Consequências jurídico processuais

Uma vez apresentadas as consequências jurídicas aos direitos fundamentais do arguido nesta secção iremos abordar as consequências

jurídico processuais da desencriptação coativa, que por muitas vezes, também estão ligadas às consequências aos direitos fundamentais já mencionadas.

Terminamos a secção anterior ao tratar a respeito da violação do direito à privacidade e por este motivo, iremos abordar uma consequência jurídico processual diretamente ligada a este direito, que tem o teoria das três esferas concêntricas.

A Teoria das Três Esferas Concêntricas foi criada na Alemanha por Hubmann[336] e posteriormente desenvolvida por Henkel. Esta teoria propõe dividir a privacidade humana em círculos concêntricos, menores e maiores, formando três esferas – chamadas *Offentlichkeit, Privatsphare* e *Intimsphare* –, sendo que elas se diferenciam por diferentes tipos de proteção da privacidade. Atualmente, esta teoria também é referida como a teoria que trata o indivíduo como "uma cebola passiva", desenvolvida pelo Tribunal Constitucional Alemão.

A primeira esfera, a camada mais superficial da privacidade, engloba informações que dizem respeito à vida privada do indivíduo, contudo são informações de certa forma públicas ou partilhadas, tais como endereço, telefone, dentre outros. A segunda esfera é a camada intermediária, restrita às informações que são íntimas porém são partilhadas com amigos íntimos e familiares. Por fim, a terceira esfera é a aquela do segredo do indivíduo, abrangendo informações que a pessoa quer manter apenas para si, pensamentos e informações íntimas[337] [338].

Esta última esfera nuclear é inviolável e inatingível e protegida contra qualquer intromissão das autoridades e de particulares. Há, aqui, uma proibição radical que não comporta exceções, tendo em vista que se trata da proteção do livre desenvolvimento da personalidade como fundação da dignidade da pessoa humana, base fundadora do Estado de Direito Democrático.[339]

---

[336] *In* HUBMANN, Heinrich, *Das Persönlichkeitsrecht.*

[337] AGUILERA, Abel Téllez - *Nuevas Tecnologías, intimidad y protección de datos*. Madrid, Editora Edisofer, 2001, p. 62

[338] Acórdão Tribunal Constitucional nº 607/2003 Processo nº 594/03 disponível em shorturl.at/ghwxL

[339] Acórdão Supremo Tribunal de Justiça n.º 886/07.8PSLSB.L1.S1. Disponível em shorturl.at/hrzLP

Em Portugal, Manuel da Costa Andrade[340] tratou da teoria no seu estudo a respeito das proibições de prova, tema que será tratado mais adiante. Já Menezes de Cordeiro tratou da teoria em âmbito civil[341]. A respeito das três esferas, Costa Andrade realizou uma análise comparativa entre o sistema alemão e norte americano.

Na Alemanha, esta teoria foi decisiva em alguns processos criminais, em especial em um caso de 1964 a respeito do diário pessoal, em que se discutiu a possibilidade da utilização de um diário íntimo do arguido como prova judicial. O Tribunal de Justiça Federal da Alemanha (*Bundesgerichtshof)* decidiu que, quando o arguido escreveu o diário pessoal, e lá pôs informações íntimas e secretas, o fez para a sua intimidade e que a sua utilização em âmbito de processo judicial feriria o direito ao livre desenvolvimento da personalidade por violar o direito à privacidade do arguido.[342] Como bem afirma, MANUEL DA COSTA ANDRADE, esta determinação vincula o estado e todos os seus órgãos a respeitar a dignidade da humana e o livre desenvolvimento da personalidade[343].

Nota-se a diferença do pensamento norte americano com relação ao alemão, que é focado na licitude ou ilicitude processual do acesso ao diário, diferentemente do pensamento alemão que é focado no conteúdo do diário que faz parte da esfera íntima do indivíduo. No caso norte americano, caso o diário seja apreendido de forma ilegal, não será admitido, caso haja mandato judicial a apreensão do diário é plenamente legal, o autor inclusive traça um paralelo com outros tipos de meios de prova como lenços e armas[344].

Atualmente, a teoria alemã criou certa flexibilização na teoria, especialmente com relação à criminalidade grave, compreendendo que, caso exista um núcleo inacessível – como no caso dos diários pessoais – haverá um aumento de insegurança, abrindo portanto a possibilidade para

[340] *Ibidem* COSTA ANDRADE, 1996, p.146
[341] CORDEIRO, António Menezes. *Tratado de Direito Civil Português*, Parte Geral – Pessoas. Vol. 1, tomo III, Lisboa: Almedina, 2004, p. 200.
[342] Disponível na Revista Neue Juristische Wochenschrift [NJW], de 1964, de p. 1139 a p. 1144, e de 1988, de p. 1037-1039.
[343] *Ibidem* COSTA ANDRADE, 2006, p. 142.
[344] *Ibidem* COSTA ANDRADE, 2006, p. 146/147.

uma ponderação caso a caso, levando em consideração a singularidade dos interesses postos em causa.[345] Além disso, disseminou-se o entendimento dos Tribunais alemães que a privacidade é um bem jurídico passível de ser flexibilizado na medida que pode salvaguardar interesses da comunidade, porém sempre com respeito à proporcionalidade[346].

No contexto português, o Tribunal Constitucional defendeu que todos os indivíduos têm o direito de proteger a sua intimidade, que engloba a vida familiar e íntima, contra intromissões alheias[347], e adotou a Teoria das Três Esferas ao afirmar que existe uma esfera pessoal íntima, "um núcleo mínimo onde ninguém penetre salvo autorização do próprio titular" que é inviolável. O Supremo Tribunal de Justiça teve o mesmo entendimento e afirmou que a dignidade da pessoa humana, como fundamento do Estado de Direito Democrático, exige que todos os indivíduos tenham um espaço de privacidade para o desenvolvimento da sua personalidade, sendo que esta privacidade deve ser a regra e não a exceção.[348]

Esta teoria não está livre de críticas, como bem aponta MANUEL DA COSTA ANDRADE, é por vezes difícil identificar quando uma intrusão afeta algum dos três níveis de privacidade de um indivíduo. Por isso, o autor defende uma análise de caso a caso[349].

Diante da relevância dos aparelhos telemóveis que já foi abordada por diversas vezes no presente estudo, é possível observar que estes aparelhos têm a capacidade de armazenar dados informáticos de diversos tipos, incluindo informações de cunho privado, como por exemplo, informações médicas, dados bancários, vídeos íntimos, dentre outros. Quando um telemóvel é alvo da pesquisa de dados informáticos, a autoridade policial terá acesso a todos os dados informáticos armazenados, sejam eles a respeito de uma eventual atuação criminosa ou sejam eles a respeito da vida privada do arguido.

---

345 Acórdão do Supremo Tribunal de Justiça n.º 886/07.8PSLSB.L1.S1. Disponível em www.dgsi.pt
346 *Ibidem* TEIXEIRA, 2010, p. 36.
347 Acórdão do Tribunal Constitucional n.º 128/92, Processo n.º 260/90. Disponível em https://www.tribunalconstitucional.pt/tc/acordaos/19920128.html
348 Supremo Tribunal de Justiça. Revista- 941/09.0TVLSB.L1. - 1.ª Secção - 21.10.14 Disponível em shorturl.at/dBGK7
349 *Ibidem* COSTA ANDRADE, 2006, p. 97.

Neste contexto, propomos realizar um paralelo entre os aparelhos telemóveis e os diários íntimos, como bem aponta COSTA ANDRADE ao dizer que os aparelhos eletrónicos são depósitos de informações pessoais tal como "diário, biblioteca, repositório de gestos, ações, planos, gostos, etc."[350] Vai no mesmo sentido a decisão da Suprema Corte dos Estados Unidos da América no caso *Riley v. California*, "telemóveis colocam uma grande quantidade de informações pessoais literalmente na mão dos indivíduos (...) telemóveis modernos são agora uma parte tão impregnada da nossa vida diária que se um visitante de Marte seria capaz de afirmar que são uma parte da anatomia humana". E, no caso *US v. Flores-Lopez,* "um usuário médio tem instalado em média trinta e três aplicações no seu telemóvel, que juntas podem criar uma montagem da vida do utilizador".

Tal como os diários íntimos, os telemóveis armazenam informações de cunho íntimo a qual não tem como objetivo serem compartilhadas com mais ninguém e que podemos compreender como parte do núcleo inviolável e inatingível das esferas. Diante disso, a desencriptação coativa de telemóveis tem a potencialidade de violar este núcleo inviolável da privacidade do indivíduo ao forçá-lo ceder acesso a ele.

Ressaltamos que, de acordo com a Lei do Cibercrime, a pesquisa de dados informáticos deverá ser determinada respeitando as normas das buscas e apreensões[351], isto posto, os dados pesquisados e apreendidos deverão ser especificados e determinados na decisão da autoridade judicial competente. Desta forma, no caso da desencriptação coativa de telemóveis o mesmo deverá ocorrer, isto é, deverá ser determinada pela autoridade judicial competente para um fim específico.

