UNIVERSIDADE DE LISBOA

FACULDADE DE DIREITO

A NECESSIDADE DE DESENCRIPTAÇÃO DE SMARTPHONES PARA OBTENÇÃO DE PROVA NO PROCESSO PENAL: Restrições ao Princípio de Não-Autoincriminação na Era Digital

VANESSA FERNANDES

DISSERTAÇÃO DE MESTRADO CIENTÍFICO EM CIÊNCIAS JURÍDICO-CRIMINAIS

LISBOA

2017

UNIVERSIDADE DE LISBOA

FACULDADE DE DIREITO

A NECESSIDADE DE DESENCRIPTAÇÃO DE SMARTPHONES PARA OBTENÇÃO DE PROVA NO PROCESSO PENAL: Restrições ao Princípio de Não-Autoincriminação na Era Digital

VANESSA FERNANDES

Dissertação apresentada para obtenção do Grau de Mestre em Ciências Jurídico-Criminais no Curso de Mestrado Científico da Faculdade de Direito da Universidade de Lisboa.

Orientador: Professor Doutor Paulo de Sousa Mendes

DISSERTAÇÃO DE MESTRADO CIENTÍFICO EM CIÊNCIAS JURÍDICO-CRIMINAIS

LISBOA

2017

Aos meus avós.

A presente dissertação é redigida segundo o antigo acordo ortográfico e método de citação Harvard.

SIGLAS E ABREVIATURAS

AA.VV.	Autores vários
ADN	Ácido Desoxirribonucleico
al.	Alínea
art.º, arts.	artigo, artigos
CEDH	Convenção Europeia dos Direitos do Homem
cf., cfr.	confira, confronte
CP	Código Penal
CPP	Código de Processo Penal
CRP	Constituição da República Portuguesa
EUA	Estados Unidos da América
FBI	Federal Bureau of Investigation
HTC	Hit the Cell
i.e.	id est (isto é)
ID	Identity
MMS	Multimedia Messaging Service
MP	Ministério Público
n.º, n.os	número, números
NSA	National Security Agency
OCDE	Organização de Cooperação e de Desenvolvimento Económico
PIN	Personal Identification Number
pp.	Páginas
RIPA	Regulation of Investigatory Powers Act 2000
séc.	Século
SMS	Short Message Service
StPO	Strafprozessordnung
TEDH	Tribunal Europeu dos Direitos Humanos
v.	Versus
v.g.	verbi gratia (por exemplo)

RESUMO

A implementação da tecnologia de encriptação em smartphones, nomeadamente por palavra-passe ou impressão digital, contribuiu para o aumento da segurança de documentos confidenciais e informações pessoais. O iPhone, por exemplo, assegura aos seus utilizadores, através da digitação da palavra-passe ou do mero toque com o dedo no sensor de impressões digitais, que ninguém terá a possibilidade de aceder aos conteúdos dos seus dispositivos electrónicos.

No entanto, destas vantagens advêm inesperadas implicações legais. Os smartphones são vistos, actualmente, como uma ferramenta indispensável, quer a nível profissional quer a nível pessoal, não só pelas suas inúmeras funcionalidades, mas também devido à sua vasta capacidade de armazenamento de dados (muita das vezes íntimos). E é esta capacidade de armazenamento que faz do smartphone um óptimo repositório de elementos probatórios. De facto, estes dispositivos electrónicos podem ser, ou não, instrumentalizados para a prossecução de finalidades contrárias ao ordenamento jurídico. No entanto, nos casos em que o dispositivo se encontra encriptado, muitas das vezes não resta outra opção às autoridades que não a de pedirem ao arguido que colabore na investigação criminal, levantando questões quanto ao princípio *nemo tenetur se ipsum accusare*.

O princípio contra a autoincriminação evita que o arguido seja transformado em colaborador involuntário das autoridades judiciárias. E, apesar de o arguido estar constitucionalmente protegido no sentido de não auxiliar na sua própria incriminação, situações há em que pode ser compelido a revelar ou a entregar provas que possam contribuir para a sua incriminação.

Mas o que acontece quando o arguido decide encriptar o seu smartphone com recurso a uma palavra-passe alfanumérica e a uma impressão digital? Ambos os métodos são actualmente usados para guardar informação pessoal e privada, sendo merecedores de igual protecção em casos de intrusão por parte do Estado. Será que compelir o arguido a revelar a palavra-passe ou a fornecer a sua impressão digital para desencriptar o seu smartphone deverá accionar o privilégio do arguido contra a autoincriminação? Este trabalho sugere que sim, veremos porquê.

Palavras-chave: smartphones, encriptação, palavra-passe, impressão digital, autoincriminação, proibição de prova.

ABSTRACT

The implementation of encryption technology on smartphones, such as password or fingerprint scanner, has facilitated the increased security of confidential documents and personal information. The iPhone, for example, assures its owner, by typing the password or merely touch his finger to a sensor, that no one else will have the ability to acess the contents of his electronic device.

However, with these advantages come unforeseen legal implications. Currently, smartphones are seen as an indispensable tool, both professionally and personally, not only for its many features but also because of its vast data storage capacity (often intimate data). And it is this storage capacity that makes the smartphone a great repository of evidence. In fact, these electronic devices may, or may not, be instrumentalized for the pursuit of purposes contrary to the legal system. However, in the cases where the device is encrypted, there is often no other choice for the authorities than to ask the defendant to collaborate in the criminal investigation, raising questions about the principle *nemo tenetur se ipsum accusare.*

The privilege against self-incrimination prevents the accused from becoming an involuntary collaborator of the judicial authorities. And although the defendant is constitutionally protected from assisting in his own incrimination, there are situations in which he may be compelled to reveal or deliver evidence that may contribute to his incrimination.

But what happens when the defendant decides to encrypt his smartphone using an alphanumeric password and a fingerprint? Both methods are currently used to guard highly private and personal information, and both are equally deserving of protection from government intrusion. Does compelling the defendant to reveal his password or to provide his fingerprint in order to decrypt the smartphone should trigger the defendant's privilege against self-incrimination? This work suggests that it does, we will see why.

Keywords: smartphones, encryption, password, fingerprint, self-incrimination, exclusionary rules.

INTRODUÇÃO

Propomo-nos fazer uma incursão na temática relativa à articulação entre as ordens de desencriptação de smartphones dirigidas ao arguido e a colaboração processual que lhe é exigível. Assim, pretendemos aferir se, em sede de Direito Processual Penal, o arguido se encontra adstrito a colaborar com as autoridades judiciárias, no sentido de, a pedido destas, facultar a sua impressão digital ou quaisquer palavras-passe que permitam o acesso a dados protegidos que se encontrem armazenados no seu smartphone.

Como se infere com facilidade, a questão *sub judice* apresenta uma matriz dual, prática e teórica, afigurando-se absolutamente compreendida no âmbito de uma indagação prévia geral a que cumpre dar resposta: será que sobre o arguido impende um dever de colaboração com as autoridades judiciárias no âmbito da investigação criminal que a estas compete? Poderá sustentar-se que a existência de um tal dever é, a toda a linha, compatível com o princípio constitucional da não-autoincriminação? Esta será, sem dúvida, a interrogação subjacente que norteará a presente investigação. Cumpre salientar que esta matéria tem sido amplamente discutida pela jurisprudência e doutrina internacionais, nomeadamente pela jurisprudência e doutrina norte-americanas. Neste sentido, mostra-se pertinente fazer remissão, logo desde o ínicio e ao longo da investigação, ao ordenamento jurídico norte-americano.

Esta problemática centra-se no confronto entre o princípio contra a autoincriminação, conhecido também por *nemo tenetur se ipsum accusare*, e os interesses, eminentemente de natureza pública, associados à investigação criminal. Aqui, ainda que se conclua pela inexistência de um princípio geral de colaboração do arguido no quadro da investigação criminal, cumpre determinar se, pontualmente, o Código Penal e o Código de Processo Penal estabelecem, ou não, a prevalência dos interesses prosseguidos pelas autoridades judiciárias sobre as garantias de defesa do arguido. Em caso afirmativo, afigurar-se-á necessário apurar se no que tange ao fornecimento de palavras-passe ou impressões digitais do arguido é, ou não, aplicável um regime de natureza excepcional.

De facto, o princípio contra a autoincriminação já foi alvo de vários estudos, nomeadamente em sede de apresentação de documentos pelo arguido, de concessão de acesso pelo arguido a espaços vedados que se encontrem na sua disponibilidade ou de sujeição a revistas e exames de natureza pericial. No entanto, os dispositivos electrónicos

de armazenamento de dados (*v.g.* smartphone, computador, tablet, etc.) apresentam peculiaridades que os elevam ao estatuto de questão autonomizável. Desde logo, importará referir que estes dispositivos electrónicos, com diversos graus de complexidade, se impuseram no quotidiano do cidadão comum, enquanto ferramentas de trabalho e de lazer. Quer isto significar que, por vezes, ainda que não instrumentalizados para a prossecução de finalidades contrárias ao ordenamento jurídico, aqueles dispositivos encerram em si um conjunto de dados susceptíveis de concorrer para o desenvolvimento da investigação criminal.

Por outro lado, os meios tecnológicos que se encontram actualmente ao dispor da sociedade permitem, com relativa facilidade, a ocultação e protecção de dados, por intermédio da encriptação. Ora, não subsistem quaisquer dúvidas quanto a saber que as dificuldades das entidades judiciárias em aceder aos dados encriptados é proporcional ao grau de sofisticação do método de protecção ou ocultação empregue. Em alguns casos, dir-se-á mesmo que a não colaboração do arguido poderá inquinar decisivamente a investigação, porquanto a desencriptação poderá consumir muito tempo ou até mesmo afigurar-se infrutífera. Como tal, estes dados, não raras vezes da maior relevância para a investigação, são, em muitos casos, extremamente voláteis, pelo que a colaboração do arguido pode ser indispensável para que os mesmos sejam acedidos. Mas não será tal colaboração violadora do princípio contra a autoincriminação? Esta interrogação serve de centro de gravidade para o presente estudo, cujo propósito central consiste em determinar se a ordem de desencriptação dirigida ao arguido, pelas autoridades judiciárias, no sentido de este fornecer a sua impressão digital ou palavra-passe que possibilitam o acesso ao seu smartphone é, ou não, violadora do princípio *nemo tenetur se ipsum accusare*.

Para que possamos dar resposta a esta problemática começaremos, no primeiro capítulo, por analisar a questão à luz do ordenamento jurídico norte-americano. Em primeira linha faremos a apresentação de quatro casos jurisprudenciais relacionados com a coacção, por parte de entidades judiciárias, sobre o arguido/suspeito no sentido de este fornecer a sua palavra-passe ou impressão digital. Posteriormente, indagaremos sobre a temática da desencriptação compelida no âmbito da Constituição dos Estados Unidos da América e perceberemos o motivo pelo qual estas situações chegaram aos tribunais norte-americanos. No entanto, uma vez que a presente investigação é feita em território nacional, cumpre fazer o enquadramento destes casos face ao direito processual penal português. Por esse motivo, decidimos tratar da questão fazendo uma desconstrução

prática do problema, sendo que, a primeira questão que se coloca num caso de desencriptação compelida de um smartphone é a de saber como se processa o acesso e a apreensão dos dados aí armazenados à luz do processo penal português (capítulo II). Depois da tentativa de acesso e apreensão dos dados armazenados no smartphone, de um ponto de vista prático, o segundo obstáculo que se coloca à investigação criminal prende-se com a constatação de que o acesso ao smartphone e a todos os seus ficheiros se encontra protegido por um sistema de encriptação. Assim, mostra-se relevante fazer, num terceiro capítulo, a explicação do que se entende por encriptação e a enunciação dos métodos de encriptação comummente utilizados pelos proprietários de smartphones. Como dissemos, existe uma correlação entre a sofisticação do método utilizado e a dificuldade em aceder ao dispositivo. Desta forma, surge a questão, no capítulo IV, de saber até que ponto o arguido poderá auxiliar as autoridades judiciárias na investigação sem com isso violar o seu direito à não-autoincriminação. Aqui, discutir-se-á se, por um lado, a revelação da palavra-passe é violadora do *nemo tenetur* e se, por outro, o fornecimento da impressão digital é violador do *nemo tenetur*. Por fim, depois de respondermos a esta contenda, cumpre indagar, no capítulo V, quais as consequências da recolha de provas em violação deste princípio constitucional.

CAPÍTULO I – O PROBLEMA DA DESENCRIPTAÇÃO DE SMARTPHONES NO ORDENAMENTO JURÍDICO NORTE-AMERICANO

1. O problema da desencriptação de smartphones na jurisprudência norte-americana

Com a evolução da tecnologia, nasce, em meados dos anos 90, a necessidade de proteger – electronicamente - a confidencialidade dos vários ficheiros que são diariamente armazenados em sistemas electrónicos (nomeadamente, o computador). Mais tarde, esta tendência alarga-se igualmente aos telemóveis ou, mais precisamente, aos smartphones. Um computador ou um smartphone têm, actualmente, uma capacidade de armazenamento de ficheiros considerável, possibilitando que o seu utilizador guarde contactos, e-mails, fotografias, vídeos, entre outros ficheiros de uma maneira fácil e rápida. No entanto, para além de existir esta necessidade, por parte do utilizador comum, de impedir que terceiros possam aceder aos seus ficheiros pessoais, também os criminosos têm idêntica preocupação com a confidencialidade dos elementos relativos aos seus crimes, mormente os que pressupõem sistemas sofisticados de comunicação ou partilha de ficheiros[1].

Atendendo a esta necessidade de confidencialidade, os utilizadores destes dispositivos electrónicos recorrem a chaves criptográficas, compostas pela combinação de dados biométricos com palavras-passe relativamente simples e memorizáveis, garantindo a privacidade das mensagens trocadas ou guardadas, das fotografias, dos vídeos ou de outros ficheiros, contra a intromissão de terceiros. Assim, a efectividade deste método reside na necessidade de colaboração activa e voluntária da pessoa que memorizou o código ou que introduziu os seus dados biométricos.

Tendo em conta que estes códigos criptográficos são, na prática, indecifráveis, surge a questão de saber se, no âmbito de uma investigação criminal e, atendendo ao princípio contra a autoincriminação, será legítimo compelir o arguido a desencriptar o seu dispositivo através da revelação da palavra-passe ou do fornecimento dos seus dados biométricos.

Esta questão já foi abordada em diversos casos nos Estados Unidos da América, pelo que faremos, nos próximos pontos, uma análise da questão na jurisprudência norte-americana.

[1] Oliveira Silva, 2015: 735.

1.1. Caso Commonwealth of Virginia v. David Charles Baust[2]

No dia 19 de Fevereiro de 2014, David Charles Baust, residente em Virginia Beach, Estados Unidos da América, e paramédico de profissão, terá alegadamente estrangulado e agredido a sua namorada no quarto de sua casa[3].

A vítima alegou que o arguido gravou todo o ataque através de um aparelho de gravação de vídeo que estaria sincronizado com o seu telemóvel pessoal, um iPhone 5S, que foi colocado no quarto. Foi ainda relatado pela vítima que, ainda na manhã do dia 19 de Fevereiro de 2014, após ter sido agredida, tentou guardar o aparelho de gravação, no entanto, o arguido, apercebendo-se da situação, voltou a agredi-la[4].

Anteriormente à alegada agressão, David Charles Baust já tinha utilizado o referido sistema de gravação de vídeo ligado ao seu iPhone 5S, enviando por mensagem de texto para a vítima um vídeo onde ambos tinham relações sexuais no quarto do arguido.

No seguimento de um mandado de busca executado diversos dias depois da agressão, foi recolhido da casa do arguido o seu telemóvel pessoal (iPhone 5S), diversos aparelhos de gravação, *flash drives* e um computador.

Tanto a vítima quanto o arguido afirmaram que seria possível que no telemóvel do segundo estivesse armazenada a gravação de vídeo da agressão[5]. No entanto, o acesso ao conteúdo do smartphone ficou impossibilitado, uma vez que o dispositivo se encontrava protegido por palavra-passe e impressão digital. Dada a situação, a acusação apresentou uma moção para a produção compelida da palavra-passe ou da impressão digital que desencriptam o smartphone.

A questão que se colocou em tribunal foi a de saber se seria possível compelir o arguido a fornecer a palavra-passe ou a sua impressão digital sem violar o seu princípio à não-autoincriminação (Quinta Emenda à Constituição dos Estados Unidos da América).

---

[2] Commonwealth of Virginia v. David Charles Baust, 2014. Disponível em: https://consumermediallc.files.wordpress.com/2014/11/245515028-fingerprint-unlock-ruling.pdf [consultado em 22.11.2016]. Pode ser consultado no Anexo I da presente Dissertação.

[3] Hudman, 2015: 213.

[4] Winterbottom, 2014: 1. Disponível em: http://jolt.law.harvard.edu/digest/telecommunications/court-rules-police-may-compel-suspects-to-unlock-fingerprint-protected-smartphones [consultado em 22.11.2016].

[5] Fermino/Feuchtbaum, 2016: 3. Disponível em: http://www.law.com/sites/articles/2016/06/23/the-laws-breakable-protections-for-unbreakable-encryption/ [consultado em 22.11.2016].

A decisão do tribunal foi fraccionada[6]. Por um lado, o juiz Steven Frucci autorizou o pedido da acusação para compelir o arguido a fornecer a sua impressão digital no sentido de desencriptar o seu smartphone, por outro, negou o pedido da acusação para compelir o arguido a fornecer a sua palavra-passe.

No que concerne à argumentação para a decisão, o juiz Steven Frucci começa por analisar a Quinta Emenda à Constituição dos Estados Unidos da América, que estabelece o seguinte: "nenhuma pessoa será obrigada a depor contra si própria em qualquer processo criminal"[7].

A Quinta Emenda concede ao arguido o privilégio contra a autoincriminação. Segundo o juiz, para que a Quinta Emenda seja violada é necessário que a ordem dada ao arguido cumpra três requisitos: a) que seja uma ordem coactiva (*compulsion)* b) de prestação de uma declaração comunicativa (*of a testimonial communication*) c) que seja incriminatória (*that is incriminating*). Quanto ao primeiro e terceiro requisitos parece não haver dúvidas para o douto tribunal, é notório que o pedido de cedência da palavra-passe ou da impressão digital é coactivo e incriminatório. A dúvida surge quanto ao segundo requisito, nomeadamente, quando se questiona se esta cedência da palavra-passe e da impressão digital é ou não uma declaração ou comunicação. É afirmado no caso, pelo juiz Steven Frucci, que um acto é declarativo (*testimonial*) "quando o arguido é forçado a revelar o conhecimento de factos que o relacionam com o delito ou quando tenha de compartilhar os seus pensamentos e crenças com o governo"[8].