Contudo, não podemos ignorar os impedimentos éticos que surgem da prática da desencriptação coativa, sob o prisma da Teoria das Três Esferas. A desencriptação coativa abre a esfera mais íntima do indivíduo à devassa praticada pelo Estado, o que na nossa opinião, ultrapassa os limites impostos pela Constituição e pelo Direito Processual Penal.

---

350 *Ibidem* ANDRADE, 2009, p. 167.

351 Ressalte-se que as buscas e apreensões presentes no Código de Processo Penal são criadas para realidades tangíveis, portanto, não aplicáveis na sua integridade aos dados informáticos, tendo em vista que esses são considerados intangíveis. *In* RODRIGUES, 2008, p. 347.

A busca pela verdade material não poderá ser feita a todo custo e deverá respeitar balizas mínimas que permitem a existência de um processo justo e equitativo e portanto, para nós, a criação de um núcleo duro inviolável da esfera íntima do indivíduo é a proteção da dignidade e do desenvolvimento da personalidade e não é um impedimento na busca pela verdade material. Em razão disso, defendemos a repercussão da Teoria das Três Esferas na esfera do Processo Penal no âmbito das proibições de prova.

O tema das proibições de prova surgem através da jurisprudência norte-americana – através de um entendimento da Suprema Corte[352] – e a doutrina alemã – por Beling sob o nome de *Beweisverbote* – que conservam uma base comum que se divide em seus fundamentos[353]. A base comum é a proteção dos direitos fundamentais como uma limitação à descoberta da verdade material[354].

Esta é uma temática complexa e extensa, alvo de estudos importantíssimos inteiramente voltados à ela, como por exemplo, o já mencionado de Manuel da Costa Andrade[355]. Ressaltamos porém, que no presente estudo não será possível abordar o tema das proibição das provas de forma exaustiva e profunda, até mesmo porque não é o objetivo final do mesmo, porém iremos tratá-lo de forma que seja suficiente para apresentar as eventuais repercussões da desencriptação coativa.

Desta forma, conforme ressaltamos anteriormente, a busca pela verdade no processo deve ser limitada pelo respeito aos direitos fundamentais do arguido e também da sociedade. É exatamente o cerne das proibições de prova.

---

352 "Numa primeira fase da jurisprudência do *Supreme Court*, cujo marco inicial é constituído pelo acórdão *Boyd v. United States*, de 1886, a proibição de prova sustentou-se numa ideia, ainda que insuficientemente explicitada, de fusão ou combinação da proteção da privacidade da autoincriminação (...) A consagração das proibições de prova constitucionais, contudo, relaciona-se com uma linha marcante desenvolvida pela jurisprudência do Supremo Tribunal dos Estados Unidos, em que se extrai a Constituição, para além do fim central de regulação *da descoberta da verdade no respeito de direitos fundamentais*, um novo patamar de afastamento da prova por força da violação de imperativos constitucionais na sua obtenção". *In* MESQUITA, 2011, p. 226-270.

353 Contudo, o sistema americano e alemão tem bases principiológicas diferentes. No sistema americano, a licitude ou ilicitude processual é determinante, ou seja, o que decidirá a exclusão ou não das provas serão as formalidades legais. Já no sistema alemão o determinante será o conteúdo do diário, se ele trata de conteúdo íntimo e parte do desenvolvimento da personalidade. Vide COSTA ANDRADE, Manuel da, Sobre as Proibições de Prova em Processo Penal, Coimbra, Coimbra Editora, 2006, p. 147.

354 *Ibidem* MESQUITA, 2011, p. 209-218.

355 Inclusive, ressalta o autor que o tema das proibições de prova muda de autor para autor, por isso iremos adotar o entendimento de Costa Andrade em razão da sua importância para a matéria em Portugal.

JOÃO CONDE CORREIA[356], sustenta que as proibições de prova como formas de interditar meios, temas, métodos ou possibilidades de valoração são claras limitações ao total esclarecimento da verdade, que não poderá ser obtida a qualquer custo. Por este motivo, MANUEL DA COSTA ANDRADE define as proibições de prova como a tentativa de solucionar o conflito entre a ordem e a liberdade dos indivíduos, que cria balizas normativas a recolha e valorização de provas[357] [358] [359], também podendo ser conceituada como um dos meios processuais de tutela dos direitos fundamentais[360].

Além de protegerem direitos, liberdades e garantias individuais, ANTÓNIO DE JESUS TEIXEIRA também ressalta que as proibições de prova protegem toda a sociedade dos abusos que podem ser cometidos em busca da verdade, tendo em vista que não é admissível que o Estado permita que seus agentes se coloquem à margem da lei em uma busca sem limites pela verdade material[361].

O enquadramento jurídico das proibições de prova no ordenamento português inicia-se no artigo 32.º, n.º 8, da Constituição no qual aduz que "São nulas todas as provas obtidas mediante tortura, coação, ofensa da integridade física ou moral da pessoa, abusiva intromissão na vida privada, no domicílio, na correspondência ou nas telecomunicações". Além da disposição constitucional, as proibições se densificam em diversos artigos do Código de Processo Penal nomeadamente nos artigos 126.º, 129.º, n.º 1, 130.º, n.º 1, 134.º n.º 2 e 356.º, n.º 1 e 2.

Por isso, é possível afirmar que o modelo português de proibições de prova aproxima-se do desenvolvido pela jurisprudência norte-americana, que se fundou na Constituição como patamar de afastamento de prova, como aponta FIGUEIREDO DIAS[362]. Ao mesmo tempo que manteve

356 *Ibidem* CORREIA, 2014 p. 29–59.
357 *Ibidem* COSTA ANDRADE, 1992, p. 193.
358 COSTA ANDRADE, Manuel da, Proibições de Prova em Processo Penal (Conceitos e Princípios Fundamentais). *Revista Jurídica da Universidade Portucalense, n. 13*, 2008.
359 CORREIA, Eduardo, Les preuves en droit pénal portugais, *Revista de Direito e de Estudos Sociais*, ano XIV, 1967, p. 8
360 *Ibidem* ROSA, 2010, pp. 219-277.
361 TEIXEIRA, António de Jesus, *Os Limites do Efeito-à-distância nas Proibições de Prova no Processo Penal Português*, Lisboa, Editora Universidade Católica, 2010, p. 26-29.
362 FIGUEIREDO DIAS, Jorge De, *Direito Processual Penal*, 1ª ed, 1974, Coimbra, Coimbra Editora, p. 194.

similaridades com o direito alemão tendo em vista que o direito processual penal também criou instrumentos de garantia e tutela da busca da verdade[363].

O artigo 126.º do Código de Processo Penal, que trata a respeito dos métodos proibidos de prova não é taxativo[364], pelo contrário, apenas apresenta exemplos gerais de provas que possam ser ofensivas da integridade física e moral do indivíduo, como bem ressalta MANUEL DA COSTA ANDRADE[365]. Isto significa que há uma porta aberta para outras provas ofensivas que possam vir a surgir. Esta foi uma escolha sábia tendo em vista que permite uma atualização diante de novos meios de prova potencialmente lesivos aos direitos do arguido, contudo, ao nosso ver, também abre portas à uma subjetividade que pode ser lesiva tendo em vista que depende integralmente do entendimento do intérprete, que poderá ser mais ou menos conservador.

Na doutrina há divergências de opiniões com relação à autonomia dogmática das proibições de provas com relação ao sistema de nulidades. PAULO SOUSA MENDES, por exemplo, defende a diferença entre os regimes[366], entendimento também defendido por MANUEL DA COSTA ANDRADE[367]. Neste sentido, os autores defendem que pese embora o legislador por vezes se utilize do termo "nula" para se referir às proibições de prova, como observamos artigo 126.º do Código de Processo Penal, não se trata de um caso de nulidades[368], e sim de proibições de prova. Como bem aponta LUÍS PEDRO MARTINS DE OLIVEIRA ao afirmar que o referido artigo se utiliza de os mesmos termos do artigo 32.º, n.º 8 da Constituição, pese embora com pouca exatidão técnica[369].

363 *Ibidem* COSTA ANDRADE, 2006, p. 96.
364 Diferentemente do que ocorre com o sistema de nulidades, que é taxativo como é possível observar no artigo 118.º, nº.1 do CPP que aduz "a violação ou a inobservância das disposições da lei do processo penal só determina a nulidade do acto quando esta for expressamente cominada na lei".
365 *Ibidem* COSTA ANDRADE, 1992, p. 216
366 *Ibidem* MENDES, 2004, p. 148-149.
367 *Ibidem* COSTA ANDRADE, 1992, p. 195
368 CORREIA, João Conde, A distinção entre prova proibida por violação dos direitos fundamentais e prova nula numa perspetiva essencialmente jurisprudencial, *Revista do CEJ*, n.º 4, 1.º Semestre, 2006, p. 175-202
369 DE OLIVEIRA, Luís Pedro Martins, Da autonomia do regime das proibições de prova. In: *Prova Criminal e Direito de Defesa*. Coimbra: Almedina, 2010, p. 264.

Além disso, as proibições de prova também são distintas das regras de produção de prova, que são apenas meras formalidades que não geram eventuais proibições de valoração[370] [371].

Desta forma, podemos concluir que o principal objetivo das proibições de prova é proibir a produção de provas que tenham potencial violador de direitos fundamentais, contudo, caso elas sejam produzidas, também irão proibir a sua valoração, não podendo ser utilizadas no processo para fundamentar qualquer decisão como aponta GERMANO MARQUES DA SILVA[372].

A doutrina e a jurisprudência optam por dividir a matéria das proibições de prova em três categorias nomeadamente: as proibições de tema de prova, as proibições de meios de prova e as proibições de métodos de obtenção de prova. As proibições de tema de prova dizem respeito à temas que não devem ser alvos de prova, como por exemplo, o segredo de Estado, conforme previsto no artigo 137.º do Código de Processo Penal. As proibições de meios de prova por sua vez, estão dispostas nos artigos 129.º, n.º 1, 130.º, n.º 1, 134.º, n.º 2 e 356.º do Código de Processo Penal e diz respeito a meios de prova que não podem ser utilizados, como por exemplo, a proibição de reprodução de vozes e rumores públicos. Por fim, as proibições de métodos de obtenção de prova estão dispostas no artigo 126.º do Código de Processo Penal, distinguindo as proibições absolutas nos n.ºs 1 e 2 do referido artigo e as proibições relativas no n.º 3 do mesmo artigo[373] [374].

Para fins deste estudo, iremos nos restringir à análise de determinados artigos acerca do tema.

O artigo 126, n.1º do CPP protege o direito à integridade física e moral do arguido, em razão da amplitude da sua esfera de proteção, é possível alargar o escopo de proteção deste *caput* para outros artigos e previsões legais. Como bem referiu LUÍS BÉRTOLO ROSA ao apontar a

[370] ROSA, Luis Bértolo, Consequências Processuais das Proibições de Prova. *Revista Portuguesa de Ciência Criminal*, Ano 20, n. 2, 2010. pp. 219-277.
[371] *Ibidem* COSTA ANDRADE, 1992, p. 83 e ss.
[372] MARQUES DA SILVA, 2011, p. 178.
[373] *Ibidem* COSTA ANDRADE, 1992, p. 89-90.
[374] *Ibidem* COSTA ANDRADE, 2013, p. 222.

proteção dada ao artigo 14.º da Lei do Cibercrime, caso a prova seja obtida através de ameaça com medida legalmente inadmissível[375].

Com base no mesmo entendimento exarado pelo autor, podemos compreender que a desencriptação coativa de telemóveis também violaria os preceitos do artigo 126.º, n.º 1 do CPP por violar a integridade física e moral do arguido, coagindo-o a realizar uma ação a qual se negou a fazê-lo. Novamente aqui resgatamos a alegação utilizada quanto à violação da dignidade da pessoa humana, no sentido de não ser possível *mensurar* uma violação subjetiva de um direito. Tal como não é possível fazê-lo com a dignidade moral, também defendemos que o mesmo não poderá ser feito com a integridade física e moral.

A desencriptação coativa também ofende outro preceito do artigo 126.º, nomeadamente o nº.3 que protege o direito de reserva da vida privada, do domicílio, da correspondência e das telecomunicações, tendo em vista a já mencionada devassa que esta ação tem com relação à esfera íntima do indivíduo.

Por consequência, o artigo 126.º prevê proibições de valoração de prova, caso ela seja produzida, associadas também, as proibições de produção e de obtenção como forma de desencorajamento[376]. Por isso, aplicando-se ao caso da desencriptação coativa, ela estaria proibida de ser realizada, e caso o fosse proibida de ser valorada, e caso uma decisão a valorasse, a referida decisão ficaria viciada, como defende GERMANO MARQUES DA SILVA[377].

Por isso, como já foi ressaltado, compreendemos que o ato da desencriptação coativa gera uma cadeia de violações tanto a integridade física e moral do arguido quanto o seu direito à privacidade, por ser uma medida grave e drástica que tem a capacidade de adentrar na esfera mais íntima do indivíduo, não sendo possível a sua comparação com outros meios de prova que a princípio possam parecer de natureza similar.

---

375 *Ibidem* ROSA, 2010, pp. 219-277.
376 ROSA, 2010, pp. 219-277.
377 SILVA, Germano Marques da, *Curso de Processo Penal*, Vol. II, 5ª ed., Editora Verbo, 2011, p. 144.

Nesta toada, FIGUEIREDO DIAS[378] aponta que uma das consequências das proibições de prova é a inadmissibilidade da valoração das declarações prestadas e das indicações que por seu intermédio foram obtidas acerca de outros meios de prova, o que demonstra a atribuição do efeito-à-distância às provas proibidas.

O efeito â distância é um conceito jurídico desenvolvido nos Estados Unidos da América com o nome de *Fruit of the poisonous tree,* e na Alemanha, com o nome de *Makel-Theorie*. A teoria determina que, na hipótese de uma prova obtida através de um método proibido de prova possibilitar o avanço de uma investigação e eventualmente alcançar outros meios de prova.[379]

Essa teoria surgiu nos Estados Unidos da América no caso *Silverthorne Lumber Co v. United States*, em 1920, no qual agentes federais apreenderam documentos de forma ilegal. Na decisão, a Suprema Corte norte americana entendeu que tais provas não poderiam ser utilizadas de maneira nenhuma, tendo em vista que o meio de obtenção de prova foi ilegal, maculando todas derivações daquele ato. [380] Na Europa, esta teoria também foi maioritariamente aceita, pese embora com algumas modificações, no que concerne ao direito português tem a denominação de efeito à distância das proibições de prova.

De modo geral, o efeito à distância das proibições de prova segundo PAULO DE SOUSA MENDES é *"a única forma de impedir que os investigadores policiais, os procuradores e os juízes menos escrupulosos se aventurem à violação das proibições de prova na mira de prosseguirem sequencias investigatórias às quais não chegariam através dos meios postos à disposição pelo Estado de Direito"*[381]*.* Desta forma, nota-se que o principal objetivo do efeito à distância é desencorajar o uso de meios de prova e a prática de atos processuais que infrinjam violações a direitos fundamentais e ao devido processo legal pelo impedimento da apreciação destes no âmbito

[378] DIAS, Jorge Figueiredo, *Direito Processual Penal*, 1ª Edição, Coimbra, Coimbra Editora, 1974, p. 462.
[379] MOURÃO, Helena, *O efeito-à-distância* das proibições de prova no Direito Processual Penal português, *Revista Portuguesa de Ciência Criminal*, Ano 16, nº. 4, Outubro-Dezembro 2006, pp. 575-620.
[380] 308 US 308, 60 S.Ct. 266, 84 L.Ed.307 (1939)
[381] MENDES, Paulo de Sousa, Lições de Direito Processual Penal, Coimbra, Editora Almedina, 2013, p. 192.

do processo[382]. Por isso, compreendemos que os efeitos à distância também são um mecanismo de proteção de direitos fundamentais e de interesses supra individuais, traçando uma linha vermelha imaginária que não poderá ser ultrapassada. [383]

A doutrina portuguesa[384] tem sido assente ao apontar que o efeito à distância é aplicável no ordenamento jurídico português com base no artigo 122.º do Código de Processo Penal, além de apontar que o artigo 32.º, n.º 8 da Constituição deixa claro que todas as provas obtidas através do método proibido serão nulas e, portanto, deverão ser removidas do processo[385]. Vai no mesmo sentido a jurisprudência, nomeadamente o Tribunal Constitucional no acórdão n.º 198/2004, de 24 de março de 2004 que também foi reafirmado na Decisão Sumária do Tribunal Constitucional n.º 13/2008, de 11 de janeiro de 2008[386].

Ressaltamos que o efeito à distância não é absoluto, desde a sua criação até hoje mitigações foram sendo construídas pela jurisprudência de tribunais norte-americanos que também foram adotadas por outros países. Dentre tais limitações, a jurisprudência portuguesa[387] reconhece três: a descoberta inevitável[388], a fonte independente[389] e a mácula

---

382 "O desencorajamento legal da utilização de meios ilegítimos para obter confissão e a necessidade de obstar às autoincriminações – muitas vezes falsa e ou motivadas por factores afectivos ou causas psicopatológicas – esteve presente no art. 174.º do Código de Processo Penal Português de 1929, norma inserida no capítulo relativo ao "Corpo do Delito" que se estendia a todas as fases processuais: a confissão do arguido, desacompanhada de quaisquer outros elementos de prova, não valia como corpo de delito e em caso de confissão o juiz deveria proceder a todas as diligências para apurar a verdade, devendo investigar, se a confissão era ou não verdadeira". *In* GUIMARÃES, 2016, p. 90.

383 MOURÃO, Helena, *O efeito-à-distância* das proibições de prova no Direito Processual Penal português, *Revista Portuguesa de Ciência Criminal*, Ano 16, nº. 4, Outubro-Dezembro 2006, pp. 575-620.

384 Nomeadamente COSTA ANDRADE, Manuel da, (1992) p. 313, MARQUES DA SILVA, Germano (2008) p. 146, CONDE CORREIA, João (2006) p. 200 e AGUILAR, Francisco (2004) p. 91.

385 ROSA, Luís Bértolo, Consequencias Processuais das Proibições de Prova. *Revista Portuguesa de Ciência Criminal*, Ano 20, n. 2, 2010.