Por esse motivo, o tribunal concluiu o seguinte: "O arguido não pode ser obrigado a 'divulgar através de processos mentais' a palavra-passe. No entanto, a impressão digital, como uma chave, não exige que a testemunha divulgue algo através de processos mentais. Pelo contrário, à semelhança das características físicas que são não declarativas ou não comunicativas, a impressão digital do arguido, se utilizada para aceder ao seu smartphone, é igualmente não declarativa ou não comunicativa, não exigindo que o arguido 'comunique qualquer tipo de conhecimento'. Ao contrário da produção de provas de

---

[6] Kerr, 2014: 2. Disponível em: https://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/11/03/virginia-state-trial-court-ruling-on-the-fifth-amendment-and-smart-phones/?utm_term=.399c18bf1a04 [consultado em 22.11.2016].

[7] "*No person shall be compelled in any criminal case to be a witness against himself*".

[8] *"When the accused is forced to reveal his knowlegde of facts relating him to the offense or from having to share his thoughts and beliefs with the government".* Cf. Commonwealth of Virginia v. David Charles Baust, 2014. Disponível em: https://consumermediallc.files.wordpress.com/2014/11/245515028-fingerprint-unlock-ruling.pdf [consultado em 22.11.2016]. Pode ser consultado no Anexo I da presente Dissertação.

carácter físico, tal como uma impressão digital, a revelação de uma palavra-passe força o arguido a 'revelar o conteúdo da sua própria mente'. Por esta razão, a moção para compelir o arguido a revelar a palavra-passe deve ser NEGADA, mas a moção para compelir o arguido a fornecer a sua impressão digital deve ser CONCEDIDA"[9].

Apesar da autorização dada pelo juiz Steven Frucci para compelir o arguido a fornecer a sua impressão digital com o propósito de desbloquear o smartphone apreendido, o acesso ao seu conteúdo acabou por não se realizar, visto que o dispositivo teria estado na posse das entidades judiciárias durante cerca de 6 meses[10] e, ao fim de 48 horas de inactividade, é necessária a palavra-passe para permitir o acesso.

O arguido foi absolvido por falta de provas.

1.2. Caso State of Minnesota v. Matthew Vaughn Diamond[11]

No dia 30 de Outubro de 2014, a vítima M.H. saiu de sua casa, em Chaska, entre as 10:30 e 10:45 da manhã para fazer alguns recados. Quando regressou, cerca das 12:00, encontrou a porta da sua garagem danificada, resultado de um arrombamento forçado. Depois de se aperceber do furto de um cofre, um computador portátil e diversa joalharia, a vítima ligou para a polícia. Enquanto aguardava a chegada da polícia, a vítima encontrou um envelope na entrada da sua garagem com o nome "S.W." escrito. A polícia tirou fotografias ao local e a diversas pegadas que foram deixadas junto à entrada da garagem.

Depois de recorrer à base de dados estatal, a detective Nelson, do Departamento de Polícia de Chaska, conseguiu determinar o número de matrícula do carro de S.W. e, descobriu ainda, que no próprio dia 30, S.W. tinha penhorado as jóias furtadas da casa da vítima numa loja de penhores.

---

[9] "*The defendant cannot be compelled to 'divulge through his mental processes' the passcode for entry. The fingerprint, like a key, however, does not require the witness to divulge anything through his mental processes. On the contrary, like physical characteristics that are non-testimonial, the fingerprint of the Defendant if used to access his phone is likewise non-testimonial and does not require Defendant to 'communicate any knowledge' at all. Unlike the production of physical characteristic evidence, such as a fingerprint, the production of a password forces the Defendant to 'disclose the contents of his own mind'. For this reason the motion to compel the passcode should be DENIED but the motion to compel the fingerprint should be GRANTED*". Cf. Commonwealth of Virginia v. David Charles Baust, 2014. Disponível em: https://consumermediallc.files.wordpress.com/2014/11/245515028-fingerprint-unlock-ruling.pdf [consultado em 22.11.2016]. Pode ser consultado no Anexo I da presente Dissertação.

[10] Pagliery, 2016: 1. Disponível em: http://money.cnn.com/2016/05/12/technology/fbi-fingerprint-iphone/ [consultado em 21.11.2016].

[11] State of Minnesota v. Matthew Vaughn Diamond, 2017. Disponível em: http://mn.gov/law-library-stat/archive/ctappub/2017/OPa152075-011717.pdf [consultado em 23.02.2017]. Pode ser consultado no Anexo II da presente Dissertação.

No dia 4 de Novembro, as autoridades judiciárias localizaram o veículo automóvel de S.W. que, no momento, estava a ser utilizado pelo arguido, Matthew Diamond. O arguido foi detido no momento, uma vez que teria pendente um mandado de detenção relativamente a um outro crime. Ficou detido na prisão de Scott County, onde foram recolhidos os seus pertences: uns sapatos e um smartphone.

Dadas as similitudes entre os sapatos de Matthew Diamond e as pegadas deixadas no local do furto, no dia 6 de Novembro, foi emitido e executado um mandado de busca e apreensão dos sapatos e do smartphone. No dia 12 de Novembro, foi emitido ainda um mandado adicional relativamente à pesquisa de conteúdos armazenados no smartphone de Matthew Diamond. No entanto, o smartphone estava encriptado, pelo que a detective Nelson não conseguiu aceder ao mesmo.

Em Dezembro, o Estado apresentou uma moção para compelir Matthew Diamond a desencriptar o seu smartphone através da leitura da sua impressão digital. Mais tarde, depois de algumas controvérsias relativamente a esta moção, a 11 de Fevereiro, o tribunal de comarca (*district court*) concedeu a ordem de desencriptação do smartphone pedida pelo Estado, atestando que tal ordem estaria justificada por "*probable cause*" e que não entraria em confronto com o privilégio contra a autoincriminação, consagrado na Quinta Emenda à Constituição dos Estados Unidos da América.

Matthew Diamond recusou-se a desencriptar o seu dispositivo electrónico. No dia 3 de Abril, o tribunal de comarca (*district court*) acusou Matthew Diamond de desobediência e informou-o que se colaborasse com a ordem de desencriptação deixaria de ser penalizado por esse crime. O arguido decidiu, por esse motivo, colaborar com as autoridades judiciárias e colocar o dedo no sensor do seu smartphone para conceder o acesso a todos os seus conteúdos.

Depois de terem sido recolhidas provas incriminatórias que relacionavam Matthew Diamond ao crime em questão, o arguido foi condenado por furto em segundo grau, "*misdemeanor theft*" e danos de propriedade em quarto grau. Apesar de o acórdão não esclarecer que tipo de smartphone estaria em causa, dado que o sistema iOS (usado em iPhones) requer a introdução da palavra-passe alfanumérica após 48 horas de inactividade ou após o dispositivo ser desligado, acreditamos que o smartphone do arguido seria de sistema Android.

O tribunal de comarca (*district court*) condenou o arguido a 51 meses de prisão pelo furto em segundo grau e 90 dias de prisão pelos danos causados na propriedade da vítima.

O arguido recorreu para o Tribunal do Estado de Minnesota, alegando que o seu privilégio contra a autoincriminação teria sido violado quando foi compelido a desencriptar o seu smartphone através da leitura da sua impressão digital, fornecendo assim provas autoincriminatórias.

O douto tribunal concluiu que a Quinta Emenda não teria sido violada no caso de Matthew Diamond, uma vez que o privilégio contra a autoincriminação apenas protege o arguido de ser compelido a fornecer elementos probatórios de tipo declarativo (*testimonial*) ou comunicativo (*communicative*), não estando aqui incluída a acção de desencriptar um smartphone através da colocação do dedo num sensor de reconhecimento de impressões digitais.

Desta forma, o Tribunal do Estado de Minnesota não deu provimento ao recurso apresentado pelo arguido, confirmando a sentença dada pelo tribunal de comarca (*district court*).

1.3. Caso Paytsar Bkhchadzhyan[12]

No dia 25 de Fevereiro de 2016, no tribunal de Van Nuys, na Califórnia, Estados Unidos da América, uma cidadã norte-americana, Paytsar Bkhchadzhyan, de 29 anos, foi condenada pelo crime de roubo de identidade (*identity theft*), depois de não ter contestado as acusações[13].

Os registos da detenção e documentos judiciais mostram que, apenas 45 minutos depois de ter sido levada sob custódia, a juíza Alicia Rosenberg, sentada num outro tribunal a cerca de 30 quilómetros de Van Nuys, assinou um mandado[14] autorizando as entidades policiais a compelirem Paytsar Bkhchadzhyan a pressionar o seu dedo no smartphone que fora apreendido durante a sua detenção (um iPhone da marca Apple), com o objectivo de permitir o acesso ao seu conteúdo por parte do FBI, uma vez que o mesmo se encontrava protegido com um método de desbloqueio através de impressão digital e palavra-passe.

[12] O processo pode ser consultado no Anexo III da presente dissertação.
[13] Hamilton/Winton, 2016: 1. Disponível em: http://www.latimes.com/local/california/la-me-iphones-fingerprints-20160430-story.html [consultado em 21.11.2016].
[14] O mandado pode ser consultado no Anexo IV da presente dissertação.

Em menos de 30 minutos um agente do FBI, especializado em cibercrime, deu início à tentativa de desencriptação do smartphone através da impressão digital de Paytsar Bkhchadzhyan.

Os motivos que levaram o FBI a pedir a emissão deste mandado são, até hoje, desconhecidos. O aparelho foi apreendido numa residência em Glendale, na Califórnia, pertencente a Sevak Mesrobian, que seria namorado de Paytsar Bkhchadzhyan e membro de um *gang* arménio, designado de *Armenian Power*[15]. O *gang* era conhecido por perpetrar inúmeros raptos, roubos de identidade, fraude bancária e clonagem de cartões através de pirataria informática.

No mandado pode ler-se o seguinte: "as autoridades judiciárias estão autorizadas a pressionar os dedos da pessoa abrangida por este mandado no sensor de Touch ID do iPhone da Apple apreendido em [...] Glendale, Califórnia 91214 em 25 de Fevereiro de 2016"[16].

Apesar da rápida actuação das entidades policiais ao compelirem Paytsar Bkhchadzhyan a usar todos os seus dez dedos para desbloquear o iPhone, o método revelou-se infrutífero[17].

Confrontados com a impossibilidade de acederem ao conteúdo do smartphone através das impressões digitais de Paytsar Bkhchadzhyan, o FBI decidiu tentar aceder ao aparelho usando um caminho diferente: pedindo a palavra-passe. Mas Paytsar Bkhchadzhyan recusou, alegando que o smartphone não seria seu.

Por este motivo o acesso ao conteúdo do iPhone, alegadamente pertencente a Paytsar Bkhchadzhyan, acabou por não se efectivar.

1.4. Mandado de 9 de Maio de 2016

No dia 9 de Maio de 2016, foi emitido um mandado que autorizava as entidades judiciárias do estado da Califórnia, nos Estados Unidos da América, a efectuar uma busca

[15] Blue, 2016: 3. Disponível em: https://www.engadget.com/2016/05/06/how-armenian-gangsters-blew-up-the-fingerprint-password-debate/ [consultado em 21.11.2016].
[16] "*Law enforcement personnel are authorized to depress the fingerprints and/or thumbprints of the person covered by this warrant onto the Touch ID sensor of the Apple iPhone seized from [...] Glendale, California 91214 on February 25, 2016*". O mandado pode ser consultado no Anexo IV da presente dissertação.
[17] Pagliery, 2016: 1. Disponível em: http://money.cnn.com/2016/05/12/technology/fbi-fingerprint-iphone/ [consultado em 21.11.2016].

a uma residência em Lancaster, na Califórnia[18]. No entanto, para além da busca, foi ainda autorizado que todos os sujeitos que se encontrassem no perímetro da busca fossem compelidos a desencriptarem os seus smartphones através da leitura das suas impressões digitais.

Apesar de o mandado não ter sido tornado público, o *memorandum*[19], assinado pela advogada do Distrito Central da Califórnia, Eileen Decker, teve outro desfecho. No *memorandum* pode ler-se: "O governo submete esta autoridade suplementar, em apoio ao pedido de mandado de busca que solicita a autorização, para recolher as impressões digitais de qualquer pessoa que se encontre nas INSTALAÇÕES DO SUJEITO durante a execução da busca, sobre as quais seja razoavelmente acreditado serem utilizadoras de dispositivos electrónicos com sensor de reconhecimento de impressão digital que se encontrem localizados nas INSTALAÇÕES DO SUJEITO e que estejam abrangidos pelo âmbito de aplicação do mandado"[20].

No entanto, neste caso, não eram apenas as impressões digitais que estavam em causa, uma vez que: "embora o governo não saiba, de antemão, a identidade de cada dispositivo digital ou impressão digital (ou, de facto, qualquer outra prova) que possa ser encontrada durante a busca, ficou demonstrada "*probable cause*" de que essas provas poderiam ser encontradas no local da busca, sendo necessário ganhar e manter o acesso aos dispositivos aí localizados para que seja possível realizar uma pesquisa sobre estes. Por esse motivo, o mandado autoriza a apreensão de palavras-passe, chaves de encriptação e outros dispositivos de acesso que sejam necessários para aceder ao dispositivo"[21].

Como justificação para poderem, por um lado, compelir todos os sujeitos que se encontrassem no perímetro da busca a desencriptarem o seu smartphone através da

[18] Fox-Brewster, 2016: 1. Disponível em: http://www.forbes.com/sites/thomasbrewster/2016/10/16/doj-demands-mass-fingerprint-seizure-to-open-iphones/#46075ff48d9d [consultado em 21.11.2016].
[19] O *memorandum* pode ser consultado no Anexo V da presente dissertação.
[20] "*The government submits this supplemental authority in support of its application for a search warrant which seeks authorization to depress the fingerprints and thumbprints of every person who is located at the SUBJECT PREMISES during the execution of the search and who is reasonably believed by law enforcement to be a user of a fingerprint sensor-enabler device that is located at the SUBJECT PREMISES and falls within the scope of the warrant*". O *memorandum* pode ser consultado no Anexo V da presente dissertação.
[21] "*While the government does not know ahead of time the identity of every digital device or fingerprint (or indeed, every other piece of evidence) that it will find in the search, it has demonstrated probable cause that evidence may exist at the search location, and needs the ability to gain access to those devices and maintain that access to search them. For that reason, the warrant authorizes the seizure of 'passwords, encryption keys, and other access devices that may be necessary to access the device*". Cf. Shaw, 2016: 1. Disponível em: http://www.thenewamerican.com/usnews/constitution/item/24354-doj-gets-warrant-to-force-people-to-use-fingerprints-to-unlock-their-phones [consultado em 21.11.2016].

impressão digital e, por outro, apreender todas as palavras-passe, chaves de encriptação, entre outros meios de desencriptação que se encontrassem no local, o Departamento de Justiça veio alegar que empresas como a Apple, Motorola, HTC e Samsung, entre outras, produzem diversos aparelhos que podem ser desbloqueados pelo utilizador com uma palavra-passe numérica, alfanumérica ou, em alguns aparelhos mais modernos e sofisticados, com a impressão digital através de um sensor[22]. Desta forma, a possibilidade de acesso das entidades judiciárias ao conteúdo dos smartphones sem o auxílio do seu utilizador torna-se extremamente difícil.

Para além deste reforço na segurança destes dispositivos, foram ainda criados alguns limites ao desbloqueio dos smartphones. O Departamento de Justiça dá o exemplo do iPhone da Apple, que após 5 tentativas de desbloqueio através da leitura da impressão digital requer palavra-passe. Além desta característica, o iPhone têm ainda a vantagem, ou desvantagem, de, após 48 horas de inactividade, necessitar obrigatoriamente da palavra-passe (e não apenas da impressão digital) para desbloquear.

É com base nestas circunstâncias que o Departamento de Justiça justifica a necessidade e a urgência da coacção dos sujeitos no sentido de desencriptarem os dispositivos através da leitura das suas impressões digitais.

O Departamento de Justiça finaliza o *memorandum* afirmando que este mandado não viola nem a Quarta nem a Quinta Emenda à Constituição dos Estados Unidos da América.

1.5. Conclusões intermédias

Depois da leitura dos quatro casos apresentados, podemos concluir que, em todos eles, a palavra-passe e a impressão digital parecem ter um tratamento diferenciado. Se, por um lado, a revelação da palavra-passe parece estar protegida pela Quinta Emenda à Constituição dos Estados Unidos da América, por outro, a impressão digital, por não se tratar de uma declaração/comunicação do arguido, parece não ter qualquer tipo de protecção contra a autoincriminação.

Para percebermos em maior detalhe esta diferenciação e o motivo pelo qual estas questões chegaram à jurisprudência norte-americana, cumpre analisar a protecção conferida pela Quinta Emenda à Constituição dos Estados Unidos da América.

[22] Vaas, 2016: 3. Disponível em: https://nakedsecurity.sophos.com/2016/10/18/feds-got-search-warrant-demanding-anyones-fingerprints-to-open-phones/ [consultado em 21.11.2016].

2. O problema da desencriptação de smartphones na Constituição dos Estados Unidos da América

Qualquer caso de desencriptação compelida dirigida ao arguido, seja através da revelação da palavra-passe, seja através da leitura da impressão digital, gera problemas quanto ao princípio da não-autoincriminação.

Segundo este princípio, o arguido não deverá colaborar com as autoridades judiciárias no sentido de auxiliar na sua própria incriminação. Assim, coloca-se a questão: estará o arguido a violar, segundo o ordenamento jurídico norte-americano, o seu direito à não-autoincriminação quando obedece a estas ordens de desencriptação?

Uma análise à Constituição norte-americana, nomeadamente à sua Quinta Emenda, ajudar-nos-á a obter uma resposta.