386 "(...) O TC afirmou a inteira vigência entre nós da doutrina da eficácia longínqua ou do efeito à distância, mas, no caso em apreciação, invocando a doutrina estabelecida pelo Supremo Tribunal dos EUA no caso *Wong Sun v. United States* (...)"

387 Vide Acórdão do Supremo Tribunal de Justiça de 20-02-2008 *"a fonte independente respeita a um recurso probatório destacado do inválido, usualmente com recuso a meio de prova anterior que permite induzir, probatoriamente, aquele a que o originário tendia, mas foi impedido; ou seja, quando a ilegalidade não foi 'conditio sine qua non' da descoberta dos novos factos (...) a descoberta inevitável a descoberta dos novos factos mostrava-se inevitável mediante recurso a outras diligências de prova, anteriores ou contemporâneas (...) a mácula dissipada a prova subsequente foi alcançada através de meios de prova autônomos e distintos, em termos tais que produzam uma decisiva atenuação da ilegalidade precedente".*

388 A limitação chamada descoberta inevitável foi fruto do entendimento jurisprudencial norte-americano no caso *Nix v. Williams-Williams II*. No caso em concreto, com base nas declarações obtidas ilegalmente ao arguido, a polícia foi capaz de encontrar o corpo da vítima de um crime de homicídio. Contudo, no entendimento da Suprema Corte americana, já havia um grupo de voluntários a buscar o referido corpo nas imediações de onde foi encontrado, sendo, portanto, uma questão de tempo até o encontrarem. Configurando, assim, uma descoberta inevitável, não invalidando a declaração. *In* PRADO, Alessandra Rapacci Mascarenhas, DA FRANÇA, Misael Neto Bispo. Teoria da descoberta inevitável: *Revista de Criminologias e Políticas Criminais*, 2017, 3.1: 42-59

389 A fonte independente pderivou dos precedentes *Silverthorne Lumber Co v. United States* e *Wong Sun v. United States* e é admissão da possibilidade de valorar provas mediatas através de uma rota alternativa, chamada fonte independente, livre de máculas. *In* MOURÃO, Helena, *O efeito-à-distância* das proibições de prova no Direito Processual Penal português, Revista Portuguesa de Ciência Criminal, Ano 16, nº. 4, Outubro-Dezembro 2006, pp. 575-620.

dissipada[390].[391] Ao defendê-las, o Tribunal Constitucional apontou que o efeito à distância não busca arrastar todas as provas consideradas máculadas sem qualquer ponderação, pelo contrário visa ponderar as situações a fim de se encontrar o nexo lógico e valorativo entre as provas.[392]

Contudo, defendemos que tais mitigações devem ser aplicadas com precaução, tendo em vista que, uma vez que o efeito à distância pode ser considerado uma proteção aos direitos fundamentais, as mitigações são brechas que possibilitam restrições a estes.

Isto posto, ao adotarmos o entendimento que a desencriptação coativa é considerada uma prova proibida por violar a dignidade do arguido juntamente com o seu direito à privacidade na sua esfera mais íntima, os dados informáticos pesquisados e eventualmente recolhidos que sejam utilizados em qualquer ponto do processo não poderão ser utilizados, devendo ser declarada a sua exclusão com base no artigo 308.º, n.º 3 do Código de Processo Penal, e em seguida, deverá haver a discussão da suficiência de outros indícios[393].

No caso da desencriptação coativa, defendemos que tais mitigações não são cabíveis tendo em vista que, como defendemos anteriormente, a desencriptação coativa é uma medida extrema que somente deve admissível quando os dados informáticos não estivessem armazenados em outro local, como por exemplo, em um serviço de nuvem. Desta forma, descartamos de pronto a fonte independente pois na desencriptação coativa a ilegalidade é, nas palavras do Supremo Tribunal de Justiça, *conditio sine qua non* da descoberta dos novos factos. O mesmo é possível firmar quanto à descoberta inevitável, tendo em vista que ao nosso entender, a desencriptação coativa deverá ser a última alternativa dentre todos os meios de obtenção de prova disponíveis para aceder aos dados informáticos armazenados no telemóvel.

---

[390] É também chamada de *purged taint exception* oriunda da jurisprudência norte-americana no caso *Wong Sun v. United States* e *United States v. Ceccolini*. Neste caso há uma "limpeza" da nódoa deixada pela ilegalidade, através de meios lícitos e alternativos posteriores que "corrigem a rota" para a legalidade.
[391] Acórdão Tribunal Constitucional nº 198/2004 de 24-03-2004 disponível em shorturl.at/yACZ3
[392] ROSA, 2010, pp. 219-277.
[393] *Ibidem* ALBUQUERQUE, 2008, p. 778-779.

Isto posto, defendemos que caso os dados armazenados estejam acessíveis através de outro modo que não seja a desencriptação, este método deverá ser adotado obrigatoriamente.

Quanto às consequências do efeito à distância das proibições de prova, PAULO PINTO ALBUQUERQUE aponta, com base no artigo 122.º, n.º 1 em conjunto com o artigo 126.º ambos do Código de Processo Penal, que sempre que uma prova proibida tenha sido utilizada como um fundamento de uma sentença ou acórdão a consequência será a nulidade do ato, devendo ser repetido sem a ponderação da prova proibida[394].

Nota-se, portanto, que todas as consequências previamente citadas neste terceiro capítulo, tanto as relacionadas com os direitos fundamentais do arguido quanto as de cunho jurídico-processuais, poderão ser relacionadas com as proibições de prova e consequentemente com o efeito à distância das proibições de prova.

Deste modo, sustentamos, que pese embora a desencriptação coativa de telemóveis seja considerada possível, as suas consequências jurídicas acarretariam inevitavelmente a proibição de provas tendo em vista a gravidade das violações perpetradas nos direitos fundamentais do arguido, o que na opinião deste estudo, não podem ser convalidadas. Deste modo, defendemos que os atos processuais advindos da desencriptação coativa devem ser considerados nulos levando em consideração os efeitos à distância das proibições de prova.

[394] *Ibidem* ALBUQUERQUE, 2008, p. 322.

CONCLUSÃO

O presente estudo incidiu sobre a temática da desencriptação coativa de telemóveis e as suas consequências jurídicas no âmbito do processo penal. Assim sendo, pretendeu-se abordar a importância da criptografia no contexto tecnológico atual, na medida em que aparelhos telemóveis se utilizam de técnicas criptográficas avançadas, que tem grande potencial de obstar meios de obtenção de prova, como a pesquisa de dados informáticos.

No primeiro capítulo deste estudo, apresentámos a história da criptografia e como ela avançou até atingir o momento atual, que a permite estar presente em aparelhos utilizados por todos nós no dia a dia, como os telemóveis. Ressaltámos como os telemóveis podem ser considerados uma extensão dos seres humanos, nos permitindo realizar diversas tarefas em poucos toques, com acesso à internet com facilidade que antes era só vista em filmes de ficção científica. Demonstrámos como a junção da internet com telemóveis operou uma verdadeira revolução tecnológica e social, gerando um número de dados informáticos – sensíveis ou não – como nunca antes foi visto. Foi neste ponto que pudemos observar que a criptografia passou a ser utilizada como meio de proteção dos dados gerados, armazenados e transmitidos pelos aparelhos telemóveis.

No entanto, apontámos que a utilização da criptografia nos telemóveis também apresenta um ónus, que é fornecer uma alta proteção aos dados que podem ser comprovativos da prática de ilícitos que podem ser eventualmente alvo de investigações. Enumerámos inúmeros casos, já conhecidos e abordados em âmbito internacional, em que indivíduos se utilizaram da criptografia como um escudo de proteção contra a investigação de comportamentos ilícitos: um grande exemplo são os atos preparatórios terroristas promovidos pelo Estado Islâmico. Por fim, apontámos como esta questão já está a ser discutida em âmbito internacional, que apresentra três soluções principais: criar uma entrada

alternativa para a criptografia, solução altamente criticada por criar uma vulnerabilidade geral para todos os usuários de telemóveis, desenvolver computadores capazes de decifrar a criptografia empregada, o que se demonstra difícil diante da tecnologia empregada neste método e, por fim, a desencriptação coativa de telemóveis, uma alternativa já empregada em diversos países por ser considerada mais simples e de rápida resolução.

No segundo capítulo, avançámos para a questão da desencriptação coativa de telemóveis. Iniciámos por apontar como ela já está a ser utilizada em alguns países europeus, quais são os critérios de aplicação e método de aplicação e, na segunda parte, abordámos a possibilidade de aplicação da desencriptação no ordenamento jurídico português.

Neste ponto, foi possível apontar que não há uma disposição legal expressa que trate a respeito da criptografia no ordenamento jurídico português, tampouco abordou-se na Lei do Cibercrime a criptografia como empecilho da realização da pesquisa de dados informáticos. Contudo, ressaltámos, ao realizarmos uma interpretação do artigo 61.º, n.º 6, alíneas a) à d), do Código de Processo Penal, que apresenta os deveres de cooperação do arguido, dentre eles o dever de sujeitar-se a diligências de prova, que se abre uma possibilidade interpretativa de inserir a desencriptação coativa de telemóveis nesta hipótese. Para sustentar este posicionamento, apontámos o Acórdão n.º 155/2007 do Tribunal Constitucional, que aplicou o mesmo entendimento à recolha de amostra de sangue para fins de exame de ADN.

Ressaltámos, porém, que, apesar de compreendermos que esta conclusão é plausível e lógica diante das disposições jurídicas atuais, nos opomos a este entendimento. Defendemos a necessidade de uma norma legal expressa que autorize a utilização da desencriptação coativa, quais as regras e parâmetros de aplicação, em que hipóteses ela poderá ser utilizada. Porém, seguimos o segundo capítulo na análise da hipótese de a interpretação ser no sentido oposto do nosso entendimento.

Apontámos assim, primeiramente, ser necessário que a autoridade judicial competente determine a realização da pesquisa de dados

informáticos, pormenorizando qual aparelho eletrónico será alvo da pesquisa, quais dados informáticos, a motivação do despacho e a importância dos dados para o processo. Uma vez que a pesquisa não possa ser feita em razão da proteção da criptografia, defendemos ser necessário um novo despacho que determine a desencriptação coativa de telemóveis, mediante pedido pormenorizado que demonstre a imprescindibilidade dos dados para o processo.

Observámos também como os dados informáticos podem ser considerados prova digital no âmbito do processo penal, a necessidade de uma análise especializada e com especial atenção à garantia da cadeia de custódia da prova que demanda extremo cuidado em razão das especiais caraterísticas dos dados informáticos.

Avançámos, em seguida, para o terceiro e último capítulo deste estudo, no qual abordámos quais as consequências jurídicas da desencriptação coativa. Dividimos este capítulo em duas partes, a primeira referente aos direitos fundamentais do arguido e a segunda referente às consequências processuais da prova obtida mediante a desencriptação.

Na secção a respeito dos direitos fundamentais afetados pela desencriptação coativa, procedemos com a análise da dignidade da pessoa humana, que compreendemos ser violada tanto na sua concepção de direito e princípio, quanto fundamento para demais direitos fundamentais em seguida analisados, nomeadamente a presunção de inocência, a igualdade de armas, o direito à privacidade e o direito à não autoincriminação. Julgámos que estes direitos são passíveis de ser violados pela desencriptação coativa de telemóveis, tendo em vista que esta coação reduz o arguido à um objeto de prova no processo, ultrapassando o mero dever de cooperação afetando de morte a sua condição humana e moral, submetendo-o a uma posição inferior à da acusação.

Ao procedermos com a análise das consequências processuais, observámos as implicações da utilização dos dados informáticos como prova obtidos mediante da desencriptação coativa. Defendemos, em seguida, a proibição de prova obtida por meio da desencriptação coativa,

em razão de ofender a dignidade e integridade física e moral do arguido, além de violar a esfera mais íntima da vida do indivíduo. Apontámos que as consequências das provas obtidas por meio de desencriptação serão determinadas pelo efeito à distância das provas proibidas, invalidando os atos processuais que as levem em consideração.

Por fim, ressaltámos novamente que não compreendemos ser admissível a aplicação da desencriptação coativa de telemóveis em razão de todo o exposto no presente estudo. Contudo, procedemos à esta análise em razão de dois motivos simples. O primeiro é o facto de haver uma lacuna jurídica a respeito da criptografia, esta lacuna não está adstrita ao ordenamento português e sim é geral, tendo em vista que este tema ainda é delicado e complexo, o que nos leva ao segundo ponto.

Ao observarmos a evolução tecnológica dos recentes anos e como a tecnologia tem tomado cada vez mais espaço no dia a dia de todos nós, é possível concluir que o tema da criptografia se tornará cada vez mais urgente. Por isso, entendemos que em razão da dificuldade de legislar acerca do assunto, a tendência será realizar uma interpretação ampla do dever de cooperação do arguido, no sentido de aplicar-se também à desencriptação coativa. Isto reforça-se no contexto de os aparelhos telemóveis permitirem a desencriptação através de dados biométricos, o que poderá ser considerada uma ofensa mínima na integridade física e moral do arguido, abrindo portas à aplicação da medida de forma desenfreada.

Urge, portanto, uma discussão séria e profunda acerca da matéria, em especial dos riscos à flexibilização dos direitos fundamentais do arguido ao ponto da diminuição próxima da extinção.

BIBLIOGRAFIA

Advanced Encryption Standard (AES): What It Is and How It Works, disponível em <https://securityboulevard.com/2020/04/advanced-encryption-standard-aes-what-it-is-and-how-it- works/ > Acesso em 10 de abril de 2021.

AFFONSO, Filipe José Medon. A criptografia na era dos bloqueios do WhatsApp: uma análise segundo a metodologia civil-constitucional. *In* TEPEDINO, Gustavo et al. (Coord.). *Anais do VI Congresso do Instituto Brasileiro de Direito Civil.* Belo Horizonte, Editora Fórum, 2019. pp. 299-324.

AGUILERA, Abel Téllez - *Nuevas Tecnologías, intimidad y protección de datos*. Madrid, Editora Edisofer, 2001.

AHLBERG, Christopher, *How Al-Qaeda uses encryption post-Snowden* (Part 2) – New Analysis in Collaboration with ReveringLabs, Recorded Future, Disponível em shorturl.at/nJUZ8 acesso em 21 de Abril de 2021.

ALBUQUERQUE, Paulo Sérgio Pinto de, *Comentário do Código de Processo Penal: à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem*, 4a ed. Lisboa, Universidade Católica Editora, 2011.

ALBUQUERQUE, Paulo Sérgio Pinto de, *Comentário do Código de Processo Penal: à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem*, 4a ed. Lisboa, Universidade Católica Editora, 2011.

ALEXANDRINO, José De Melo, *A Estruturação do Sistema de Direitos, Liberdades e Garantias na Constituição Portuguesa*, Volume II. Coimbra, Editora Almedina, 2006.

ALEXY, Robert, *Teoria de los derechos fundamentales*, Centro de Estudios Constitutionales, Madrid, 1993.

ALMEIDA, Reginaldo Rodrigues de, *Sociedade Bit: Da Sociedade da informação à Sociedade do Conhecimento*, Porto, Editora Quid Iuris, 2004.

ANDRADE, Manuel da Costa, *Liberdade de Imprensa e Inviolabilidade Pessoal*, Coimbra, Coimbra Editora, 1996.

ANTUNES, Maria João, Direito Processual Penal, Coimbra, Editora Almedina, 2016.

Associação Portuguesa de Apoio à Vítima – APAV, Folha Informativa: Segurança de telemóveis, disponível em: https://apav.pt/apav_v3/images/folhas_informativas/fi_seguranca_dispositivos_moveis.pdf

BARBAGALO, Fernando Brandini. *Presunção de inocência e recursos criminais excepcionais: em busca da racionalidade no sistema processual penal brasileiro*, Editora TJDFT, 2015.

BECK, Ulrich, *Sociedade de risco*, São Paulo: Editora 34, 2010.

BIONI, Bruno. "Compreendendo o conceito de anonimização e dado anonimizado." *Cadernos Jurídicos. São Paulo, ano* 21, 2020, pp. 191-201.

BOLINA, Helena Magalhães, Razão de ser, significado e consequências do princípio da presunção de inocência (art. 32.o, n.o 2 da CRP), *Boletim da Faculdade de Direito de Coimbra*, Vol. IXX (Separata), Estudos nos Cursos de Mestrado, 1994.

BRANN, Noel L. *Trithemius and Magical Theology: A Chapter in the Controversy over Occult Studies in Early Modern Europe*, State University of New York Press, 1998.

BRAVO, Jorge Dos Reis, Tetis Contra Se - A possibilidade de um Direito ao Silêncio Corporal. *Revista do CEJ, 2018 - I*. Lisboa. 2018, pp. 151–194.

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

BRENNER, Susan W., FREDERIKSEN, Barbara A., Computer Searches and Seizures: Some Unresolved Issues, 8 Mich. Telecomm. & Tech. Law Review, n.º 39, 82, 2002.

BURUM, Sue, HOLMES, Georgia, Apple v. FBI: Privacy vs. Security?, Minnesota State University, Volume 48, Number 2, 2016.

CANCELA, Alberto Gil Lima, *A prova Digital: Os meios de obtenção de prova na Lei do Cibercrime* em dissertação apresentada à Faculdade de Direito da Universidade de Coimbra no âmbito do 2.º Ciclo de Estudos em Direito, na área de especialização em ciências jurídico-forenses sob orientação da Professora Doutora Sónia Mariza Florêncio Fidalgo em 2016.

CANOTILHO, J.J Gomes e MOREIRA, Vital, *Constituição da República Portuguesa Anotada*, Vol. I, 4.o, Ed. Revista, Coimbra, Coimbra Editora, 2007.

CANOTILHO, José Joaquim Gomes, *Direito Constitucional e Teoria da Constituição*, Coimbra, Editora Almedina, 4ª edição, 2000, p. 1137-1139.

CANOTILHO, José Joaquim Gomes, MOREIRA, Vital Martins, *Constituição da República Portuguesa Anotada*, Vol. I, Coimbra, Coimbra Editora, 2007.

CASEY, Eoghan, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*, 3ª ed., Academic Press/Elsevier, 2011.