2.1. A Quinta Emenda à Constituição dos Estados Unidos da América e a necessidade de desencriptação de smartphones com o auxílio do arguido

A Quinta Emenda à Constituição dos Estados Unidos da América estabelece o seguinte: "Nenhuma pessoa será obrigada a responder por um crime capital ou infame, salvo por denúncia ou pronúncia de um grande júri, excepto quando se trate de casos que, em tempo de guerra ou de perigo público, ocorram nas forças terrestres ou navais, ou na milícia, quando em serviço activo; nenhuma pessoa será, pelo mesmo crime, submetida duas vezes a julgamento que possa causar-lhe a perda da vida ou de algum membro; nem será obrigada a depor contra si própria em processo criminal ou ser privada da vida, liberdade ou propriedade sem processo legal regular; a propriedade privada não será desapropriada para uso público sem justa indemnização"[23]. Do texto retiramos a seguinte frase: "Nenhuma pessoa será […] obrigada a depor contra si própria em processo criminal […]".

2.1.1. Requisitos da Quinta Emenda

Da Quinta Emenda podemos extrair a defesa do brocardo latino *nemo tenetur se ipsum accusare*, ou seja, o princípio de não-autoincriminação. O princípio protege o arguido "de

[23] "*No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offence to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation".*

ser chamado a testemunhar contra si próprio no seu próprio julgamento e permite que recuse responder a perguntas oficiais que possam incriminá-lo em futuros processos, sejam eles civis ou criminais, formais ou informais"[24]. Na doutrina norte-americana é igualmente defendido que este princípio tem ainda como finalidade proteger o arguido do "*cruel trilemma*"[25] de ter de escolher entre: a) fornecer provas incriminadoras contra si próprio, arriscando ser alvo de uma acção criminal; b) mentir às autoridades judiciárias e judiciais sob o risco de cometer perjúrio; c) manter o silêncio e incorrer em desobediência[26].

No entanto, o princípio vertido na Quinta Emenda não é absoluto[27], para que seja reivindicado é necessário, como já tivemos oportunidade de salientar, ainda que sucintamente, na exposição do caso Baust, que estejam verificados três requisitos distintos[28]: a) coacção (*compulsion*); b) incriminação (*incrimination*); c) declaração/comunicação (*testimony/communication*)[29]. É ainda necessário que estes requisitos sejam comprovados cumulativamente. Assim, o governo pode compelir o arguido a autoincriminar-se desde que a autoincriminação não seja declarativa ou comunicativa[30]. Semelhantemente, o arguido pode autoincriminar-se através do fornecimento de um testemunho, no entanto, se o fizer sem a coacção das entidades judiciárias não poderá reivindicar o seu privilégio contra a autoincriminação[31]. O governo

[24] "*From being called to testify against himself at his own trial and permits him to refuse to answer official questions put him in any other proceeding, civil or criminal, formal or informal, where the answers might incriminate him in future criminal proceedings*" Cf. Minnesota v. Murphy, 1984. Disponível em: https://supreme.justia.com/cases/federal/us/465/420/case.html [consultado em 24.11.2016].
[25] Cauthen, 2016: 5.
[26] Thompson II/Jaikaran, 2016: 6-7.
[27] Engel, 2012: 105-106.
[28] "*It is also clear that the Fifth Amendment does not independently proscribe the compelled production of every sort of incriminating evidence but applies only when the accused is compelled to make a Testimonial Communication that is* incriminating". Cf. Fisher v. United States, 1976. Disponível em: https://supreme.justia.com/cases/federal/us/425/391/case.html [consultado em 24.11.2016].
[29] Allen/Mace, 2004: 246.
[30] Cf. Fisher v. United States, 1976. Disponível em: https://supreme.justia.com/cases/federal/us/425/391/case.html [consultado em 24.11.2016]; Schmerber v. California, 1966. Disponível em: https://supreme.justia.com/cases/federal/us/384/757/case.html [consultado em 24.11.2016]; "*But the prohibition of compelling a man in a criminal court to be witness against himself is a prohibition of the use of physical or moral compulsion to extort communications from him, not an exclusion of his body as evidence when it may be material. The objection in principle would forbid a jury to look at a prisioner and compare his features with a photograph in proof. Moreover, we need not consider how far a court would go in compelling a man to exhibit himself. For when he is exhibited, whether voluntarily or by order, and even if the order goes too far, the evidence, if material, is competent*". Cf. Holt v. United States, 1910. Disponível em: https://supreme.justia.com/cases/federal/us/218/245/case.html [consultado em 24.11.2016].
[31] Cf. Fisher v. United States, 1976. Disponível em: https://supreme.justia.com/cases/federal/us/425/391/case.html [consultado em 24.11.2016]; United States

pode ainda compelir o arguido a prestar um depoimento desde que este não culmine na sua incriminação[32].

Os primeiros dois requisitos, em matéria de desencriptação de smartphones com o auxílio do arguido, não trazem grandes dúvidas. Em contrapartida, na maior parte dos casos sobre esta temática, o problema de saber se o fornecimento de palavra-passe ou de impressão digital para desencriptar um smartphone se inclui ou não na categoria de declaração/comunicação gera várias questões.

2.1.1.1. Coacção (*compulsion*)

Para o preenchimento do requisito da coacção (*compulsion*), terá de se verificar uma pressão por parte do governo, sobre o arguido, no sentido de o obrigar a divulgar algum tipo de informação[33]. A jurisprudência norte-americana vai mais longe, chegando a afirmar que é necessário, para responder afirmativamente ao teste da coacção, apurar, perante todas as circunstâncias do caso, se o livre arbítrio do arguido foi reprimido[34]. Essencialmente, os tribunais devem decidir se o depoimento é prestado de forma livre e esclarecida[35] ou, contrariamente, se foi obtido através do uso de influência imprópria[36]. Na circunstância de se confirmar esta última situação, a jurisprudência norte-americana já se fez ouvir no sentido de considerar esta coacção como uma "extorsão de informações do acusado ofensiva ao senso de justiça"[37].

2.1.1.2. Incriminação (*incrimination*)

No que concerne ao requisito da incriminação, para que este se verifique, é necessário que o acto incrimine o arguido ou leve à descoberta de provas incriminatórias[38]. Os

---

v. Doe, 1984. Disponível em: https://supreme.justia.com/cases/federal/us/465/605/ [consultado em 24.11.2016].

[32] Jarone, 2015: 771.

[33] Morrison, 2012: 144.

[34] Cf. United States v. Washington, 1977. Disponível em: https://supreme.justia.com/cases/federal/us/431/181/case.html [consultado em 24.11.2016].

[35] Se um documento é escrito e entregue às entidades judiciárias voluntariamente, o requisito da coacção não se irá verificar. No entanto, se o governo intimar o arguido a produzir o mesmo documento, o requisito da coacção passa a estar preenchido. Cf. Jarone, 2015: 772.

[36] Wilson, 2015: 24.

[37] "*Extortion of information from the accused himself as offensive to our sense of justice*". Cf. Couch v. United States, 1973. Disponível em: https://supreme.justia.com/cases/federal/us/409/322/ [consultado em 24.11.2016].

[38] Cf. Kastigar v. United States, 1972. Disponível em: https://supreme.justia.com/cases/federal/us/406/441/case.html [consultado em 24.11.2016]. United States v. Hubbel, 2000. Disponível em: https://supreme.justia.com/cases/federal/us/530/27/case.html [consultado em 24.11.2016]. "*The privilege afforded not only extends to answers that would in themselves support a*

tribunais devem, desta forma, determinar se a revelação do testemunho gera um risco substancial de autoincriminação, ou se expõe de qualquer outra forma o sujeito a uma acusação criminal[39]. Para além desta exigência é ainda imprescindível, para a verificação do requisito em causa, que o sujeito se autoincrimine. Assim, se o depoimento do arguido incriminar apenas terceiros, o requisito da incriminação não se verificará[40]. O arguido não se pode apoiar na protecção conferida pela Quinta Emenda para alegar que um terceiro será incriminado com o seu testemunho[41]. Desta forma, o requisito da (auto)incriminação poderá permitir que arguidos invoquem a protecção conferida pela Quinta Emenda no sentido de não fornecerem as suas palavras-passe ou impressões digitais, no entanto, impede que terceiros recorram à mesma protecção quando são compelidos a fornecerem palavras-passe ou impressões digitais dos suspeitos[42].

2.1.1.3. Declaração/comunicação (*testimony/communication*)

Resta-nos tecer algumas considerações sobre o terceiro e último requisito: declaração/comunicação (*testimony/communication*). De um ponto de vista mais científico, declaração significa cognição substantiva, ou seja, é o produto da cognição que resulta da realização ou afirmação de proposições de valor autêntico[43]. Desta forma, pode ser entendida como a revelação coactiva, causada pelo Estado, dos resultados substantivos incriminatórios da sua cognição[44][45]. De uma outra perspectiva, podemos definir a prova declarativa (*testimonial evidence*) como sendo uma prova reveladora de ideias, informações, dados, conceitos, conhecimentos e pensamentos.

Tipicamente estas revelações são feitas através de comunicações escritas ou orais, no entanto, nada impede que sejam feitas igualmente através de actos, condutas e gestos,

---

conviction under a federal criminal statute but likewise embraces those which would furnish a link in the chain of evidence needed to prosecute the claimant for a federal crime". Cf. Hoffman v. United States, 1951. Disponível em: https://supreme.justia.com/cases/federal/us/341/479/case.html [consultado em 24.11.2016].

[39] "*The suspect must be faced with substancial and real hazards of self-incrimination*". Cf. United States v. Reis, 1985. Disponível em: https://www.ravellaw.com/opinions/35b1b3165aed24221933677a50da6059 [consultado em 24.11.2016]. Hale v. Henkel, 1906. Disponível em: https://supreme.justia.com/cases/federal/us/201/43/case.html [consultado em 24.11.2016].

[40] Jarone, 2015: 773.

[41] Cf. Hale v. Henkel, 1906. Disponível em: https://supreme.justia.com/cases/federal/us/201/43/case.html [consultado em 24.11.2016]. Fisher v. United States, 1976. Disponível em: https://supreme.justia.com/cases/federal/us/425/391/case.html [consultado em 24.11.2016].

[42] Wilson, 2015: 25.

[43] Allen/Mace, 2004: 267.

[44] A cognição involve aquisição, armazenamento, recuperação e uso do conhecimento. Cf. Matlin/Farmer, 2015: 26.

[45] Allen/Mace, 2004: 267-268.

desde que estes, por sua vez, revelem factos, pensamentos, crenças e/ou conhecimento de factos. A título de exemplo, acenar com a cabeça para cima e para baixo quando é perguntado "foste tu que o fizeste?" transmite uma resposta afirmativa. Apontar para o roupeiro quando é perguntado "onde está a arma?" transmite conhecimento sobre o paradeiro da arma, conhecimento sobre a sua localização e acesso[46]. Por fim, existe ainda quem defenda que a prova declarativa (*testimonial evidence*) pode ser entendida como a comunicação de informação através da memória ou do conhecimento do arguido[47].

No que respeita à jurisprudência, o Supremo Tribunal dos Estados Unidos da América, definiu que um acto compelido pode ser considerado como declarativo se, explícita ou implicitamente, divulgar uma afirmação factual ou qualquer tipo de informação[48]. No entanto, o acto tem que fazer mais do que apenas revelar informações, deve envolver, igualmente, a divulgação compelida do conteúdo da mente do arguido[49]. Neste sentido, o Supremo Tribunal chega mesmo a afirmar que "é a extorsão de informação do acusado, a tentativa de forçá-lo a revelar o conteúdo da sua própria mente, que implica a Cláusula de Autoincriminação"[50].

Por este motivo, não causa estranheza que no caso United States v. Kirschner[51], quando as autoridades judiciárias compeliram o arguido a fornecer a palavra-passe do seu computador encriptado, o tribunal tenha decidido que o fornecimento da palavra-passe seria semelhante ao acto de fornecer a combinação de um cofre, pelo que seria considerado como uma comunicação declarativa (*testimonial communication*) violadora da Quinta Emenda[52]. Semelhantemente, no caso United States v. Doe (Doe III)[53], o tribunal decidiu no sentido de que "tanto a produção como a desencriptação do disco rígido exigiriam o recurso ao conteúdo da mente do suspeito, não podendo ser justamente

[46] Cauthen, 2016: 6.
[47] Dripps, 2005: 335.
[48] Doe v. United States, 1988. (Doe II) Disponível em: https://supreme.justia.com/cases/federal/us/487/201/ [consultado em 25.11.2016].
[49] *"[…] it must also involve some compelled use of the contents of the suspect's mind".* Cf. Allen/Mase, 2004: 246.
[50] "*It is the extortion of information from the accused, the attempt to force him to disclose the contents of his own mind, that implicates the Self-Incrimination Clause*". Cf. Doe v. United States, 1988. (Doe II) Disponível em: https://supreme.justia.com/cases/federal/us/487/201/ [consultado em 25.11.2016].
[51] United States v. Kirschner, 2010. Disponível em: https://www.ravellaw.com/opinions/789d10be33066b73e4377a26bf5c574a [consultado em 25.11.2016].
[52] Bales, 2012: 1302.
[53] United States v. Doe, 2011. (Doe III) Disponível em: http://law.justia.com/cases/federal/appellate-courts/F3/112/910/585109/ [consultado em 25.11.2016].

caracterizada como um acto físico que seria não declarativo por natureza"[54]. O tribunal acabou por concluir que o arguido invocou correctamente o seu privilégio contra a autoincriminação, sendo que não poderia ser compelido a produzir ou desencriptar (através de palavra-passe) as *hard drives* do seu computador.

Na esteira do defendido pela jurisprudência, também a doutrina norte-americana, na sua grande maioria, é apoiante da tese de que o fornecimento de palavra-passe para a desencriptação de um smartphone é um acto declarativo (*testimonial*) por natureza, uma vez que obriga o arguido a divulgar o conteúdo da sua mente[55].

Ainda assim, alguns tribunais têm uma abordagem diferente relativamente a esta temática. Para evitar violar a Quinta Emenda ao compelir o arguido a fornecer a palavra-passe, alguns tribunais optaram por compelir o arguido a fornecer o próprio dispositivo já desencriptado sem revelar a palavra-passe a qualquer entidade judiciária[56]. Esta opção é também defendida por alguma doutrina minoritária, nomeadamente, Orin Kerr, Dan Terzian[57] e Anna Bodi[58]. O primeiro Autor chega mesmo a reiterar que "desta forma, o governo recebe o telefone desbloqueado, mas nunca é revelada a palavra-passe. Pedir ao arguido que digite ele próprio a palavra-passe minimizaria as implicações da Quinta Emenda, uma vez que não envolveria a revelação potencialmente incriminatória da palavra-passe"[59].

Em contrapartida, no que diz respeito às provas não declarativas (*non-testimonial*), importa ter presente que o Supremo Tribunal dos Estados Unidos da América começou por fazer a distinção entre provas físicas e provas comunicativas para diferenciar, por sua vez, entre as provas declarativas (*testimonial*) e não declarativas (*non-testimonial*). O

---

[54] "*Both the production and decryption of the hard drives would require the use of the contents of the suspect's mind and could not be fairly characterized as a physical act that would be non-testimonial in nature*". Cf. United States v. Doe, 2011. (Doe III) Disponível em: http://law.justia.com/cases/federal/appellate-courts/F3/112/910/585109/ [consultado em 25.11.2016].

[55] "*Proving a password could also implicate the cruel trilemma.*" Cf. Bales, 2012: 1304. Atwood, 2015: 413-415. "*The act of decryption and production would be testimonial*" Cf. Ajello, 2015: 454-457.

[56] In re Grand Jury Subpoena to Sebastien Boucher, 2009. Disponível em: http://volokh.com/files/BoucherDCT.1.pdf [consultado em 25.11.2016].

[57] Terzian, 2016: 170-174.

[58] Bodi, 2015: 2-4. Disponível em: http://www.americancriminallawreview.com/aclr-online/phones-fingerprints-and-fifth-amendment/ [consultado em 28.11.2016].

[59] "*That way the government gets the unlocked phone but never gets the passcode. Having the defendant enter his passcode would minimize the Fifth Amendment implications of the compelled compliance, as it would not involve disclosing the potentially incriminating evidence of the passcode itself*". Cf. Kerr, 2014: 2-3. Disponível em: https://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/11/03/virginia-state-trial-court-ruling-on-the-fifth-amendment-and-smart-phones/?utm_term=.399c18bf1a04 [consultado em 28.11.2016].

primeiro caso a fazer a distinção entre provas físicas e comunicativas foi o caso Holt v. United States[60], onde a coacção de um prisioneiro a vestir uma camisa para que a testemunha o conseguisse identificar foi considerada como não sendo violadora da Quinta Emenda[6162]. Mas foi com o caso Schmerber v. California que este entendimento foi expandido no sentido de incluir outras formas de obtenção de prova através do corpo do arguido, nomeadamente, recolha de sangue, amostra de caligrafia e exames através do ar expirado.

No caso Schmerber v. California[63], o arguido alegou que o seu privilégio contra a autoincriminação fora violado uma vez que a polícia teria instruído um médico a recolher uma amostra de sangue do seu corpo sem o seu consentimento[64]. A amostra foi analisada com o desígnio de descobrir se o arguido teria álcool no sangue depois de ter sido detido por condução sob o efeito de álcool[65].

O Supremo Tribunal vem considerar, actualmente, como provas não declarativas (*non-testimonial evidence*) todas as provas utilizadas com o propósito de identificar pessoas e de correlacioná-las com o crime investigado, tais como: impressões digitais, sangue, urina, ADN, amostras de cabelo, amostras de caligrafia, *lineups*, entre outras[6667]. Isto porque nenhuma destas provas físicas obriga a que o arguido divulgue qualquer tipo de conhecimento[68].

---

[60] Holt v. United States, 1910. Disponível em: https://supreme.justia.com/cases/federal/us/218/245/case.html [consultado em 28.11.2016].

[61] "*The prohibition of compelling a man in a criminal court to be a witness against himself is a prohibition of the use of physical or moral compulsion to extort communications from him, not an exclusion of his body as evidence when it may be material*". Cf. Holt v. United States, 1910. Disponível em: https://supreme.justia.com/cases/federal/us/218/245/case.html [consultado em 28.11.2016].