CAVOUKIAN, Ann, STOIANOV, Alex, Biometric Encryption. In: TILBORG Henk, JAJODIA, Suschil, *Encyclopedia of Cryptography and Security*, Springer, Boston, 2011.

CHOONG, Yee-Yin, FRANKLIN, Joshua M., GREENE, Kristen M., *Usability and Security Considerations for Public Safety Mobile Authentication, Maryland*, National Institute of Standards and Technology, 2016.

Comissão Europeia, *Technical Solutions to detect child sexual abuse in end-to-end encrypted communications,* Disponível em <

https://www.politico.eu/wp-content/uploads/2020/09/SKM_C45820090717470-1_new.pdf> Acesso em 22 de Abril de 2021.EN E- 005255/2020

CORDEIRO, António Menezes. *Tratado de Direito Civil Português*, Parte Geral – Pessoas. Vol. 1, tomo III, Lisboa: Almedina, 2004.

CORREIA, Eduardo, Les preuves en droit pénal portugais, *Revista de Direito e de Estudos Sociais*, ano XIV, 1967.

CORREIA, João Conde, A distinção entre prova proibida por violação dos direitos fundamentais e prova nula numa perspetiva essencialmente jurisprudencial, *Revista do CEJ*, n.º 4, 1.º, Semestre, 2006.

CORREIA, João Conde, Prova digital: as leis que temos e a lei que devíamos ter. *Revista do Ministério Público n.º 139*, 2014, pp. 29–59.

CORREIA, Victor, *Sobre a Privacidade.* Lisboa: Sinapis Editores, 2014.

COSTA ANDRADE, Manuel da, *Bruscamente no Verão Passado: a reforma de Processo Penal,* Coimbra, Coimbra Editora, 2006.

COSTA ANDRADE, Manuel da, *Constituição e direito penal in A justiça nos dois lados do Atlântico*, Lisboa, Fundação Luso-Americana para o desenvolvimento, 1998.

COSTA ANDRADE, Manuel da, Proibições de Prova em Processo Penal (Conceitos e Princípios Fundamentais). *Revista Jurídica da Universidade Portucalense, n. 13*, 2008.

COSTA ANDRADE, Manuel da, Sobre as Proibições de Prova em Processo Penal, Coimbra, Coimbra Editora, 2006.

COSTA, José de Faria, *As telecomunicações e a privacidade: o olhar (in)discreto de um penalista*, Coimbra, Coimbra Editora, 1999.

CRORIE, Benedita Mac, O Recurso ao Princípio da Dignidade da Pessoa Humana na Jurisprudência do Tribunal Constitucional. Em Separata - *Estudos em Comemoração ao 10 Aniversário da Licenciatura em Direito da Universidade do Minho*. Coimbra, Almedina, 2003.

DÁ MESQUITA, Paulo, *A prova do Crime e o que se disse antes do julgamento*. Coimbra, Coimbra Editora, 2011.

DE JESUS, Francisco Marcolino. *Os Meios de Obtenção da Prova em Processo Penal.* 2a. Edição. Almedina, 2019, p. 33/84.

DE OLIVEIRA, Luís Pedro Martins, Da autonomia do regime das proibições de prova. In: *Prova Criminal e Direito de Defesa*. Coimbra: Almedina, 2010.

DECHAMPS, Claude, *Cybercriminalité*, La Commission de la Defense Nationale et des Forces Armées, Avril 2005.

Decision Makers Decrypting the Encryption Debate: A Framework for National Academies of Sciences, Engineering, and Medicine, National Academies Press, 2018.

DEL CANTO, Enrique Rovira, Delincuencia informática y fraudes informáticos. Editorial Comares, 2002..

DIAS, Jorge de Figueiredo, *Para uma nova justiça penal*, Coimbra, Editora Almedina, 1996.

DIAS, Jorge Figueiredo, *Direito Processual Penal*. Coimbra, Coimbra Editora, 1974.

DIAS, Vera Elisa Marques, *A problemática da investigação do cibercrime*, Trabalho de conclusão do I Curso de pós-graduação de aperfeiçoamento em direito da investigação criminal e da prova, Universidade de Lisboa, Faculdade de Direito, 2010.

DIFFIE, Whitfield e HELLMAN, Martin E., New Directions in Cryptography, IEEE Transactions on Information Theory, Vol. IT-22, n.º 6, November 1976. Disponível em: https://ee.stanford.edu/~hellman/publications/24.pdf

Diretiva (EU) 2016/343 do Parlamento Europeu e Conselho de 9 de março de 2016, disponível em https://eur-lex.europa.eu/legalcontent/PT/TXT/?uri=celex%3A32016L0343

Revista Neue Juristische Wochenschrift [NJW], de 1964, de p. 1139 a p. 1144, e de 1988, de p. 1037-1039.

DOS SANTOS, Gil Moreira, *Princípios e Prática Processual Penal*, Coimbra, Coimbra Editora, 2014.

DRUMMOND, Victor, *Internet, Privacidade e Dados Pessoais*. Rio de Janeiro: Lumen Iuris, 2003.

ARZAMENDI, José Luis de la Cuesta, *Derecho Penal Informático*, 1a edición, Civitas, 2010.

EuroJust Cybercrime Judicial Monitor, Issue n.º 4, 01 December, 2018, 2018/00017.

European Commission, *Technical solutions to detect child sexual abuse in end-to-end encrypted communications*, Disponível em < shorturl.at/gvKSW > Acesso em 21 de Abril de 2021.

European Union Agency for Cybersecurity, *Eletronic evidence – a basic guide for First Responders*. Disponível em < https://www.enisa.europa.eu/publications/electronic-evidence-a-basic-guide-for-first- responders > Acesso em 24 de abril de 2021.

European Union Legislation, Fight against organized crime *In* https://eur-lex.europa.eu/summary/chapter/2308.html acesso em 06 de setembro de 2021

Europol Press Release disponível em shorturl.at/ryTU7 acesso em 21 de Abril de 2021.

FIGUEIREDO DIAS, Jorge De, *Direito Processual Penal*, 1ª ed., 1974, Coimbra, Coimbra Editora.

FIGUEIREDO DIAS, Jorge de, *Direito Processual Penal*, Coimbra, Coimbra Editora, reimpressão, 2004.

FRIED, Ina, Feds warn threats are harder to track as extremists shift to encryption, Disponível em shorturl.at/ehlCl acesso em 21 de Abril de 2021.

"This is our house!" A preliminary assessment of the Capitol Hill Siege Participants disponível em shorturl.at/xLMPY acesso em 20 de Agosto de 2021

FUSTER, Gloria González - *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Editora Springer, 2014.

GOMES CANOTILHO, J.J., MOREIRA, Vital, *Constituição da República Portuguesa Anotada*, vol. I, 4a ed. revista, Coimbra, Coimbra Editora, 2007.

GONÇALVES, Manuel, Recolha de amostras de ADN para fins de investigação criminal Suspeito. *Revista do Ministério Público,* n.o 136, p. 199–222.

GUIMARÃES, Ana Paula, *A Pessoa como objecto de prova em Processo Penal: Exames, Perícias e Perfis de ADN – Reflexões à luz da dignidade humana*, Editora Nova Causa, 2016.

HUBMANN, Heinrich, *Das Persönlichkeitsrecht.*

JONES, Nigel*, et. al.* Vic CyberCrime@IPA, European Union and Council of Europe, Joint Project on Regional Cooperation against Cybercrime, *Electronic evidence guide - A basic guide for police officers, prosecutors and*

judges, Version 2.0, 2020. Disponível em shorturl.at/cdP06 acesso em 24 de Abril de 2021.

JÚDICE, Dr. José Miguel, Escutas telefónicas: a tortura do Século XXI?, *Revista da Ordem dos Advogados*, Ano 64, Vol. I/II, Nov. 2004 disponível em shorturl.at/bdxLP acesso em 06 de setembro 2021

Grupo de Proteção de Dados do Artigo 29.o, Adotado em 27 de abril de 2012. Disponível em < https://www.gpdp.gov.mo/uploadfile/others/wp193_pt.pdf >

KEENAN, Thomas P., *Replacing Something Bad with Something Worse: Why Biometric Authentication Will Be So Creepy*, Canada, University of Calgary, 2016.

Kelly v Jamaica, Merits, Communication No 253/1987, UN Doc CCPR/C/41/D/253/1987, IHRL 2403 (UNHRC 1991), 8th April 1991, United Nations [UN]; Human Rights Committee [CCPR]

KERR, Orin S., Compelled Decryption and the Privilege Against Self-Incrimination. *Texas Law Review,* n.º 97, 2018, pp. 767
KERR, Orin S., & SCHNEIER, Bruce, Encryption workarounds. *Georgetown Law Journal,* 2018, pp. 989- 1019.

KERR, Orin S., Search Warrants in na Era of Digital Evidence, *Mississippi Law Journal*, Vol. 75 (2005), pp. 92-97.

KU Kleven CiTiP. Disponível em https://www.law.kuleuven.be/citip/blog/you-have-the-right-to-remain-silent-until-we-want-your- smartphone-password/ Acesso em 18 de maio de 2021.