[62] Desta forma, segundo o entendimento do Supremo Tribunal, a coacção de "*bodily evidence*" nunca será violadora da Quinta Emenda. Cf. Goldman, 2015: 217.

[63] Cf. Schmerber v. California, 1966. Disponível em: https://supreme.justia.com/cases/federal/us/384/757/case.html [consultado em 28.11.2016].

[64] "*The privilege protects an accused only from being compelled to testify against himself, or otherwise provide the State with evidence of a testimonial or communicative nature.*" Cf. Schmerber v. California, 1966. Disponível em: https://supreme.justia.com/cases/federal/us/384/757/case.html [consultado em 28.11.2016].

[65] Sales, 2014: 199-200.

[66] Fakhoury, 2012: 82. Silver, 2012: 811. Farahany, 2012: 356-357.

[67] Cf. United States v. Doe, 1984. Disponível em: https://supreme.justia.com/cases/federal/us/465/605/ [consultado em 28.11.2016]. United States v. Wade, 1967. Disponível em https://supreme.justia.com/cases/federal/us/388/218/case.html [consultado em: 28.11.2016]. United States v. Dionisio, 1973. Disponível em: https://supreme.justia.com/cases/federal/us/410/1/case.html [consultado em 28.11.2016]. Gilbert v. California, 1967. Disponível em: http://supreme-court-cases.insidegov.com/l/2630/Gilbert-v-California [consultado em 28.11.2016]. Schmerber v. California, 1966. Disponível em: https://supreme.justia.com/cases/federal/us/384/757/case.html [consultado em 28.11.2016].

[68] Palfreyman, 2009: 354-355.

Também a grande maioria da doutrina norte-americana segue o entendimento de que a Quinta Emenda não protege o arguido contra o fornecimento de provas físicas[69] ou atributos identificadores[70].

Deste modo, podemos reiterar que, segundo o entendimento da jurisprudência norte-americana, nomeadamente do Supremo Tribunal, e da maioria da doutrina, a diferença entre um acto declarativo (*testimonial*) e um acto não declarativo (*non-testimonial*) reside no facto de o primeiro exigir que o arguido faça uso do conteúdo da sua mente e o segundo não[71].

Uma vez que o tema central da nossa dissertação prende-se com a desencriptação de smartphones, nomeadamente, através de impressão digital, mostra-se relevante, nesta sede, tecer algumas reflexões sobre a possibilidade de considerarmos esta conduta como declarativa (*testimonial*) ou não declarativa (*non-testimonial*).

Pela parte da jurisprudência norte-americana, podemos obter uma rápida resposta através da análise dos casos apresentados no início da presente dissertação. Tendo em consideração o resultado do caso Baust e do caso Diamond, e a argumentação apresentada pela jurisprudência nos restantes casos, torna-se clara a sua tendência no sentido de considerar o fornecimento de impressão digital para a desencriptação de um smartphone como um acto não declarativo (*non-testimonial*).

No que à doutrina diz respeito, o entendimento da grande maioria dos Autores vai de encontro ao defendido pela jurisprudência: afirmando que as impressões digitais podem ser compelidas sem violação da Quinta Emenda, contrariamente às palavras-passe. Albert Gidari defende a ideia de que na leitura da impressão digital do arguido, "contrariamente à revelação de palavras-passe, não há coacção para comunicar ou dizer o que 'vai na cabeça' às autoridades judiciárias. 'Coloque o seu dedo aqui' não é um acto declarativo ou autoincriminador"[72]. Na mesma esteira, Riana Pfefferkorn afirma que "de facto, é preocupante pensar que as autoridades judiciárias podem acabar por usar contra o arguido uma decisão que este tomou por conveniência e para tornar mais difícil o acesso de

[69] Bonin, 1996: 509.
[70] Colarusso, 2011: 134.
[71] Jarone, 2015: 774.
[72] "U*nlike disclosing passcodes, you are not compelled to speak or say what's in 'your mind' to law enforcement. 'Put your finger here' is not testimonial or self-incriminating*". Cf. Hamilton/Winton, 2016: 2. Disponível em: http://www.latimes.com/local/california/la-me-iphones-fingerprints-20160430-story.html [consultado em 28.11.2016].

terceiros ao seu telefone sem o seu conhecimento. No entanto, não acredito que isto vá contra a Quinta Emenda"[73]. Por seu turno, Sarah Wilson, apoiando-se no entendimento da jurisprudência, afirma que "o governo poderia exigir a desencriptação por dados biométricos sem implicar a Quinta Emenda uma vez que o Supremo Tribunal decidiu que os dados biométricos não são declarativos"[74]. Por fim, acompanha ainda este pensamento George Dery III, que reitera a ideia de que a impressão digital deve ser vista em similitude com uma chave de um cofre, sustentando ainda que "mesmo que seja problemático pensar na possibilidade de alguém aceder ao telefone do arguido, as autoridades judiciárias têm autorização de um juiz e isso significa que existe a probabilidade de estarmos perante uma actividade criminosa"[75].

Há ainda que salientar duas ideias que são unanimemente defendidas, tanto pela jurisprudência quanto pela doutrina norte-americana: a primeira prende-se com a necessidade de mandado judicial para a apreensão de um smartphone[76], a segunda tem que ver com a concepção de que as autoridades judiciárias podem compelir o arguido detido a fornecer provas físicas, incluindo impressões digitais, sem autorização judicial[77], com o propósito de auxiliar à sua identificação ou de possibilitar a sua ligação com o local do crime.

2.1.2. Limites da Quinta Emenda

Chegados a este ponto, e depois de analisados os três requisitos da Quinta Emenda à Constituição dos Estados Unidos da América, cumpre esclarecer que mesmo que as entidades judiciárias compelissem o arguido a prestar um depoimento ou testemunho incriminatório (nomeadamente a palavra-passe do seu smartphone), preenchendo assim os três requisitos mencionados, poderíamos estar aqui perante uma conduta não violadora

[73] "*To be sure, it's troubling to think that the police could end up using against you a choice you made for the sake of convenience and to make it harder for someone to snoop into your phone without your knowledge. But I don't think it runs counter to the Fifth Amendment*". Cf. Farivar, 2016: 2. Disponível em: http://arstechnica.com/tech-policy/2016/05/should-the-govt-be-able-to-force-you-to-open-your-phone-with-just-your-fingerprint/ [consultado em 28.11.2016].

[74] "*The government could demand biometric passwords without implicating the Fifth Amendment because the Supreme Court has decided that biometrics are not testimonial".* Cf. Wilson, 2015: 28.

[75] "*Even though it is a big deal having someone open up their phone, they've gone to a judge and it means there's a likelihood of criminal activity*". Cf. Hamilton/Winton, 2016: 3. Disponível em: http://www.latimes.com/local/california/la-me-iphones-fingerprints-20160430-story.html [consultado em 28.11.2016].

[76] Cf. Riley v. California, 2014. Disponível em: https://www.supremecourt.gov/opinions/13pdf/13-132_8l9c.pdf [consultado em 28.11.2016].

[77] Cf. Holt v. United States, 1910. Disponível em: https://supreme.justia.com/cases/federal/us/218/245/case.html [consultado em 28.11.2016].

do princípio *nemo tenetur se ipsum accusare*, por duas vias[78]: se as informações prestadas fossem uma conclusão inevitável (*foregone conclusion*); ou se o governo concedesse imunidade ao arguido[79].

2.1.2.1. Conclusão inevitável (*foregone conclusion*)

Segundo a doutrina da conclusão inevitável (*foregone conclusion*), se o governo conseguir mostrar, com razoável particularidade, que no momento em que pretende compelir a produção de determinada prova já terá em sua posse informações relativas à sua existência e localização, o arguido acrescentará, através do seu testemunho, pouco ou nada a essa informação, pelo que, a coacção será legítima de acordo com a Quinta Emenda[80]. Uma vez que a comunicação de uma conclusão inevitável não revela, de facto, nenhuma informação nova, o privilégio contra a autoincriminação não opera, independentemente de estarmos ou não perante uma prova declarativa (*testimonial evidence*).

A jurisprudência norte-americana desenvolveu um teste de três passos para a aplicação da excepção da conclusão inevitável[81]. Assim, o governo deve estabelecer o seu conhecimento sobre: a) a existência da prova exigida; b) a posse e o controlo dessa prova pelo arguido; c) a autenticidade da prova[82].

Esta doutrina foi mencionada pela primeira vez no caso Fisher v. United States[83], onde o Supremo Tribunal alegou que a entrega de documentos relativos ao pagamento de impostos pelo contribuinte não constituiria um depoimento incriminatório, uma vez que a existência e localização dos documentos eram uma conclusão inevitável[84]. Assim, o contribuinte não iria acrescentar nada à informação já recolhida pelo governo pelo simples facto de admitir que tinha a documentação em sua posse[85].

---

[78] Terzian, 2015: 1134.
[79] Soares, 2012: 2004.
[80] Soares, 2012: 2006.
[81] Werner, 2016: 4.
[82] Efectivamente, apesar de a prestação de depoimento ter, geralmente, um aspecto declarativo, se o governo conseguir mostrar que tinha conhecimento prévio da existência, posse e autenticidade da informação, a informação declarativa passa a ser uma conclusão inevitável. Cf. Fruiterman, 2013: 658. Sales, 2014: 203.
[83] Cf. Fisher v. United States, 1976. Disponível em: https://supreme.justia.com/cases/federal/us/425/391/case.html [consultado em 28.11.2016].
[84] *"The government can compel production when the existence and location of documents are a foregone conclusion and the defendant adds little to nothing to the sum total of the government's information by conceding that he in fact has the papers*". Cf. Mohan/Villasenor, 2012: 14.
[85] Sales, 2014: 203.

A doutrina da conclusão inevitável tem sido igualmente considerada como uma justificação legal viável nos casos de desencriptação de dispositivos electrónicos[86]. Alguns tribunais requerem que o governo tenha conhecimento sobre um certo ficheiro[87] para que a doutrina da conclusão inevitável seja aplicada, outros exigem apenas que o governo tenha acesso a qualquer tipo de informação sobre determinados ficheiros[88], mesmo que não esteja informado sobre o seu conteúdo, dado que se encontram encriptados[89]. Quatro tribunais, em quatro casos distintos, aprovaram a desencriptação compelida de dispositivos electrónicos com base na doutrina da conclusão inevitável[90]: a) caso United States v. Gavegnano[91]; b) caso United States v. Fricosu[92]; c) caso United States v. Hatfield[93]; d) caso In re Grand Jury Subpoena to Sebastien Boucher[94].

Num caso relativamente recente, Commonwealth v. Gelfgatt[95], o tribunal decidiu que o arguido poderia ser compelido a fornecer a palavra-passe do seu computador com base na doutrina da conclusão inevitável. Visto que a posse e o controlo do computador por parte do arguido e o seu conhecimento sobre a encriptação e a respectiva palavra-passe já eram conhecidos pelo governo, o Supremo Tribunal de Massachusetts concluiu que o fornecimento da palavra-passe, neste caso, seria considerado como conclusão inevitável, não estando assim protegido pelo privilégio concedido pela Quinta Emenda[96].

---

[86] Silver, 2012: 811.

[87] Cf. In re Grand Jury Subpoena to Sebastien Boucher, 2009. Disponível em: http://volokh.com/files/BoucherDCT.1.pdf [consultado em 28.11.2016]. Commonwealth of Virginia v. David Charles Baust, 2014. Disponível em: https://consumermediallc.files.wordpress.com/2014/11/245515028-fingerprint-unlock-ruling.pdf [consultado em 28.11.2016]. Pode ser consultado no Anexo I da presente Dissertação.

[88] Cf. United States v. Fricosu, 2012. Disponível em: https://www.wired.com/images_blogs/threatlevel/2012/01/decrypt.pdf [consultado em 28.11.2016]. Commonwealth v. Gelfgatt, 2014. Disponível em: http://law.justia.com/cases/massachusetts/supreme-court/2014/sjc-11358.html [consultado em 28.11.2016].

[89] Terzian, 2016: 173.

[90] Silver, 2012: 811.

[91] Cf. United States v. Gavegnano, 2012. Disponível em: http://federalevidence.com/pdf/Comput/U.S.%20v.%20Gavegnano.pdf [consultado em 28.11.2016].

[92] Cf. United States v. Fricosu, 2012. Disponível em: https://www.wired.com/images_blogs/threatlevel/2012/01/decrypt.pdf [consultado em 28.11.2016].

[93] Cf. United States v. Hatfield, 2010. Disponível em: http://caselaw.findlaw.com/us-7th-circuit/1519786.html [consultado em 28.11.2016].

[94] Cf. In re Grand Jury Subpoena to Sebastien Boucher, 2009. Disponível em: http://volokh.com/files/BoucherDCT.1.pdf [consultado em 28.11.2016].

[95] Cf. Commonwealth v. Gelfgatt, 2014. Disponível em: http://law.justia.com/cases/massachusetts/supreme-court/2014/sjc-11358.html [consultado em 28.11.2016].

[96] Wilson, 2015: 26.

2.1.2.2. Imunidade (*immunity*)

Para que se possa invocar o privilégio contra a autoincriminação é necessário, como tivemos oportunidade de salientar anteriormente, que se crie um risco específico de incriminação[97]. No entanto, se o governo eliminar esse risco concedendo imunidade ao suspeito, poderá compeli-lo a fornecer determinadas provas e a responder a diversas perguntas. Esta imunidade tem de ser deferida de acordo com o âmbito de proteção concedido pela Quinta Emenda[98].

A necessidade de concessão de imunidade para que se ultrapasse o risco de incriminação e, consequentemente, de desrespeito pelo princípio *nemo tenetur se ipsum accusare*, não responde à questão de saber qual será a "quantidade" necessária de imunidade para evitar tal violação.

Uma imunidade total ou absoluta afastaria por completo o risco de incriminação, contudo, dar-se-ia ao suspeito a possibilidade de evitar a acusação na sua plenitude. Em última análise, o Supremo Tribunal dos Estados Unidos da América concluiu que o preço a pagar pela imunidade total ou absoluta é mais alto do que o governo deverá suportar no intuito de obter, coactivamente, determinadas provas[99].

O estatuto federal de imunidade estabelece que se for concedida imunidade: "[...] a testemunha não pode recusar-se a cumprir a ordem com base no seu privilégio contra a autoincriminação; mas nenhum testemunho ou outra informação compelida pela ordem (ou qualquer informação derivada directa ou indirectamente de tal testemunho ou outra informação) pode ser usada contra a testemunha em qualquer processo criminal [...]"[100].

No caso Kastigar v. United States[101], o Supremo Tribunal esclareceu que a imunidade deve proibir o governo de usar o testemunho compelido, bem como as provas daí provenientes, directa ou indirectamente, para acusar o arguido. Estas duas formas de imunidade foram classificadas como "*use immunity*" e "*derivative use immunity*"[102],

---

[97] Berger, 2002: 235.
[98] Soares, 2012: 2007.
[99] Kiok, 2015: 60.
[100] "*[...] the witness may not refuse to comply with the order on the basis of his privilege against self-incrimination; but no testimony or other information compelled under the order (or any information directly or indirectly derived from such testimony or other information) may be used against the witness in any criminal case [...]*".
[101] Cf. Kastigar v. United States, 1972. Disponível em: https://supreme.justia.com/cases/federal/us/406/441/case.html [consultado em 29.11.2016].
[102] Fakhoury, 2012: 83.

consoante as provas fossem retiradas directamente do testemunho prestado ou derivadas deste[103].

Assim, o tribunal deve, em primeira instância, averiguar se o governo estará ou não a tentar compelir um testemunho incriminatório. Se tal se verificar, o tribunal deve conceder imunidade no sentido de proibir o governo não só de utilizar as palavras proferidas ou os actos realizados contra o arguido, como também de utilizar qualquer outra prova obtida através do testemunho[104]. No caso de o governo querer utilizar qualquer tipo de prova derivada do testemunho prestado sob coacção contra o arguido numa subsequente acusação, deverá demonstrar que tal prova deriva de uma fonte legítima e independente do testemunho compelido[105].

Para que a imunidade possa ser concedida, é necessário que a ordem dada seja coactiva e que resulte numa acção incriminatória, de natureza testemunhal, que envolva comunicação e que expresse o conteúdo do pensamento do arguido, e que a informação prestada não seja considerada como uma conclusão inevitável (*foregone conclusion*)[106].

3. Conclusões intermédias

Podemos comprovar, pela análise da jurisprudência, Constituição e doutrina norte-americanas, que a problemática da desencriptação de smartphones para a obtenção de prova no processo penal com o auxílio do arguido é uma questão jurídica actual e real.

A Quinta Emenda à Constituição dos Estados Unidos da América protege o arguido contra determinadas medidas, sempre que estas se revelem, cumulativamente: a) coactivas; b) incriminatórias; c) e declarativas/comunicativas.

Se por um lado, estes três requisitos estão cumulativamente verificados na desencriptação de smartphones através da revelação da palavra-passe, sendo esta ordem violadora do princípio contra a autoincriminação, por outro, o último requisito da declaração/comunicação não se encontra preenchido na ordem de desencriptação de smartphones através da leitura da impressão digital do arguido, resultando na não violação do princípio de não-autoincriminação. Esta conclusão pelo não preenchimento do terceiro

[103] Duong, 2009: 339.
[104] Fakhoury, 2012: 84.
[105] Pfefferkorn, 2009: 4-5. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1883697&download=yes [consultado em 29.11.2016].
[106] Soares, 2012: 2007.

requisito no caso de desencriptação através da leitura da impressão digital está relacionada com a teoria defendida pela doutrina e jurisprudência norte-americanas de que uma acção só se considera declarativa/comunicativa nas situações em que o arguido é compelido a divulgar o conteúdo da sua mente. Assim se explicam os resultados a que a jurisprudência norte-americana chegou nos casos apresentados: o arguido não pode ser compelido a fornecer a palavra-passe do seu smartphone, mas pode ser compelido a colocar o seu dedo no leitor de impressões digitais para desencriptar o dispositivo.

Ademais, ficou esclarecido que, mesmo nas situações em que todos os requisitos da Quinta Emenda tenham sido cumulativamente preenchidos, as ordens de desencriptação de smartphones (independetemente do método) podem ser dirigidas ao arguido, ficando a sua validade a depender de duas situações: a) da demonstração pelas autoridades de um conhecimento de tal ordem particularizado sobre a existência e localização dos ficheiros que essa informação possa ser considerada como uma conclusão inevitável (*foregone conclusion*); b) da concessão de imunidade ao arguido.

Apesar de, segundo o ordenamento jurídico norte-americano, a revelação coactiva da palavra-passe que desencripta um smartphone ser considerada ilegítima por violação do princípio contra a autoincriminação e, contrariamente, a leitura coactiva da impressão digital do arguido que desencripta um smartphone ser considerada legítima, cumpre saber, uma vez que a nossa investigação é realizada em território português, se estes casos jurisprudenciais teriam a mesma solução segundo o ordenamento jurídico nacional.

CAPÍTULO II – O ACESSO E A APREENSÃO DE DADOS ARMAZENADOS EM SMARTPHONES NO PROCESSO PENAL PORTUGUÊS

Ficou analisado no capítulo anterior como o ordenamento jurídico norte-americano dá resposta ao problema da desencriptação compelida de smartphones dirigida ao arguido. No entanto, torna-se evidente a necessidade de perceber, em pormenor, como o ordenamento jurídico nacional daria resposta a esta problemática na eventualidade de estes casos jurisprudenciais surgirem em Portugal.

Para respondermos a esta pertinente contenda, recorreremos à desconstrução prática do problema. Assim, de uma perspectiva prática, a primeira questão que se coloca, em sede de desencriptação compelida de smartphones para obtenção de prova no processo penal, é a de saber, *a priori*, como se processa a apreensão e o acesso aos conteúdos armazenados no smartphone de acordo com a legislação portuguesa. Posteriormente à tentativa de acesso e apreensão desses conteúdos, às autoridades judiciárias é colocado um segundo problema: a encriptação do dispositivo. Visto que o smartphone se encontra encriptado por palavra-passe ou por biometria, a colaboração do arguido para sua a desencriptação mostra-se indispensável. É nesta sede que surge o problema se saber se esta colaboração é ou não violadora do princípio *nemo tenetur se ipsum accusare*.

De facto, como dissemos, a problemática da desencriptação de smartphones para obtenção de prova em processo penal levanta um problema a montante, sobre o qual nos devemos debruçar em primeira instância durante este capítulo. O desbloqueio do smartphone pressupõe, *a priori*, duas circunstâncias: que o dispositivo tenha sido legitimamente apreendido pelas autoridades judiciárias; e, posteriormente, que se tenha feito uma tentativa de acesso aos conteúdos electrónicos aí armazenados. Assim, parece lógico que as entidades judiciárias só podem constatar que um dispositivo está encriptado se houver, previamente, uma tentativa de acesso ao seu conteúdo, após a apreensão do aparelho. É sobre esta apreensão e acesso aos ficheiros armazenados em smartphones que discorreremos nas próximas páginas.

1. Os smartphones e a prova digital

Vivemos actualmente no seio de uma sociedade informatizada, uma sociedade que se regula diariamente com recurso a sistemas electrónicos. Durante esta última década

assistimos a uma rápida evolução tecnológica, evolução essa que se tem manifestado igualmente na área da criminalidade informática.

O telemóvel é, hoje em dia, um aparelho indispensável na vida dos cidadãos, quer pela sua capacidade comunicacional com o resto do mundo, quer pelo seu constante progresso no que concerne às suas aplicações que vão facilitando o dia-a-dia de cada um. Ainda assim, no seio da investigação de um crime, o telemóvel poderá ser visto como o maior inimigo do homem, neste caso, o maior inimigo dos investigadores criminais. Isto porque, o acesso a um telemóvel, ou mais precisamente, a um smartphone, para obtenção de prova em processo penal, terá de cumprir determinadas regras e obedecer a tantos outros procedimentos.

Em todos os casos de criminalidade, o objectivo do processo penal passa pela descoberta da verdade e pela persecução da justiça. Para tal, é necessário que se proceda à recolha de prova para que se possa condenar os culpados. Na investigação criminal, a obtenção e recolha da prova rege-se por dois artigos previstos no Código de Processo Penal: o artigo 125.º e o artigo 126.º. O primeiro estipula o princípio de que são permitidas todas as provas que não forem proibidas por lei, ao passo que o segundo estabelece que o valor de cada elemento de prova é determinado pelas regras da experiência e pela livre convicção de quem tem que decidir sobre elas[107]. Daqui resulta que as provas de índole digital são admitidas, desde que a sua obtenção tenha sido realizada dentro dos estritos critérios da legalidade e objectividade[108].

A prova digital é definida, por Benjamin Silva Rodrigues, como qualquer tipo de informação, com valor probatório, armazenada ou transmitida sob forma binária ou digital[109]. Por seu turno, Armando Dias Ramos, define a prova digital como "toda a informação passível de ser obtida ou extraída de um dispositivo digital (local, virtual ou remoto) ou de uma rede de comunicações"[110]. O legislador português não definiu o que seria prova digital, no entanto, acreditamos que, de um ponto de vista geral, a prova digital será toda e qualquer informação/dados que tenham sido recebidos, transmitidos ou que estejam armazenados num dispositivo electrónico[111]. Por outro lado, de um ponto de vista

[107] Este princípio não é absoluto, havendo excepções ao mesmo, designadamente, quanto ao valor da prova pericial.
[108] Ramos, 2014: 85.
[109] Rodrigues, 2009a: 39.
[110] Ramos, 2014: 86.
[111] Mukasey/Sedgwick/Hagy, 2008: 9.

mais técnico, cumpre esclarecer que a designação de "digital" advém do facto de a informação armazenada electronicamente ser repartida em dígitos, mais precisamente, numa sequência de números binários (isto é, zero ou um), que são reconhecidos e traduzidos pelo aparelho informático, transformando-se em informação[112].

Por este motivo, como facilmente se adivinha, a prova digital carece de ser tratada de um forma diferente, mais precisamente de uma forma mais diligente e cautelosa, uma vez que um mero lapso poderá tornar a prova irremediavelmente inutilizada[113]. Uma vez que se trata de informação em formato digital, existe sempre a preocupação da mesma ser apagada, modificada ou destruída em segundos, sem se deixar rasto[114]. Daí resulta que a rapidez na obtenção desta prova, aliada a uma correcta recolha, são dois passos fundamentais para o êxito da investigação e imputação dos factos ao suspeito do crime[115].

Toda esta constelação de problemas é também enfatizada por Figueiredo Dias, ao afirmar que entre as novas problemáticas que se têm vindo a colocar tanto à legislação como à ciência do processo penal nos últimos tempos, a primeira tem que ver, precisamente, com a circunstância de os novos horizontes técnico-científicos terem aberto a porta a métodos de investigação até há não muito tempo desconhecidos[116]. Estando aí incluídos, entre outros, os métodos de investigação computadorizados ou, de forma mais geral, permitidos pelos avanços informáticos[117] (*v.g.* o smartphone).

Atendendo à quantidade, cada vez maior, de utilizadores de smartphones, e à sua capacidade de armazenamento[118], estes dispositivos podem ser úteis ferramentas para os investigadores criminais na recolha de prova em processos crime. Se durante uma investigação criminal for apreendido um smartphone relativamente recente, com cerca de seis ou sete anos, a amplitude de informação que pode ser obtida pelos investigadores é significante, abrangendo: linguagem e outras definições; agenda de contactos; informação de calendário; mensagens escritas; registo de chamadas feitas e recebidas; e-mail; fotografias; gravações áudio e vídeo; mensagens de multimédia; mensagens instantâneas;

[112] Militão, 2012: 261.
[113] Ramos, 2014: 87.
[114] Mouraz Lopes/Antão Cabreiro, 2006: 72.
[115] Ramos, 2014: 87.
[116] Figueiredo Dias, 2009: 808-809.
[117] Figueiredo Dias, 2009: 809.
[118] Os smartphones são constantemente utilizados para as mais variadas funções: chamadas de voz; chamadas de vídeo; mensagens de texto; mensagens de imagem; pesquisas na internet, incluindo toda a panóplia de redes sociais; acesso a correio electrónico; fotografias e vídeos; calculadora; agenda; relógio; leitor de música; mapa; entre outras.

histórico de navegação na internet; documentos electrónicos; dados relacionados com as redes sociais; dados relacionados com aplicações; informação sobre localizações geográficas, entre outras[119].

Todas estas informações que podem ser recolhidas apenas de um pequeno smartphone podem fazer toda a diferença no processo penal, auxiliando os investigadores criminais de inúmeras maneiras: recolhendo informação sobre um crime cometido (através de imagens, vídeos, e-mails, documentos, etc); recolhendo informação que comprove a intenção ou a tentativa da prática de um crime (por exemplo, através da análise do histórico do *web browser*); recolhendo informação que comprove o envolvimento de suspeitos que negam estar implicados num delito; recolhendo informação que revele a prática de diferentes crimes ainda desconhecidos; recolhendo informação de vários dispositivos electrónicos que, combinados, permitem criar um cronograma de eventos.

Em vários processos criminais é deixado um rasto de informação electrónica para os investigadores criminais analisarem. E, uma vez que o smartphone poderá ser considerado um óptimo repositório de elementos probatórios, dada a sua vasta capacidade de armazenamento, coloca-se a questão: no caso de necessidade de recolha de prova armazenada num smartphone encriptado, como se procederá a apreensão do dispositivo e o posterior acesso aos conteúdos aí guardados?

Para respondermos a esta questão importa analisar a Lei do Cibercrime, de 15 de Setembro de 2009.

2. A Lei do Cibercrime

Actualmente, a prova digital é regulada, na sua essencialidade, pela Lei do Cibercrime.

No dia 15 de Setembro de 2009, o legislador português reagiu aos inúmeros desafios causados pela lacuna legislativa quanto à matéria da obtenção de prova digital, por via da publicação da Lei do Cibercrime – Lei n.º 109/2009, de 15 de Setembro (em vigor desde 15 de Outubro de 2009). Cerca de 8 anos após a assinatura da Convenção sobre o Cibercrime[120], foram publicados em Diário da República a Resolução da Assembleia da

[119] George/Mason, 2015: 250.

[120] A Convenção sobre o Cibercrime é o primeiro tratado internacional sobre criminalidade contra sistemas de computadores, redes ou dados e conta com três objectivos principais: pretende harmonizar legislações e os crimes nelas previstos; pretende estender às jurisdições de Estados Parte determinados instrumentos processuais e de produção de prova modernos e adequados à investigação da cibercriminalidade; por último, pretende facilitar a cooperação internacional e viabilizar investigações. Para tal a Convenção está compartimentada em quatro capítulos distintos: Cap. I – Terminologia; Cap. II – Medidas a tomar ao nível

República n.º 88/2009, que aprova a Convenção, o Decreto do Presidente da República n.º 92/2009, que a ratifica, e ainda a já acima referida Lei n.º 109/2009, que adapta o direito interno à Convenção e à Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de Fevereiro, relativa a ataques contra sistemas de informação.

Do ponto de vista sistemático, a Lei do Cibercrime tem uma estrutura tripartida, entre disposições materiais, processuais e relativas à cooperação internacional em matéria penal, à semelhança do consagrado na Convenção sobre o Cibercrime. A nossa atenção desviar-se-á, obviamente, para o Capítulo III, dedicado às disposições processuais, nomeadamente: a preservação expedita de dados (artigo 12.º), a revelação expedita de dados de tráfego (artigo 13.º), a injunção para a preservação ou concessão de acesso a dados (artigo 14.º), a pesquisa de dados informáticos (artigo 15.º), a apreensão de dados informáticos (artigo 16.º), a apreensão de correio electrónico e de registos de comunicações de natureza semelhante (artigo 17.º), a intercepção de comunicações (artigo 18.º), as acções encobertas (artigo 19.º) e, ainda, a cooperação internacional (artigos 20.º a 26.º).

Estas disposições processuais penais contidas na Lei do Cibercrime aplicam-se, segundo o artigo 11.º do referido diploma (em consonância com o determinado no artigo 14.º da Convenção sobre o Cibercrime) aos crimes aí previstos: a) crimes informáticos *stricto sensu* (al. a); b) "crimes cometidos por meio de um sistema informático"[121] independentemente da previsão típica do crime (al. b); c) e, por fim, a quaisquer crimes sempre que "seja necessário proceder à recolha de prova em suporte electrónico" (al. c). Podemos concluir, na esteira do defendido por Paulo Dá Mesquita, que as regras de direito probatório previstas no diploma não são assim meras normas processuais sobre cibercrimes ou sequer apenas relativas a crimes praticados em sistemas informáticos, mas

nacional: Secção I – Direito Material; Secção II – Direito Processual; Cap. III – Cooperação internacional; e, por último, Cap. IV – Cláusulas Finais. Cf. Ramalho, 2014: 134.

[121] Sistema informático significa nesta sede "qualquer dispositivo ou conjunto de dispositivos interligados ou associados, em que um ou mais de entre eles desenvolve, em execução de um programa, o tratamento automatizado de dados informáticos, bem como a rede que suporta a comunicação entre eles e o conjunto de dados informáticos armazenados, tratados, recuperados ou transmitidos por aquele ou aqueles dispositivos, tendo em vista o seu funcionamento, utilização, protecção e manutenção" (al. a) do artigo 1.º da Lei do Cibercrime, cuja primeira parte corresponde à previsão da al. a) do artigo 1.º da Convenção sobre o Cibercrime e no essencial similar à al. a) do artigo 1.º da Decisão-Quadro n.º 2005/222/JAI (sistema de informação), onde, contudo, não se prevê de forma especificada a rede que suporta a comunicação entre dados informáticos).

correspondem a um regime consideravelmente mais abrangente sobre prova electrónica em processo penal aplicável a qualquer crime[122].

Voltando ao nosso caso concreto, cumpre referir que, a alínea c) do artigo 11.º da Lei do Cibercrime, ao abranger todos os crimes em relação aos quais seja necessário proceder à recolha de prova em suporte electrónico, acaba por alargar o âmbito de aplicação da lei a quaisquer casos de recolha de prova em smartphones. Uma vez que o smartphone é caracterizado como um "suporte electrónico", toda a recolha de prova feita com recurso a este dispositivo será regulada pela Lei do Cibercrime, de acordo com o consagrado na alínea c) do seu artigo 11.º.

Visto que o cerne do nosso estudo se centra na desencriptação de smartphones para obtenção de prova em processo penal, torna-se fundamental nesta etapa fazer uma breve análise a algumas destas medidas processuais, nomeadamente, à injunção para apresentação ou concessão do acesso a dados (artigo 14.º), à pesquisa de dados informáticos (artigo 15.º), à apreensão de dados informáticos (artigo 16.º) e à apreensão de correio electrónico e registos de comunicações de natureza semelhante (artigo 17.º).

No entanto, antes de passarmos à análise destas medidas, importa esclarecer que, em sede de Lei do Cibercrime, há que fazer a distinção entre a apreensão de dados informáticos e a apreensão de registos de comunicações. Como já deixámos claro nas páginas anteriores da presente investigação, o smartphone armazena os mais variados ficheiros electrónicos, incluindo mensagens de texto (SMS) e mensagens de multimédia (MMS), e-mails, contactos telefónicos, fotografias, gravações de vídeo e áudio, entre outros. O tratamento destes ficheiros vai depender da sua natureza, nomeadamente, se estes comportam algum tipo de comunicação ou não. Assim, se por um lado a apreensão de fotografias, vídeos, gravações áudio, contactos, entre outros, pode ser tratada como apreensão de meros dados informáticos (artigo 16.º da Lei do Cibercrime), a apreensão de mensagens de texto, mensagens de multimédia e e-mails, por se tratarem de ficheiros de comunicação electrónica, deve ser tratada como apreensão de correio electrónico e registos de comunicações de natureza semelhante (artigo 17.º da Lei do Cibercrime). Analisaremos em maior detalhe esta distinção nos próximos parágrafos.

No que respeita à injunção para apresentação ou concessão do acesso a dados, prevista no artigo 14.º da Lei n.º 109/2009, o legislador veio, desta forma, criar uma ordem a ser

[122] Mesquita, 2010: 98.

emitida por autoridade judiciária, dirigida a quem tenha disponibilidade ou controlo sobre determinados dados informáticos, no sentido de que os comunique ao processo em causa, ou que permita o acesso aos mesmos[123].

No entanto, esta medida é apenas aplicada a fornecedores de serviços, proibindo, o número 5 do referido artigo, que seja dirigida contra suspeito ou arguido no processo. Desta forma, o fornecedor de serviço pode ser ordenado a comunicar ao processo dados relativos aos clientes ou assinantes, neles se incluindo qualquer informação, desde que não inserida na categoria dos dados relativos ao tráfego ou ao conteúdo. Voltaremos, em maior detalhe, a esta questão da proibição de injunção dirigida a arguido e suspeito mais adiante no nosso estudo.

As razões que estão subjacentes à criação desta medida prendem-se, em primeira medida, com a imensidade de espaço de armazenamento dos modernos suportes digitais, que dificulta a investigação e, em segunda medida, com as diversas possibilidades de ocultar a informação ou de bloquear o acesso a ela (por exemplo, por via da encriptação do smartphone), que podem igualmente tornar malsucedida a procura de informação, sem a colaboração de quem tem o domínio sobre ela.

O artigo 15.º da Lei do Cibercrime, que consagra a pesquisa de dados informáticos, veio criar uma forma de acesso coercivo ao sistema informático objecto de um processo criminal. Assim, esta pesquisa pode perfeitamente ser comparada a uma busca tradicional, mas num ambiente digital. Desta forma, sempre que, numa investigação criminal, as entidades judiciárias, verificarem que se afigura oportuno e necessário, para a produção de prova, com vista à descoberta da verdade material, que se obtenham certos dados[124], armazenados num determinado sistema informático, a autoridade judiciária competente autoriza ou ordena, por despacho, que se proceda a uma pesquisa nesse sistema informático[125].