LEINER, Barry M., *et al*. "A brief history of the Internet." *ACM SIGCOMM Computer Communication Review* 39.5, 2009, pp. 22-31. https://dl.acm.org/doi/pdf/10.1145/1629607.1629613

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

LIM, Nena, & KHOO, Anne, "Forensics of computers and handheld devices: identical or fraternal, *Communications of the ACM,* 52 (6), pp. 132-135.

LOUREIRO, Flávia Noversa, "O direito fundamental à não autoincriminação – Essência, refrações e configuração moderna no espaço lusófono", III Congresso Internacional Direito da Lusofonia, Braga, 2016.

Loureiro, Flávia Noversa. "The spoken word, the written word and the digital word – discursive discontinuities and change of legal canons". In *Legal Challenges in The New Digital Age*, Leiden: Koninklijke Brill NV, 2021, pp. 253-263.

LOUREIRO, Flávia Noversa, "A palavra falada, a palavra escrita, e a palavra digital – descontinuidades discursivas e alteração dos cânones jurídico-penais" In *Direito na Lusofonia. Direito e Novas Tecnologias.* Braga, Escola de Direito da Universidade do Minho, JUSGOV, 2019, pp. 11-18.

LOPES DO REGO, Carlos, Acesso ao direito e aos tribunais, *Estudos sobre a jurisprudência do Tribunal Constitucional*, Aequitas/Editorial de Notícias, 1993.

LOPES JR, Aury, O problema da "verdade" no Processo Penal em Verdade e Prova no Processo Penal *In Estudos em homenagem ao professor Michele Taruffo*, Editora Gazeta Jurídica, São Paulo.

LÓPEZ, Manuel José Lucena, *Criptografia y seguridad em computadores*, 3ª edição, Universidad de Jaén, 2001.

MARCACINI, Augusto Tavares Rosa, *Direito e Informática: uma abordagem jurídica sobre a criptografia*, São Paulo, 2010.

MARCACINI, Augusto Tavares Rosa, O documento eletrônico como meio de prova, São Paulo, Novembro, 1999, Disponível em: https://simagestao.com.br/wp-content/uploads/2016/05/Odocumentoeletronicocomomeiodeprova.pdf

MARCOLINO DE JESUS, Francisco, *Os Meios de Obtenção da Prova em Processo Penal*, 2a edição, Coimbra, Editora Almedina, 2019,

Taylor, Mark, John Haggerty, David Gresty, and Robert Hegarty. "Digital evidence in cloud computing systems." *Computer law & security review n.º* 26, nº. 3, 2010, pp. 304-308.

MARQUES DA SILVA, Germano, *Curso de Processo Penal*, Volume III, Editorial Verbo, 2000.

MARQUES DA SILVA, Germano, Curso de Processo Penal, Vol. II, Lisboa, Editora Verbo, 4.ª edição, 2008.

MARR, Berbard, How much data do we create very day? The mind-blowing stats everyone should read. Forbes Magazine, disponível em: shorturl.at/ahxKZ acesso em 06 de junho de 2021.

Mary-Ann Russon & Jason Murdock, "Welcome to the Bizarre and Frightening World of Islamic State channels on Telegram," *IB Times*, June 2, 2016, disponível em shorturl.at/copDH acesso em 6 de setembro de 2021

MASON, Stephen e SHELDON, Andrew, *Proof: The investigation, collection and examination of digital evidence in Evidence*, University of London Press, Institute of Advanced Studies, 2017.

MEDERO, GEMA SÁNCHEZ, Cibercrimen, Ciberterrorismo y Ciberguerra: Los Nuevos Desafíos Del S. XXI, *Revista Cenipec*, n.o 31, Enero-Diciembre, 2012, pp. 239-267.

MENDES, Paulo de Sousa, em *Jornadas de Direito Processual Penal e Direitos Fundamentais*, Almedina, 2004..

MENDES, Paulo de Sousa, Lições de Direito Processual Penal, Coimbra, Editora Almedina, 2013, p. 192.

MENDONÇA JÚNIOR, Francisco de Paula Souza de Mendonça *Artífice do Segredo: O Abade Johannes Trithemius (1462-1516) Entre o Magus e o Secretarium do Princeps*, Dissertação de Mestrado na Faculdade de Filosofia e Ciências Humanas da Universidade Federal de Minas Gerais, Belo Horizonte, 2009.

MESQUITA, Paulo Dá, *Processo Penal, Prova e Sistema Judiciário*, Coimbra, Coimbra Editora, 2010.

MICHALEK, Marta, Fishing Expeditions and Subsequent Electronic Searches in the Light of the Principle of Proportionality of Inspections in Competition Law Cases in Europe, *Yearbook of Antitrust and Regulatory Studies*, Vol. 2014, 7 (10), pp. 129- 157. Disponível em shorturl.at/htyP4

MILITÃO, Renato Lopes, A propósito da prova digital no Processo Penal. *Revista da Ordem dos Advogados*, 2012, pp. 247–281.

MIRANDA, Jorge, *Escritos Vários sobre Direitos Fundamentais.* Estoril, Principia, 2006.

MIRANDA, Jorge, *Manual de Direito Constitucional. Direitos Fundamentais*, Tomo IV, 5.a edição, Coimbra, Coimbra Editora, 2012.

MIRANDA, Jorge, MEDEIROS, Rui, *Constituição Portuguesa Anotada*, Tomo I, Coimbra, Coimbra Editora, 2005.

MOURA, José Souto de "A *Questão da Presunção de Inocência do Arguido*".RMP. Lisboa, Sindicato dos Magistrados do Ministério Público, Ano 11, no 42, pp. 31-47.

MOURÃO, Helena, *O efeito-à-distância* das proibições de prova no Direito Processual Penal português, *Revista Portuguesa de Ciência Criminal*, Ano 16, no. 4, Outubro-Dezembro 2006, pp. 575-620.

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

NOVAIS, Jorge Reis, *A dignidade da pessoa humana*, Coimbra, Editora Almedina, 2015.

NOVAIS, Jorge Reis, *Os princípios Constitucionais Estruturantes da República Portuguesa,* 1ª Edição, Coimbra, Almedina, 2011.

NUNES, Duarte Rodrigues, *Os Meios de Obtenção de Prova previstos na Lei do Cibercrime*, Coimbra, Editora Getlegal, 2018.

O'NEILL, Patrick Howell, *How a drug cartel used encryption and a fake website to launder millions*. Disponível em <https://www.dailydot.com/debug/mexican-cartel-encryption/ > Acesso em 21 de Abril de 2021.

OLIVEIRA E SILVA, Sandra, *O Arguido como meio de prova contra si mesmo: Considerações em torno do princípio nemo tenetur se ipsum accusare*. Coimbra, Editora Almedina, 2019.

OLIVEIRA, Ronielton Rezende, Criptografia simétrica e assimétrica: os principais algoritmos de cifragem, *Segurança Digital Revista Online*, n.o 31, pp. 11-15.

OWEN, Gareth e SAVAGE, Nick,The Tor and Dark Net, *Global Comission on Internet Governance Paper Series* n.o 20, Setembro 2015, disponível em shorturl.at/rtFLR acesso em 14 de março 2021

PAAR, Christof e PELZL, Jan, *Understanding Cryptography: A textbook for Students and Practitioners*, Nova Iorque, Editora Springer, 2010

PALACIOS, Fernando Pinto, CAPILLA, Purificación Pujol. *La prueba en la era digital* Madrid, Wolters Kluwer, 2017.

PALMA, Maria Fernanda, Tutela da Vida Privada e Processo Penal: Realidades e Perspetivas Constitucionais em *VIII Conferencia Trilateral – A proteção da vida privada na jurisprudência do Tribunal Constitucional*, 2-3 de outubro 2006, Lisboa. 2006.

PALMER, Gary, A Road Map for Digital Forensic Research, *DFRWS Technical Report, Report from the First Digital Forensic Research Workshop*, 6 de Novembro de 2001, disponível em https://dfrws.org/wpcontent/uploads/2019/06/2001_USA_a_road_map_for_digital_forensic_research. pdf acesso em 13 de abril de 2020

PINHEIRO, Alexandre Sousa, *Privacy e Protecção de Dados Pessoais: A Construção Dogmática do Direito à Identidade Informacional.* Lisboa: AAFDL, 2015.

PINTO, Lara Sofia, Privilégio contra a auto-incriminação versus colaboração do arguido. In: *Prova Criminal e Direito de Defesa*. Coimbra, Almedina, 2010.

PRADO, Alessandra Rapacci Mascarenhas, DA FRANÇA, Misael Neto Bispo. Teoria da descoberta inevitável: *Revista de Criminologias e Políticas Criminais*, 2017, 3.1, pp. 42-59.

BATISTA, Vera Malaguti (coord.). *Discursos Sediciosos*: *crime, direito e sociedade.* Rio de Janeiro: Editora Revan, p. 67-74, ano 17, n. 19/20, p. 1.º e 2.º semestres de 2012.

QUINTANILHA, Tiago Lima, CARDOSO, Gustavo, ESPANHA, Rita, A apropriação dos Telemóveis na Sociedade em Rede, *A Sociedade em Rede*, 2010.