Esta autorização tem uma validade de 30 dias, sob pena de nulidade nos termos do n.º 2 do artigo 15.º da Lei do Cibercrime. Nos casos de obtenção de consentimento por quem tenha a disponibilidade ou controlo dos dados, de terrorismo, criminalidade violenta ou

[123] Venâncio, 2011: 107.
[124] Contrariamente à injunção para apresentação ou concessão do acesso a dados, na pesquisa de dados informáticos a lei não coloca quaisquer restrições relativamente aos conteúdos dos dados que podem ser pesquisados.
[125] Rodrigues, 2010: 446.

altamente organizada e quando haja fundados indícios da prática iminente de crime que ponha em grave risco a vida ou a integridade de qualquer pessoa, os órgãos de polícia criminal poderão proceder à pesquisa sem prévia autorização da autoridade judiciária, devendo a diligência ser-lhe de imediato comunicada e elaborado um relatório em tudo semelhante ao disposto no artigo 253.º do Código de Processo Penal (nos termos dos n.os 3 e 4 do artigo 15.º).

Pode ainda acontecer que, no decurso da pesquisa, aos órgãos de polícia criminal, executores da medida, surja a convicção de que os dados procurados se encontram noutro sistema informático, ou numa parte diferente do sistema pesquisado, mas que tais dados são legitimamente acessíveis a partir do sistema inicial, então, por força do n.º 5 do artigo 15.º da Lei do Cibercrime, haverá lugar à extensão da medida àqueles outros sistemas ou lugares, mediante autorização ou ordem da autoridade competente, nos termos dos n.os 1 e 2 do artigo 15.º da citada lei[126].

No caso concreto de as autoridades judiciárias encontrarem um smartphone armazenado com e-mails, mensagens de texto, mensagens de multimédia, fotografias, gravações áudio ou vídeo, histórico de navegação na internet, documentos electrónicos, dados relacionados com as redes sociais, dados relacionados com aplicações, entre outros, estamos claramente perante dados informáticos, definidos pela al. b) do artigo 2.º da Lei do Cibercrime como "qualquer representação de factos, informações ou conceitos sob uma forma susceptível de processamento num sistema informático, incluindo os programas aptos a fazerem um sistema informático executar uma função". Assim, a pesquisa destes dados, armazenados no smartphone, por parte das autoridades judiciárias, deverá ser regulada pelo citado artigo 15.º da Lei do Cibercrime.

Por seu turno, a apreensão de dados informáticos vem prevista no artigo 16.º da Lei do Cibercrime, que vem estabelecer a possibilidade de os investigadores pedirem à autoridade judiciária competente que autorize ou ordene, por despacho, a apreensão dos dados ou documentos informáticos que, no decurso de uma pesquisa informática ou de outro acesso legítimo a um sistema informático, forem encontrados e que se afigurem necessários à produção da prova, tendo em vista a descoberta da verdade[127].

[126] Rodrigues, 2010: 449-450.
[127] Rodrigues, 2010: 451.

No entanto, nos casos em que tenha sido um órgão de polícia criminal a realizar a pesquisa (artigo 15.º da Lei do Cibercrime), existe a possibilidade de o órgão de polícia criminal levar igualmente a cabo a apreensão dos dados informáticos (sem prévia autorização da autoridade judiciária), ficando estas diligências sujeitas a validação pela autoridade judiciária, no prazo máximo de setenta e duas horas[128]. Assim, a título de exemplo, se durante uma busca domiciliária, promovida pelo Ministério Público e autorizada pelo Juiz de Instrução competente, for encontrado um smartphone – que não estaria incluído no despacho judicial -, os órgãos de polícia criminal, executores da medida, poderão apreender validamente o conteúdo do dispositivo, de acordo com o n.º 2 do artigo 16.º da Lei do Cibercrime, ficando esta diligência sujeita a validação pela autoridade judiciária, no prazo máximo de setenta e duas horas.

O n.º 3 do artigo 16.º da Lei do Cibercrime vem consagrar a obrigatoriedade de intervenção do juiz de instrução sempre que forem apreendidos para junção ao processo dados ou documentos informáticos cujo conteúdo seja susceptível de revelar dados pessoais ou íntimos, que possam pôr em causa a privacidade do respectivo titular ou de terceiros. Nestas situações, os dados informáticos apreendidos – que possam por em causa a privacidade do respectivo titular ou de terceiros (*v.g.* fotografias, gravações de vídeo ou áudio, entre outros) - serão apresentados ao juiz que ponderará a sua junção aos autos, tendo em conta os interesses do caso concreto. A não observância destas formalidades legais tem como consequência a nulidade da prova obtida por esta via[129].

Por fim, cabe-nos fazer uma análise mais detalhada do artigo 17.º da Lei do Cibercrime, que consagra a apreensão de correio electrónico e registos de comunicações de natureza semelhante. A criação desta norma é uma das grandes novidades da Lei do Cibercrime, não só por estabelecer um regime especial para a apreensão de correio electrónico e registos de comunicação de natureza semelhante (aqui incluindo as SMS e MMS) em matéria de criminalidade informática e obtenção de prova em suporte electrónico, mas também por estabelecer um regime que não encontra correspectivo directo na Convenção sobre o Cibercrime.

O artigo 17.º da Lei n.º 109/2009, determina que é possível apreender mensagens de correio electrónico ou registos de comunicações de natureza semelhante que se encontrem armazenados no sistema informático (*v.g.* smartphone) que tenha sido alvo de pesquisa

[128] Morais, 2012: 101-102.
[129] Verdelho, 2009: 741.

informática ou outro acesso legítimo, desde que: a) seja o juiz a autorizar ou ordenar a apreensão; b) e, esta seja de grande interesse para a descoberta da verdade ou para a prova[130].

Dois comentários iniciais sobre este dispositivo: primeiro, podemos afirmar que há aqui um aumento substancial das exigências para esta medida, dado que a mesma só poderá ser autorizada se for de grande interesse para a descoberta da verdade ou para a prova; segundo, importa também referir que não estamos aqui perante um meio de obtenção de prova autónomo e independente, mas sim perante uma possibilidade decorrente de uma pesquisa informática (artigo 15.º da Lei do Cibercrime) já em curso que tenha sido regularmente executada[131]. Efectivamente, consagra esta disposição normativa que "Quando, no decurso de uma pesquisa informática ou outro acesso legítimo a um sistema informático, forem encontrados, armazenados nesse sistema informático ou noutro a que seja permitido o acesso legítimo a partir do primeiro, mensagens de correio electrónico ou registos de comunicações de natureza semelhante, o juiz pode autorizar ou ordenar, por despacho, a apreensão daqueles que se afigurem ser de grande interesse para a descoberta da verdade ou para a prova, aplicando-se correspondentemente o regime da apreensão de correspondência previsto no Código de Processo Penal".

Relativamente à remissão feita no final do referido artigo para o regime da apreensão de correspondência, estamos com Rita Castanheira Neves quando afirma que se compreende que, em respeito pelo artigo 11.º da Lei do Cibercrime, "a remissão para o regime da apreensão de correspondência não abranja a exigência de se tratar de crime punível com pena de prisão superior a três anos. Esta remissão para o regime da apreensão de correspondência parece, pois, realizada a quatro aspectos do regime: à referência à nulidade no caso de não respeito pelos requisitos estabelecidos (n.os 1 e 2 do artigo 179.º do Código de Processo Penal); ao facto de ter que estar em causa correio electrónico e registos de comunicações de natureza semelhante enviados ou recebidos pelo suspeito, mesmo que de/a partir de endereço electrónico ou outros registos de pessoa diversa (alínea a) do n.º 1 do mesmo artigo 179.º); à proibição da apreensão de correio electrónico e registos de comunicações de natureza semelhante trocado entre arguido e defensor, salvo se o juiz tiver fundadas razões para crer que aquele correio electrónico ou aqueles registos constituem objecto ou elemento do crime (n.º 2 do artigo 179.º); e finalmente ao facto de

[130] Neves, 2011: 273.
[131] Morais, 2012: 102.

ter que ser o juiz que tiver autorizado ou ordenado a diligência a primeira pessoa a tomar conhecimento do conteúdo do correio electrónico e demais registos de comunicações apreendido, mandando-o juntar ao processo se o considerar relevante […] – n.º 3 do artigo 179.º"[132].

Quanto a esta última questão, parece-nos necessário focar em especial dois aspectos distintos: primeiro, a necessidade ou não de despacho judicial para a apreensão das mensagens de correio electrónico e registos de comunicação de natureza semelhante (n.º 1 do artigo 179.º do Código de Processo Penal); segundo, a necessidade de ter que ser o juiz a primeira pessoa a ler o correio electrónico ou as mensagens de texto ou multimédia apreendidas e a decidir da sua junção ou não ao processo (n.º 3 do artigo 179.º do Código de Processo Penal).

Tendo em conta que a única exigência do artigo 17.º da Lei do Cibercrime para a apreensão de correio electrónico e registos de comunicação de natureza semelhante é a existência de uma forma legítima de acesso ao meio informático, concordamos com Pedro Verdelho quando defende que a referida medida permite fazer uma apreensão provisória de mensagens de correio electrónico, de texto ou multimédia, no decurso de pesquisas, realizadas, por exemplo, com a autorização do Ministério Público, devendo todavia tais mensagens ser presentes ao juiz, para que ordene a respectiva apreensão definitiva e junção ao processo. Ou seja, não se requererá, para a apreensão provisória de e-mails, SMS ou MMS, que haja uma prévia decisão judicial[133].

Em regra, antes de uma busca ainda não se tem conhecimentos bastantes para certificar que se encontrará ou não um smartphone. Assim, na prática, seria inviável um sistema que exigisse, antes de toda e qualquer busca, a obtenção de autorização judicial para a eventual possibilidade de vir a ser encontrado, no decurso de uma busca, um smartphone, e que tal smartphone contivesse registos de comunicações, e que tais comunicações fossem prova necessária à investigação do caso concreto.

De salientar, no entanto, que esta apreensão será meramente uma apreensão cautelar, cuja validade (definitiva) e consequente valoração no processo em curso estará sempre dependente do despacho do juiz (n.º 1 do artigo 179.º do CPP).

[132] Neves, 2011: 274-275.
[133] Verdelho, 2009: 743-744.

Neste sentido vai também a jurisprudência, ao afirmar que "a apreensão de mensagens de telemóvel (SMS), mesmo que resultante de uma pesquisa de dados informáticos validamente ordenada pelo Ministério Público, deve depois ser autorizada pelo JIC. Embora o MP deva tomar conhecimento em primeira mão das mensagens, ordenando a apreensão provisória, deve depois ser o juiz a ordenar a apreensão definitiva – artigo 17.º da Lei do Cibercrime"[134].

No entanto, nos casos de apreensão de mensagens decorrentes da autorização do seu destinatário (por exemplo, quando é o próprio a facultar o telemóvel para a obtenção das mensagens), a jurisprudência tem sido unânime quanto à desnecessidade de intervenção judicial na obtenção e junção ao processo desses registos[135].

Assim, concluímos no sentido de não carecer de autorização judicial a mera apreensão provisória/cautelar de mensagens de correio electrónico, de texto ou de multimédia encontradas, no decurso de uma pesquisa informática (artigo 15.º da Lei do Cibercrime) ou outro acesso legítimo, num smartphone[136]. Sem embargo, a validade definitiva desta apreensão e a sua consequente valoração no processo em curso dependerá sempre do despacho do juiz (n.º 1 do artigo 179.º do CPP).

No que concerne à questão da necessidade de ter que ser o juiz a primeira pessoa a ler o correio electrónico e outros registos de comunicações de natureza semelhante apreendidos (n.º 3 do artigo 179.º do Código de Processo Penal), importa trazer à colação a posição defendida por dois Autores nacionais.

Rita Castanheira Neves defende a tese de que, dada a dificuldade prática de ser o juiz a primeira pessoa a tomar conhecimento do conteúdo de todas as mensagens, cuja quantidade pode ser bastante significativa, se deveria proceder a uma inversão da lógica das coisas. Assim, a Autora afirma que "não há que deixar de exigir que seja o juiz o primeiro a tomar conhecimento do conteúdo do correio electrónico […]", mensagens de texto e multimédia, "[…] pelas dificuldades práticas de atribuir a um só juiz essa tarefa,

---

[134] Acórdão do Tribunal da Relação de Guimarães, de 29 de Março de 2011, disponível em: http://www.dgsi.pt/jtrg.nsf/86c25a698e4e7cb7802579ec004d3832/6aa96edf91e899b2802578a00054631f?OpenDocument [consultado em 29.08.2016].

[135] Acórdão do Tribunal da Relação de Lisboa, de 11 de Janeiro de 2011, disponível em: http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/e5ed1936deb44eb180257824004ab09d?OpenDocument [consultado em 29.08.2016].

[136] Acórdão do Tribunal da Relação de Guimarães, de 29 de Março de 2011, disponível em: http://www.dgsi.pt/jtrg.nsf/86c25a698e4e7cb7802579ec004d3832/6aa96edf91e899b2802578a00054631f?OpenDocument [consultado em 29.08.2016].

mas sim exigir que durante a diligência se tenha sempre em atenção que para a eficácia da mesma devem-se seguir estritos critérios de abrangência, apenas apreendendo os e-mails […]", mensagens de texto e de multimédia "[…] que se afiguram realmente determinantes para a prova"[137].

Em sentido semelhante, Pedro Verdelho, vem apoiar-se na letra da lei que, segundo o próprio, aponta para a possibilidade de quem procede à pesquisa encaminhar para o juiz mensagens concretas, com relevância para o caso concreto, que aquele depois apreenderá ou não[138]. Entendendo-se a lei de outra forma, estar-se-ia, segundo o Autor, a optar por uma solução processual inviável, que exigiria a verificação, pelo juiz, de todas as mensagens de correio electrónico e registos, em todos os smartphones, que fossem encontrados no decurso de pesquisas.

Pela nossa parte, apoiamo-nos na ideia de que o artigo 17.º da Lei do Cibercrime ao remeter, quanto à apreensão de mensagens de correio electrónico e registos de comunicações de natureza semelhante, para o regime geral previsto no Código de Processo Penal, determina a aplicação daquele regime com as devidas adaptações.

Assim, e de encontro com o defendido por Rita Castanheira Neves, Pedro Verdelho e pela jurisprudência, aquelas apreensões (definitivas) têm, efectivamente, de ser autorizadas ou determinadas por despacho judicial[139], devendo ser o juiz a primeira pessoa a tomar conhecimento do conteúdo da correspondência previamente seleccionada como determinante para a prova, sob pena de nulidade.

Chegados a esta parte, e tendo em consideração o objecto do nosso estudo, podemos então concluir, depois de analisado o artigo 17.º da Lei do Cibercrime, que este preceito é aplicável a todas as situações em que surja a necessidade, por parte das entidades judiciárias, de apreensão de correio electrónico, mensagens de texto e mensagens de multimédia armazenados num smartphone.

---

[137] Neves, 2011: 275.
[138] Verdelho, 2009: 744.
[139] Morais, 2012: 105. No caso de e-mails, SMS e MMS, "a intervenção judicial, tendo em vista a sua apreensão ou não, é sempre exigida em momento ulterior, portanto após se ter encontrado este tipo de informação. Nessa altura compete ao juiz escolher, de entre as mensagens encontradas, as que são relevantes para a prova. Sublinha-se portanto que, no sistema legal da Lei do Cibercrime, não poderá nunca haver mensagens de correio electrónico […]", mensagens de texto e mensagens de multimédia "[…] apreendidas para serem utilizadas como prova de determinado processo sem que haja um despacho de um juiz nesse sentido". Cf. Verdelho, 2009: 745.

3. A relação entre a Lei do Cibercrime e o Código de Processo Penal

Já foi analisado, em sede de apreensão de correio electrónico e registos de comunicações de natureza semelhante, que a remissão do artigo 17.º da Lei do Cibercrime para o regime da apreensão de correspondência previsto no Código de Processo Penal determina a aplicação deste regime com as devidas adaptações.

A questão que se coloca agora é a de saber qual será a relação entre o regime vertido no Código de Processo Penal sobre a intercepção de comunicações guardadas em suporte digital (artigos 187.º a 190.º do CPP), e o regime estabelecido na nova Lei do Cibercrime para a apreensão de correio electrónico e registos de comunicações de natureza semelhante (artigo 17.º da Lei do Cibercrime).

É da nossa opinião, na esteira do defendido pela maioria da doutrina, que no ordenamento jurídico português a intercepção e o registo das transmissões de dados informáticos segue, a partir da entrada em vigor da Lei do Cibercrime, em 15 de Outubro de 2009, o regime aí vertido. Efectivamente, a Lei do Cibercrime ao optar por mobilizar um critério lato para a sua aplicação – necessidade de proceder à recolha de prova em suporte electrónico -, acabou por esvaziar o âmbito de aplicação do artigo 189.º do Código de Processo Penal, na parte relativa a comunicações electrónicas[140].

Em suma, podemos concluir que a legislação contida no Código de Processo Penal foi, no essencial[141], ultrapassada pela Lei n.º 109/2009, levando assim à aplicação do artigo 17.º da Lei do Cibercrime aos casos de apreensão de correio electrónico, mensagens de texto e mensagens de multimédia, como tínhamos concluído *supra*, e à aplicação do artigo 16.º da Lei do Cibercrime aos casos de apreensão de dados informáticos (*v.g.* fotografias, gravações de vídeo e áudio, contactos, documentos electrónicos, entre outros) armazenados em smartphones.

4. Conclusões intermédias

Após uma análise detalhada sobre a Lei do Cibercrime, encontramo-nos aptos a responder à questão que colocámos no início do presente capítulo: como se processa o acesso e a apreensão de conteúdos armazenados num smartphone de acordo com a legislação portuguesa?

[140] Neves, 2011: 280. Neste sentido vai também Mesquita, 2010: 103.
[141] Tal não invalida que todas as medidas, gerais ou excepcionais, e obrigações previstas na Lei n.º 109/2009, se cumulem, em tudo o que as não contrarie, com as estabelecidas no Código de Processo Penal.

Ao abranger todos os crimes em relação aos quais seja necessário proceder à recolha de prova em suporte electrónico, a Lei do Cibercrime, na al. c) do seu artigo 11.º, acaba, por um lado, por alargar o seu âmbito de aplicação a quaisquer casos de desencriptação de smartphones para obtenção de prova em processo penal e, por outro, por esvaziar o âmbito de aplicação do regime da intercepção de comunicações guardadas em suporte digital previsto no Código de Processo Penal.