RAMALHO, David Silva, *Métodos Ocultos de Investigação Criminal em Ambiente Digital*, Coimbra, Coimbra Editora, 2017.

RAMOS, Vânia Costa, Corpus Iuris 2000 – Imposição ao arguido de entrega de documentos para prova e *nemo tenetur se ipsum accusare*" (Parte I), *Revista do Ministério Público*, n.o 108, Out-Dez-, 2006, pp. 132-133.

RIBEIRO, Maria da Conceição Fernandes, Dissertação de mestrado apresentada para a obtenção do grau de Mestre em Ciências Jurídico-Forenses sob a orientação da Professora Doutora Cristiane Reis e da Co-Orientadora Mestre Sara Moreira no Instituto Superior Bissaya Barreto em 2015.

RIBEIRO, Telma Sofia Martins, *A "intercomunicabilidade probatória" entre o procedimento de inspeção tributária e o processo penal*. Dissertação do Mestrado em Direito Judiciário, Escola de Direito, Universidade do Minho. Braga, 2017.

RIJMEN, Vincent, DAEMEN, Joan, *Advanced encryption standard. Proceedings of Federal Information Processing Standards Publications*, National Institute of Standards and Technology, 2001.

RISTORI, Adriana Dias Paes, Sobre o silêncio do arguido no interrogatório no processo penal português, Editora Almedina, Coimbra, 2007.

RODRIGUES, Benjamim da Silva, *Da Prova Penal – Tomo IV: da prova eletrónico-digital e da criminalidade informático-digital,* Lisboa, Editora Rei dos Livros, 2008.

RODRIGUES, Benjamim Silva, *Da Prova Penal, Tomo VI: Novos métodos "Científicos" de investigação Criminal nas Fronteiras das Nossas Crenças*, 1ª Ed., Editora Rei dos Livros, 2011.

RODRÍGUEZ LAINZ, José Luiz, *La intervención judicial de las comunicaciones del concursado*, Editorial Bosch, S.A, 2004.

ROSA, Luis Bértolo, Consequências Processuais das Proibições de Prova. *Revista Portuguesa de Ciência Criminal*, Ano 20, n.º 2, 2010. pp. 219-277.

ROXIN, Claus E SCHÜNEMANN, Bernd, *Derecho Procesal Penal,* 29.ª Edição de Darío Rolón e Mario Amoretti, Buenos Aires, Editora Didot.

ROXIN, Claus, *Introdução ao Direito Penal e ao Direito Processual Penal*, Belo Horizonte, Del Rey Editora, 2007.

Senate of the United States of America, *A bill to improve the ability of law enforcement agencies to access encrypted data*, and for other purposes. Disponível em https://www.docdroid.net/lHilrMA/oll20597-pdf Acesso em 22 de Abril de 2021.

SHEHABAT, Ahamad, MITEW, Teodor & ALZOUBI, Yahia, Encrypted Jihad: Investigating the Role of Telegram App in Lone Wolf Attacks in the West, *Journal of Strategic Security,* n.o 10 (3), 2017, pp. 27–53

SILVA, Germano Marques da, *Curso de Processo Penal*, Vol. II, 5a ed., Editora Verbo, 2011.

DIAS, Jorge Figueiredo, *Direito Processual Penal*, 1a Edição, Coimbra, Coimbra Editora, 1974.

SILVA, Germano Marques, *Do Processo Penal Preliminar*, Editorial Minerva, 1990.

SILVA, Sandra Oliveira e. Legalidade da prova e provas proibidas. *Revista Portuguesa de Ciência Criminal,* Ano 21, n.º 4, 2011, p. 545–591.

SIRACUSANO, Fabrizio, GALATI, Antonino, TRANCHINA, Giovanni, ZAPPALA, Vicenzo, DI CHIARA, Giuseppe, *Diritto Processuale Penale*, volume primo, Giuffrè Editore, 2004.

SMITH, Bradford, The third Industrial Revolution, *Policymaking and Technology Law*

TEIXEIRA, António de Jesus, *Os Limites do Efeito-à-distância nas Proibições de Prova no Processo Penal Português*, Lisboa, Editora Universidade Católica, 2010.

TEIXEIRA, Maria Leonor - Proteção de dados e big data, Os desafios líquidos do pós-panoptismo. *Revista do Ministério Público n. 159*, Lisboa, 2019.

The History of Secure Phones, disponível em <https://www.mssdefence.com/blog/secure-phones- history/ > Acesso em 10 de abril de 2021.

Third Report of the Observatory Function on Encryption, Joint Report Europol & Eurojus Information, June 2021. Disponível em: https://www.europol.europa.eu/publications-documents/third-report-of-observatory-function-encryption acesso em 06 de setembro 2021 Eurojust, Cybercrime Judicial Monitor.

Third Report of the Observatory Function on Encryption, Joint Report Europol & Eurojus Information, June 2021. Disponível em: https://www.europol.europa.eu/publications-documents/third-report-of-observatory-function-encryption

TIAN, Zhihong, *et al.* Block-DEF: A secure digital evidence framework using blockchain."*Information Sciences* 491 (2019): 151-165. Disponível em < shorturl.at/bmLPX>

TRECHSEL, Stefan - *Human Rights in Criminal Proceedings*. Oxford, Oxford University Press, 2005.

U.S. Department of Justice, Office of Justice Programs, National Institute of Justice, *Forensic Examination of Digital Evidence: A Guide for Law Enforcement*, 1st ed, 2014 p. 46. Disponível em <https://www.ncjrs.gov/pdffiles1/nij/199408.pdf > Acesso em 24 de abril de 2021.

VALENTE, Manuel Monteiro Guedes, *Cadeia de Custódia da Prova*, Coimbra, Editora Almedina, 2019.

VATTIMO, Gianni, *A sociedade transparente*, Lisboa, Editora Relógio d'Água, 1992.

VEEN, Jeroen, BOEKE, Sergei, No Backdoors: Investigating the Dutch Standpoint on Encryption. *Policy & Internet*, 2020, 12.4, pp. 503-524.

VERDELHO, Pedro, A nova lei do Cibercrime, *Scientia Juridica*, LVIII, Braga, 2009.

VERDELHO, Pedro, Cibercrime *In Direito da Sociedade da Informação*, Volume n.º V. Coimbra: Coimbra Editora, 2004. p. 23–64.

WARREN, Samuel D, BRANDEIS, Louis D, *The Right to Privacy,* Harvard Law Review, Vol. 4, N.º 5, Dez. 1890 pp.193-220.

WEIR, George R.S & MASON, Stephen, *Electronic Evidence*, Londres, LexisNexis Butterwoths, 2012.

WOLFLAST, G, Beweisführung durch heimliche Tonbandayfzeichnung, NStZ 1987, p. 103 ss.

ZANELLATO, Marco Antonio, Condutas ilícitas na sociedade digital, Direito e Internet, *Caderno de Escola Superior do Ministério Público de São Paulo*, São Paulo, Ano II, n.o IV, p. 165-228.

JURISPRUDÊNCIA

Tribunal Constitucional

Acórdão do Tribunal Constitucional n.o 128/92, Processo n.o 260/90. Disponível em https://www.tribunalconstitucional.pt/tc/acordaos/19920128.html

Acórdão do Tribunal Constitucional n.o 155/2007 disponível em https://www.tribunalconstitucional.pt/tc/acordaos/20070155.html

Acórdão do Tribunal Constitucional n.o 418/2013, relativo ao Processo n.o 120/2011, de 15/07/2013 disponível em http://www.tribunalconstitucional.pt/tc/acordaos/20130418.html

Acórdão n.o 254/99 do Tribunal Constitucional, Processo n.o 456/97, Disponível em shorturl.at/doyE0

Acórdão Tribunal Constitucional nº 607/2003 Processo nº 594/03 disponível em shorturl.at/ghwxL 339 Acórdão Supremo Tribunal de Justiça n.o886/07.8PSLSB.L1.S1. Disponível em shorturl.at/hrzLP

Supremo Tribunal de Justiça

Acórdão do Supremo Tribunal de Justiça n.o 251/15.3GDCTX.L2.S1 disponível em shorturl.at/hstN7

Acórdão do Supremo Tribunal de Justiça n.o 886/07.8PSLSB.L1.S1. Disponível em www.dgsi.pt

Supremo Tribunal de Justiça. Revista· 941/09.0TVLSB.L1. · 1.a Secção · 21.10.14 Disponível em shorturl.at/dBGK7

Tribunal da Relação de Lisboa

Acórdão do Tribunal da Relação de Lisboa, Processo n.o 581/12.6PLSNT-A.L1-5 de 22-01-2012, Disponível em shorturl.at/huzEZ acesso em 03 de abril de 2020. [51]

Tribunal da Relação de Évora

Acórdão do Tribunal da Relação de Évora, Processo 648/14.6GCFAR-A.E1, de 20-01-2015, disponível em shorturl.at/gtBV4 acesso de 04 de junho de 2020.

Tribunal de Justiça da União Europeia

Tribunal de Justiça da União Europeia no caso *Orkem v. Comissão* de 18 de outubro de 1989.

Suprema Corte dos Países Baixos

HR, 09-02-2021, n.o 19/05471 Disponível em shorturl.at/nsMVW acesso em 06 de setembro 2021