No que concerne ao acesso e à apreensão de conteúdos armazenados num smartphone para a obtenção de prova em processo penal, cumpre deixar claro que, em primeira instância, é autorizada, por despacho, uma pesquisa ao conteúdo do smartphone, regulada pelo artigo 15.º da Lei do Cibercrime e equiparada a uma busca tradicional, mas em ambiente digital. Desta pesquisa podem resultar duas situações: a necessidade de apreensão de determinados ficheiros electrónicos ou, contrariamente, a desnecessidade de apreensão de quaisquer ficheiros electrónicos.

Caso se venha a verificar a primeira situação (necessidade de apreensão de determinados ficheiros electrónicos) deverá ser feita a divisão entre: a) a necessidade de apreensão de dados informáticos (artigo 16.º da Lei do Cibercrime); b) e a necessidade de apreensão de mensagens de correio electrónico ou registos de comunicações de natureza semelhante (artigo 17.º da Lei do Cibercrime).

Se, depois de feita uma primeira pesquisa ao conteúdo do smartphone, os investigadores encontrarem determinados dados ou documentos informáticos, tais como fotografias, vídeos, gravações de aúdio ou listas de contactos, cuja apreensão se mostre necessária para a investigação criminal, deverá ser pedido à autoridade judiciária competente que autorize ou ordene, por despacho, a sua apreensão (artigo 16.º da Lei do Cibercrime). Existe ainda a possibilidade de o próprio órgão de polícia criminal levar a cabo esta apreensão, sem a prévia autorização da autoridade judiciária, ficando esta diligência sujeita a validação pela autoridade judiciária no prazo máximo de setenta e duas horas. Como a apreensão destes dados, nomeadamente de fotografias, vídeos ou gravações aúdio pode pôr em causa a privacidade do arguido ou de terceiros, o n.º 3 do referido artigo vem consagrar a obrigatoriedade de intervenção do juiz de instrução.

Por seu turno, se no decorrer da pesquisa ao conteúdo do smartphone, os investigadores encontrarem mensagens de correio electrónico, mensagens de texto ou de multimédia, cuja apreensão se mostre de grande interesse para a descoberta da verdade ou para a prova,

deverá ser pedido ao juiz que autorize ou ordene a apreensão dessas mensagens de correio electrónico e registos de comunicações de natureza semelhante (artigo 17.º da Lei do Cibercrime).

Isto posto, parece-nos ser possível afirmar que o acesso e a apreensão de ficheiros electrónicos armazenados num smartphone é um processo relativamente simples. No entanto, durante a abordagem da referida questão, não colocámos a possibilidade de o acesso e a apreensão destes ficheiros serem dificultados pela encriptação do smartphone. Assim, a tentativa de aceder e apreender ficheiros potencialmente incriminatórios armazenados num smartphone pode ser impossibilitada pelo bloqueio do dispositivo por parte do seu proprietário, através da encriptação por palavra-passe ou por biometria. É sobre esta encriptação que nos pronunciaremos de seguida.

CAPÍTULO III – A ENCRIPTAÇÃO DE SMARTPHONES

Num caso típico de desencriptação de smartphones, após a recolha do dispositivo, às autoridades judiciárias cabe aceder e apreender os conteúdos aí armazenados a fim de obterem provas incriminatórias. Sem embargo, como ficou assente anteriormente, não raras vezes os investigadores deparam-se com um entrave ao acesso aos ficheiros guardados no smartphone: a encriptação do dispositivo. Dada a circunstância, a tarefa de aceder ao dispositivo com o desígnio de recolher prova digital para auxiliar à investigação criminal torna-se mais complexa.

Nos casos apresentados no primeiro capítulo da presente investigação, a encriptação dos smartphones em causa era feita através de dois métodos distintos: a palavra-passe alfanumérica e a biometria (leitura de impressões digitais). Tendo em consideração os casos apresentados, que nos hão de servir de modelo ao longo da nossa investigação, e o elevado número de utilizadores que, actualmente, recorre a estes dois métodos de encriptação, mostra-se imperativo, não só analisar a noção e as funcionalidades da encriptação, mas também, como funcionam estes dois métodos em concreto.

1. A sociedade na era digital e a crescente necessidade de encriptar

No final do século passado, com os avanços tecnológicos, científicos, sociais e o fenómeno da globalização, a sociedade industrial passou a caminhar para uma sociedade informacional e comunicacional, ganhando o epíteto de sociedade na era digital[142].

A entrada de Portugal na era comum da informação tornou-se irreversível e afectou todos os aspectos da sociedade[143], estando o seu surgimento umbilicalmente relacionado com o apogeu e o sucesso da Internet. Assim, com o nascimento da Internet é simultaneamente criado um novo paradigma de sociedade, onde a energia é progressivamente substituída pela informação[144], como fonte primeira do progresso social, tendo como produto essencial a prestação de novos serviços[145]. Numa realidade recente, a informação é divulgada à velocidade da luz, funcionando como moeda de troca em diversas negociações.

---

[142] Quelhas, 2008: 22.
[143] Rodrigues, 2009a: 96.
[144] "*The world isn't run by weapons anymore, or energy, or money. It's run by ones and zeros – little bits of data. It's all electrons… There's a war out there, a world war. It's not about who has the most bullets. It's about who controls the information… It's all about information*." Cf. Weinberg, 1998: 675.
[145] Marques/Martins, 2006: 109.

Contudo, dada a facilidade na troca de informações – muita das vezes confidenciais ou de carácter privado - esta sociedade da informação ou, como preferimos, sociedade digital, deverá pautar-se, sempre, em respeito pelos princípios democráticos da igualdade e solidariedade, visando a melhoria da qualidade de vida de todos os cidadãos[146].

O telemóvel, nomeadamente o smartphone, é um dos resultados desta evolução tecnológica, sendo considerado, actualmente, como uma necessidade tanto pessoal quanto profissional para a generalidade das pessoas[147]. Na sociedade actual, informação é sinónimo de poder. Esta realidade levou a que o homem médio passasse a armazenar – digitalmente - uma quantidade considerável de informação, convertendo, por sua vez, os telemóveis em tesouros dos tempos modernos. Desta forma, não causa estranheza afirmar que a informação aí armazenada tem, frequentemente, carácter pessoal ou privado, pelo que surgem diversas preocupações por parte dos proprietários relativamente à sua privacidade.

Efectivamente, a protecção da vida privada na era digital deixou de ser um índice de condição social: é um problema colectivo. O Estado social moderno tem um grau de participação ou ingerência na sociedade impensável no modelo de Estado liberal. Desta forma, de uma maneira ou de outra, todos os cidadãos acabam por estabelecer, a dado momento, contacto com a máquina estatal, vendo-se compelidos a ceder-lhe dados de carácter pessoal[148]. Como exemplo desta ingerência estatal, podemos chamar à colação o escândalo norte-americano que envolveu o funcionário da agência NSA americana, Edward Snowden[149]. No verão de 2013, Edward Snowden tornou públicas diversas informações sobre programas que constituiriam o sistema de vigilância global de comunicações e tráfego de informações executada pela NSA americana[150].

No entanto, não é apenas esta ingerência estatal no âmbito digital que inquieta a sociedade moderna, mas também a ingerência de terceiros. Diversos são os dispositivos de pequenas dimensões, tais como os smartphones, que podem ser perdidos e posteriormente encontrados por terceiros curiosos. Assim, não será só o Estado, mas também estes terceiros, que geram na sociedade um receio de devassa da vida privada.

[146] Benevides, 2002: 90.
[147] Clemens, 2004: 2.
[148] Benevides, 2002: 84.
[149] Jaffer/Rosenthal, 2016: 286.
[150] McCarthy, 2016: 21.

Ora, numa sociedade em que grande parte das trocas de informações ocorre por meios electrónicos, como o smartphone, é natural que exista a preocupação de implementar técnicas e meios de transmissão seguros dessa mesma informação. A necessidade de desenvolvimento de um meio técnico que permita, no âmbito do armazenamento digital de informações, a confirmação de determinados aspectos relacionados com a segurança da informação aí armazenada levou ao desenvolvimento da encriptação[151]. Percebe-se que a encriptação seja especialmente importante quando a informação que se pretende manter segura é armazenada em suportes electrónicos de pequena escala que se encontram presentes no dia-a-dia de qualquer cidadão (*v.g.* smartphone).

2. Encriptação de smartphones

O recurso à encriptação como tentativa de proteger certo tipo de informação não é algo recente, pelo contrário, existe, de uma forma ou de outra, há milhares de anos. Apesar de alguns exemplos dos últimos 4000 anos diferirem daquilo que hoje conhecemos como encriptação, diferentes formas de encriptar foram utilizadas por padres, imperadores, diplomatas, generais, espiões, comerciantes, insurgentes, criminosos, prisioneiros e amantes ao longo do tempo[152].

Actualmente, e atendendo ao tema da nossa investigação, uma das formas mais utilizadas de encriptação é, precisamente, a encriptação de smartphones. De facto, esta encriptação passou a ser a norma e não a excepção, sendo utilizada de diversas maneiras e com variados propósitos[153].

2.1. Noção

A encriptação pode ser definida como o processo através do qual uma qualquer informação é convertida numa forma ilegível com recurso a algoritmos matemáticos[154]. No nível mais básico, a encriptação usa a arte da criptografia (em grego "escrita secreta"), para transformar informação que pode ser lida (*plaintext*) em informação que não pode ser lida (*ciphertext*)[155]. O processo é executado de acordo com um algoritmo de encriptação: o *cipher*[156] (um conjunto de regras que regula como o *"plaintext"* é codificado). Apesar de este processo poder ser tão simples quanto substituir cada letra

[151] Martins/Marques/Dias, 2004: 69.
[152] Vagle, 2015: 106-107.
[153] Swire/Ahmad, 2012: 453.
[154] Sales, 2014: 208.
[155] Thompson II/Jaikaran, 2016: 2.
[156] Colarusso, 2011: 141.

numa mensagem por um respectivo número, os algoritmos da encriptação mais moderna consistem, frequentemente, numa série complexa de funções matemáticas[157]. Assim, a encriptação pode ser usada para baralhar todo o conteúdo do smartphone, tornando impossível a distinção entre zeros e uns que poderão representar um documento, e zeros e uns que poderão ser apenas espaço de armazenamento vazio[158]. Independentemente do modo de encriptação, o resultado final será sempre a ininteligibilidade da informação para terceiros – governo ou particulares.

Para que a encriptação possa ser vista como um método útil de armazenamento ou envio de informação é necessário que seja reversível. Desta forma, os mais modernos sistemas de encriptação utilizam uma chave que deve ser aplicada ao algoritmo de encriptação escolhido para a recuperação do "*plaintext*"[159]. A desencriptação poderá ser então definida como o processo pelo qual se transforma ou converte a informação codificada em informação legível. Igualmente correcta é a afirmação de que a desencriptação será o processo de transformação de um "*ciphertext*" em "*plaintext*"[160].

2.2. Funcionalidades

Para o correcto funcionamento da encriptação são necessários cinco elementos distintos: a) a função da encriptação[161]; b) a função da desencriptação; c) a chave; d) o "*plaintext*"; e) e o "*ciphertext*"[162].

A encriptação tem como função principal a garantia de confidencialidade e a prevenção de intromissão de terceiros em determinadas informações. Efectivamente, a encriptação pode ser caracterizada como um dos métodos mais idóneos na protecção de informação electrónica contra intercepções ilícitas por parte do governo, empresas concorrentes, criminosos e outros[163]. O recurso à encriptação passou a ser tão comum que inúmeros fabricantes de aparelhos tecnológicos a consideram como uma medida de segurança básica. Mesmo que a informação codificada seja perdida ou furtada, não será acessível a terceiros não autorizados.

[157] Ungberg, 2009: 540.
[158] Mohan/Villasenor, 2012: 17.
[159] Lehtinen/Gangemi, 2006: 141-142.
[160] Mathur, 2012: 1650.
[161] A "função" será o processo matemático usado.
[162] Thompson II/Jaikaran, 2016: 3.
[163] Sherwinter, 2007: 512.

Após o escândalo de Snowden ter espalhado a sensação de desconfiança e de falta de privacidade na sociedade digital, e atendendo às valências da encriptação, empresas como a Apple, Samsung, Google, Facebook, WhatsApp e Blackberry, anunciaram a implementação de sistemas de encriptação nas suas plataformas e produtos como uma medida de segurança e privacidade[164].

A título de exemplo, a empresa Apple, que será objecto de estudo durante a nossa investigação, no seu sistema operativo iOS, nos iPads, iPhones e iPods, recorre à encriptação não só para prevenir o acesso de pessoas não autorizadas, como também para evitar que o sistema operativo seja apagado por terceiros. No final do mês de Novembro de 2016, cerca de 95% dos iPhones a nível mundial - uma percentagem com uma clara tendência para aumentar - seriam inacessíveis às autoridades judiciárias[165][166]. Só nos Estados Unidos da América cerca de 85 milhões de aparelhos da marca Apple estão encriptados[167].

Apesar das suas claras vantagens no âmbito da segurança e privacidade de determinadas informações, a encriptação tem, igualmente, algumas vulnerabilidades e desvantagens. De facto, todas as formas de encriptação estão sujeitas a três categorias básicas de ataque: a) ataques de força bruta (*brute-force attacks*); b) ataques através de "*peer-review*"; c) e "*backdoors*"[168].

Nos ataques de força bruta, ou *brute-force attacks*, os terceiros que pretendem aceder ao smartphone recorrem a programas informáticos que testam todas as combinações de diferentes caracteres possíveis até conseguirem desencriptar o dispositivo através da combinação correcta[169]. Dependendo da força da combinação este processo poderá ser mais ou menos demorado.

A segunda e mais sofisticada forma de ataque, designada por "*peer-review*", envolve a tentativa, por parte de especialistas em segurança e criptógrafos, de desencriptar sistemas para testar a sua segurança. Até que um sistema de encriptação tenha resistido durante

---

[164] McCarthy, 2016: 21-22.
[165] Cf. App Store Support – Apple Developer. Disponível em: https://developer.apple.com/support/app-store/ [consultado em 09.12.2016].
[166] "*When conducting criminal investigations, if you pull the power on a smartphone that is encrypted you have lost any chance of recovering that data*". Cf. Garfinkel, 2012: 2. Disponível em: https://www.technologyreview.com/s/428477/the-iphone-has-passed-a-key-security-threshold/ [consultado em 09.12.2016].
[167] Jaffer/Rosenthal, 2016: 289.
[168] Swire/Ahmad, 2012: 429.
[169] McCarthy, 2016: 19.

anos, porventura décadas, a um escrutínio por parte destes criptógrafos experientes, não será considerado seguro o suficiente para uso comercial[170]. Ser submetido a um "*peer-review*" é, portanto, essencial para a implementação comercial de um "*cryptosystem*".

Por fim, a terceira forma de ataque a um smartphone pode passar pelo uso de "*backdoors*". As *backdoors* são intencionalmente construídas no sistema de encriptação com o desígnio de fornecer uma alternativa para aceder ao conteúdo codificado. Podem ser vistas como brechas de segurança inerentes, uma vez que permitem um acesso secundário ao dispositivo sem a necessidade de desencriptar[171].

Numa outra perspectiva, podemos ainda chamar à colação uma possível desvantagem que a implementação de encriptação em smartphones pode gerar: o aumento do crime. De um ponto de vista mais extremo, há quem defenda que a encriptação pode levar a que criminosos e terroristas tracem os seus planos e armazenem informações relevantes sobre os seus intentos nos seus smartphones encriptados, longe dos olhares das entidades judiciárias[172].

2.3. Métodos de encriptação de smartphones

Existem, actualmente, diversos métodos de encriptação e desencriptação de smartphones, muito dependente da marca do dispositivo. Tipicamente, os métodos de encriptação (ou de autenticação, como são muitas vezes designados), baseiam-se em três factores distintos: a) possessão (algo que a pessoa tem, como um cartão do banco, uma chave ou um *token*[173]); b) conhecimento (algo que a pessoa sabe, como um *username*, uma palavra-passe ou um *PIN*); c) identidade (algo que a pessoa é ou faz, como uma impressão digital, a íris, a voz ou o rosto)[174]. No que à nossa investigação diz respeito, a distinção revelante será feita entre o factor do conhecimento e da identidade.

---

[170] Swire/Ahmad, 2012: 431-432.
[171] "*The image is that the front door to a house is securely locked, but someone can enter through a backdoor that appears to be locked, but is actually easy to open*". Cf. Swire/Ahmad, 2012: 432.
[172] Andrews, 2000: 211.
[173] *Tokens* são dispositivos físicos utilizados para auxiliarem a segurança pessoal do seu utilizador em determinadas transacções (muitas das vezes bancárias). Normalmente o processo é feito através de um aparelho semelhante a uma chave que vai gerando diversas senhas com um único clique.
[174] Hoyos Labs, 2016: 4. Disponível em: http://pimn-public.sharepoint.com/Documentatie/2016-06-10-idm-Hoyos-Labs-Guaranteeing-identity-with-biometric-authentication.pdf [consultado em 12.12.2016]. Neste sentido cf. Pato/Millett, 2010: 5. "*Un soggetto, dunque, può essere identificato non solo mediante qualcosa che conosce (una password, un PIN) o qualcosa che possiede (un dispositivo di autenticazione, una smart card), come comunemente avviene, ma anche mediante qualcosa che gli è proprio, una caratteristica biometrica appunto*". Cf. Girotto, 2009: 454.

Com base nos vários modelos de smartphones disponíveis actualmente no mercado, podemos enumerar os seguintes métodos de encriptação/desencriptação: a) palavra-passe e *PIN*; b) gesto (padrão desenhado no *touchscreen* conectado com uma série de pontos ou formas); c) impressão digital; d) reconhecimento facial; e) reconhecimento da íris; f) reconhecimento de voz[175].

Na maioria dos casos referidos no primeiro capítulo da presente investigação, o dispositivo móvel que estaria sobre escrutínio seria um iPhone da marca Apple. Por esse motivo, toda a nossa investigação irá centrar-se no método de encriptação/desencriptação implementado em tal smartphone, sem prejuízo de toda a informação apresentada poder ser ainda pertinente para todos os dispositivos que funcionem com os mesmos métodos (quer simultânea quer separadamente).

Actualmente, o iPhone utiliza duas medidas de segurança distintas: a palavra-passe e a impressão digital[176]. Desta forma, serão estes os dois métodos de encriptação e desencriptação que analisaremos ao longo do nosso estudo.

2.3.1. Palavra-passe

A palavra-passe pode ser definida como um código numérico ou alfanumérico que tem como objectivo principal criar uma barreira entre a informação armazenada no smartphone e um terceiro que queira aceder ao dispositivo. Actualmente, as palavras-passe são consideradas o método padrão de encriptação de smartphones[177].

Para comprovar a sua eficácia, é necessário que as palavras-passe sejam resistentes a uma variedade de ataques. Assim, a sua eficiência vai depender da força do *cipher* e do segredo da palavra-passe. Geralmente, quanto maior for a palavra-passe maior será a força da encriptação, uma vez que os *brute-force attacks* vão testar todas as combinações possíveis até chegarem à combinação correcta[178]. De facto, uma palavra-passe longa dificilmente será descoberta, atendendo à actual velocidade e capacidade de processamento de programas de descoberta de palavras-passe e plataformas de smartphones. Numa palavra-passe com 4 dígitos existem 10,000 combinações possíveis, por outro lado, numa palavra-passe alfanumérica com 6 caracteres, o número de combinações possíveis sobe para 139

[175] Choong/Franklin/Greene, 2016: 11-14.
[176] Vogl, 2015: 202.
[177] Choong/Franklin/Greene, 2016: 17.
[178] Colarusso, 2011: 152-153.

biliões[179]. Nesta última hipótese, seriam necessários cerca de cinco anos e meio para conseguir descobrir a palavra-passe correcta e desencriptar o smartphone sem o auxílio do proprietário.

A palavra-passe nos iPhones dos últimos quatro anos é tipicamente composta por 6 dígitos, no entanto, o utilizador poderá optar por uma palavra-passe alfanumérica mais complexa. Por sua vez, os iPhones anteriores a 2012 têm uma palavra-chave padrão de apenas 4 dígitos, sendo que os seus utilizadores também poderão optar por uma palavra-passe alfanumérica.

Em 2010, com o lançamento do novo sistema operativo iOS4, foi introduzida pela Apple a primeira de muitas medidas de segurança e privacidade nos seus produtos: a protecção de correio electrónico e lista de contactos através de encriptação por palavra-passe. No entanto, estes códigos de 4 dígitos eram facilmente descobertos em menos 20 minutos com recurso a ferramentas forenses[180]. Até Outubro de 2014, a Apple possuía capacidades para aceder ao conteúdo (SMS, MMS, fotografias, vídeos, contactos, histórico de chamadas, entre outros) de qualquer dispositivo encriptado da sua marca. Atendendo a esta capacidade, não raras vezes eram feitos pedidos à Apple, por parte das entidades judiciárias, no sentido de lhes serem fornecidos todos os ficheiros armazenados no smartphone, que seriam posteriormente usados como prova em determinada investigação. Com o lançamento do iOS8, em Outubro de 2014, e a consequente melhoria no sistema de total encriptação dos seus dispositivos, a Apple deixa de conseguir aceder aos iPhones, mesmo que a pedido das autoridades judiciárias[181]. Desta melhoria no sistema de encriptação, podemos ainda extrair a possibilidade de activação de uma definição de segurança que permite apagar todos os dados do iPhone após 10 tentativas de introdução da palavra-passe[182].

De facto, a encriptação com palavra-passe tem sido utilizada pelos grandes fabricantes de smartphones como um método padrão de segurança e privacidade. No entanto, como tantos outros métodos de segurança, as palavras-passe têm desvantagens.

O método de encriptação por palavra-passe envolve dois problemas principais.

---

[179] Thompson II/Jaikaran, 2016: 4.
[180] Potapchuk, 2016: 1409.
[181] Jaffer/Rosenthal, 2016: 287-288.
[182] Garfinkel, 2012: 3-4. Disponível em: https://www.technologyreview.com/s/428477/the-iphone-has-passed-a-key-security-threshold/ [consultado em 12.12.2016].

O primeiro tem que ver com a segurança da palavra-passe. Este método de encriptação exige necessariamente que o seu utilizador memorize a combinação. Uma vez que os ataques de força bruta a smartphones são cada vez mais recorrentes, a necessidade de criação de palavras-passe mais longas e complexas é cada vez maior, tornando a sua memorização numa tarefa extremamente difícil[183]. Para agravar a situação, o número de palavras-passe que o utilizador terá de memorizar relativamente a dispositivos de uso profissional ou pessoal também tem aumentado[184]. Quantas mais palavras-passe o utilizador tem de memorizar maior será a probabilidade de errar ou esquecer-se de alguma. Essencialmente, qualquer método de encriptação/desencriptação que envolva a memorização e o segredo de uma palavra-passe ou uma sequência de números por parte do utilizador é falível, dado que os seres humanos são, por natureza, igualmente falíveis.

Por outro lado, para evitar a tarefa de ter de memorizar uma diversidade de palavras-passe longas e complexas, o utilizador acaba por, muitas das vezes, escolher uma palavra-passe curta e fraca[185]. Estas palavras-passe, para além de serem facilmente descobertas através de ataques de força bruta, são ainda passíveis de ser adivinhadas por terceiros[186], dado que não raras vezes os utilizadores utilizam datas de aniversário ou nomes de familiares para protegerem os seus smartphones. Uma outra maneira, diversas vezes utilizada, para evitar memorizar ou, por outro lado, esquecer palavras-passe complexas é anotá-las num papel ou em outro formato. Desta forma, o utilizador estará a comprometer toda a segurança e privacidade do sistema, possibilitando que terceiros (nomeadamente, autoridades judiciárias) encontrem a palavra-passe e acedam ao smartphone.

O segundo problema relacionado com a encriptação por palavra-passe prende-se com a sua falta de conexão directa com o utilizador[187]. Visto que a palavra-passe não tem qualquer ligação com o utilizador, o sistema que executa o algoritmo criptográfico é incapaz de diferenciar entre o utilizador legítimo e um invasor que adquiriu ilicitamente (ou mesmo que licitamente) a palavra-passe. Assim, qualquer terceiro que tome

[183] Keenan, 2016: 5.
[184] Paul/Irvine, 2016: 80.
[185] Rubens, 2012: 3. Disponível em: http://www.esecurityplanet.com/trends/biometric-authentication-how-it-works.html [consultado em 12.12.2016].
[186] Casey, 2002: 107.
[187] Soutar/Roberge/Stoianov/Gilroy/Kumar, 2007: 3. Disponível em: http://www.cse.lehigh.edu/prr/Biometrics/Archive/Papers/BiometricEncryption.pdf [consultado em 12.12.2016].

conhecimento da palavra-passe, seja porque lhe foi concedida ou porque a descobriu, poderá aceder a todo o conteúdo do smartphone.

Atendendo às desvantagens da encriptação por palavra-passe, foi criada uma alternativa: a encriptação biométrica.

2.3.2. Biometria

Para além da encriptação por palavra-passe, existe ainda uma outra tecnologia que permite a protecção de dados sensíveis, esta tecnologia é designada por biometria.

A encriptação/desencriptação biométrica não é uma realidade recente. Já no ano de 1892, o cientista Francis Galton desenvolveu um sistema de classificação para impressões digitais[188]. Vários avanços foram alcançados desde essa altura. Actualmente, o recurso à biometria na encriptação e desencriptação de qualquer dispositivo electrónico é visto como um passo fundamental para a garantia da segurança e privacidade[189].

A biometria é um ramo da biologia que mede e analisa dados biológicos para que as propriedades biológicas de determinada pessoa possam ser usadas para garantir a segurança do seu acesso a determinada informação[190].

Por seu turno, a biométrica pode ser definida como uma característica única, mensurável e biológica cujo objectivo é reconhecer ou verificar automaticamente a identidade de determinado ser humano[191]. Numa outra perspetiva, podemos afirmar que a tecnologia biométrica é utilizada para verificar a identidade de determinada pessoa com base nas suas características físicas ou comportamentais através de meios digitais[192]. A análise

---

[188] National Science and Technology Coucil, 2006: 2. Disponível em: https://www.fbi.gov/file-repository/about-us-cjis-fingerprints_biometrics-biometric-center-of-excellences-fingerprint-recognition.pdf/view [consultado em 13.12.2016].

[189] Keenan, 2016: 6.

[190] Silver, 2012: 813.

[191] "*La biometria è dunque una tecnica che, permettendo di autenticare o identificare un soggetto, trova vasta applicazione in molteplici ambiti, soprattutto laddove si pone una concreta esigenza di garanzia della sicurezza pubblica o privata*". Cf. Girotto, 2009: 455.

[192] Feldman, 2003: 103. Neste sentido vai também a OCDE, que definiu a identificação biométrica como "*the automated use of physiological or behavioural characteristics to determine or verify identity"*. Cf. OCDE, 2004: 10. Disponível em: http://www.oecd-ilibrary.org/docserver/download/232075642747.pdf?expires=1481644102&id=id&accname=guest&checksum=B1A21B7898A864D5763D4AB7F7310AFA [consultado em 13.12.2016].

estatística destas características biológicas ficou conhecida como a "*science of biometrics*"[193].

As impressões digitais, objecto do nosso estudo, são a forma de dados biométricos mais utilizada na encriptação de dispositivos electrónicos.

No entanto, existem outras tecnologias biométricas que são igualmente usadas, são elas: a) o rosto; b) a geometria da palma da mão; c) a marcha/passada; d) a íris; e) a impressão da palma da mão; f) o reconhecimento de voz, entre outros[194].

A tecnologia biométrica, de uma forma geral, é dividida em duas fases distintas: a) o registo (*enrollment*); b) e a verificação (*verification*)[195]. Durante a fase do registo, uma amostra da biométrica designada é obtida (*v.g.* através de microfones ou de *scanners* de impressões digitais)[196]. Posteriormente, algumas das características únicas dessa amostra são extraídas para formar um modelo (*template*) biométrico que será alvo de uma subsequente comparação. Durante a fase da verificação é necessária uma actualização da amostra biométrica, que se obtém através do fornecimento de uma nova amostra. À semelhança do que acontece na fase de registo, características desta nova amostra serão igualmente recolhidas. Por fim, as suas características serão comparadas com o modelo biométrico fornecido anteriormente.

É ainda pertinente, neste âmbito, esclarecer que todas as tecnologias biométricas apresentadas podem ser aplicadas sob duas formas distintas: a) como método de identificação; b) ou como método de autenticação. A identificação biométrica consiste na tarefa de determinar a identidade de uma pessoa desconhecida, ao passo que a autenticação biométrica simplesmente atesta se o indivíduo é quem afirma ser[197].

---

[193] Soutar/Roberge/Stoianov/Gilroy/Kumar, 2007: 1. Disponível em: http://www.cse.lehigh.edu/prr/Biometrics/Archive/Papers/BiometricEncryption.pdf [consultado em 13.12.2016].

[194] Pato/Millett, 2010: 31. Corcoran/Costache, 2016: 70. "S*i è soliti, inoltre, distinguere le caratteristiche biometriche fisiche o fisiologiche da quelle comportamentali. Tra le prime, rientrano principalmente la verifica delle impronte digitali, l'analisi dell'immagine delle dita, il riconoscimento dell'iride, l'analisi della retina, il riconoscimento del volto, la geometria della mano, il riconoscimento della forma dell'orecchio, il rilevamento dell'odore del corpo, il riconoscimento vocale, l'analisi dei pori della pelle, e altro ancora. Tra le seconde, le più utilizzate sono la verifica della firma manoscritta, l'analisi della battitura su tastiera, l'analisi dell'andatura*". Cf. Girotto, 2009: 454.

[195] Soutar/Roberge/Stoianov/Gilroy/Kumar, 2007: 2. Disponível em: http://www.cse.lehigh.edu/prr/Biometrics/Archive/Papers/BiometricEncryption.pdf [consultado em 13.12.2016].

[196] Gelb/Clark, 2013: 62-63.

[197] Corcoran/Costache, 2016: 72.

No processo de autenticação biométrica o utilizador submete a reivindicação da sua identidade ao sistema (através do fornecimento de uma amostra biométrica), sendo que apenas um modelo biométrico é recuperado da base de dados dos utilizadores e comparado com a amostra por si fornecida. A autenticação biométrica é tipicamente usada nas circunstâncias em que é feito um controlo do acesso, seja o acesso físico a uma sala ou edifício, ou o acesso a um sistema eletrónico, como um smartphone[198].

Desta forma, no que concerne ao objecto da nossa investigação, apenas se mostra relevante a autenticação biométrica, uma vez que é a técnica utilizada na encriptação/desencriptação de smartphones. Quando determinado utilizador quiser aceder a um smartphone encriptado através de biometria, terá de fornecer uma amostra biométrica (*v.g.* a sua impressão digital) para que esta seja comparada com o modelo registado. Caso haja correspondência entre a impressão digital fornecida e a impressão digital registada anteriormente, o utilizador vê o acesso ao smartphone autorizado, caso não haja correspondência, o acesso mantém-se interdito. De facto, actualmente, a autenticação biométrica através da impressão digital é, como tivemos oportunidade de salientar anteriormente, um dos métodos mais utilizados na encriptação de smartphones[199].

Este aumento significativo e exponencial do recurso às tecnologias biométricas na encriptação de smartphones não causa estranheza, tomando em consideração todas as vantagens destes métodos.

Contrariamente às palavras-passe, que para serem seguras e "fortes" necessitam da utilização de diversos números, letras e outros caracteres especiais, tornando a tarefa de memorização mais difícil, a encriptação através da biometria não necessita de qualquer processo de memorização[200]. Uma vez que a biometria utiliza as características pessoais

---

198 Soutar/Roberge/Stoianov/Gilroy/Kumar, 2007: 4. Disponível em: http://www.cse.lehigh.edu/prr/Biometrics/Archive/Papers/BiometricEncryption.pdf [consultado em 13.12.2016].

199 "*Fingerprints are a commom biometric used in modern mobile devices over the past several years. Multiple types of fingerprint sensors exist, such as optical, capacitive, and ultrasonic, each with unique ways of assessing characteristics of a biometric sample. In general, fingerprint scanners on mobile devices have a smaller surface area than traditional scanners, affecting resolution, which may impact accuracy*". Cf. Choong/Franklin/Greene, 2016: 13.

200 SaintGermain, 2014a: 8-9. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2367479 [consultado em 14.12.2016].

do utilizador não há qualquer possibilidade de esquecimento ou necessidade de memorização[201]. O próprio utilizador é a palavra-passe, tornando-a única.

Visto que deixa de existir a necessidade de criação de palavras-passe longas e complexas, deixa igualmente de existir a necessidade de as escrever ou guardar, correndo o risco de serem descobertas ou furtadas por terceiros. Na encriptação biométrica não se coloca a possibilidade de furto dos dados biométricos.

Advém da circunstância de o utilizador ser a própria "palavra-passe" do smartphone, a dificuldade de a copiar ou duplicar[202]. Esta vantagem torna o método de encriptação por biometria apropriado para o controlo do acesso a informações pessoais por parte de terceiros não autorizados[203]. Decorre ainda desta circunstância a impossibilidade de partilha dos dados biométricos (*v.g.* impressão digital, voz, íris, rosto) para desencriptação de um determinado smartphone[204].

À medida que a tecnologia se vai desenvolvendo e melhorando ao longo do tempo, também estas técnicas de encriptação/desencriptação de smartphones com recurso à biometria vão aperfeiçoando a sua precisão e robustez[205].

Com a encriptação biométrica, para além de se evitar a inconveniência de se ter de memorizar palavras-passe longas e complexas, deixa de ser necessário estar constantemente a digitar a palavra-passe (longa e complexa) sempre que o utilizador precisa de aceder ao seu smartphone[206]. Dado que um smartphone é desbloqueado, em média, cerca de 48 vezes por dia, esta é uma clara vantagem no que concerne à conveniência do método[207].

---

[201] Chu/Rajendran, 2009: 3-4. Disponível em: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.363.739 [consultado em 14.12.2016].
[202] Keenan, 2016: 6.
[203] SaintGermain, 2014b: 3. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2498707 [consultado em 14.12.2016].
[204] Rubens, 2012: 1. Disponível em: http://www.esecurityplanet.com/trends/biometric-authentication-how-it-works.html [consultado em 14.12.2016].
[205] Keenan, 2016: 7.
[206] Paul/Irvine, 2016: 80-81.
[207] "*Among all biometrics technologies, fingerprint biometrics technology has captured majority of the market share. Ease of usage, low cost and benefits over smart card-based access control systems have fuelled the growth of fingerprint biometrics systems globally. Government projects such as national IDs, e-passports and driving license are also playing a vital role for the growth of biometrics market*". Cf. Hustle, 2014: 1. Disponível em: http://rebelpundit.com/biometrics-and-the-constitution-why-fingerprints-are-less-secure-than-passwords/ [consultado em 14.12.2016].

A encriptação biométrica é vista como uma das formas mais seguras de aceder a qualquer tipo de dispositivo[208]. No que concerne à impressão digital em particular, atendendo à sua natureza singular[209], este método de encriptação acaba por gerar um maior sentimento de segurança e protecção relativamente à informação armazenada no smartphone.

Por fim, é imperativo fazer ainda menção, em sede de vantagens da utilização de encriptação biométrica, à importância que é dada à privacidade na utilização deste método. A título de exemplo, podemos trazer à colação o caso dos sistemas de leitura de impressões digitais, que apenas capturam as principais características da impressão digital e não a impressão digital integral, garantindo assim a privacidade destes dados pessoais[210].

Apesar das claras vantagens que advém da utilização de dados biométricos na encriptação de smartphones, não podemos concluir que esta técnica é completamente perfeita[211]. Nos casos de reconhecimento facial, basta que a luz, o ambiente de fundo ou os ângulos sejam diferentes para que a autenticação não seja possível. Para uma eficaz autenticação ocular é necessário que o olho esteja perfeitamente posicionado para evitar possíveis erros. Por fim, apesar de a leitura da impressão digital ser um dos métodos mais eficazes e mais utilizados, basta que o ângulo ou a pressão aplicada sejam diferentes para inviabilizar a autenticação.

Contrariamente às palavras-passe, os dados biométricos não são secretos[212]. Isto significa que é possível que um terceiro, tomando conhecimento de que um tipo de dado biométrico é utilizado para a encriptação de determinado smartphone, faça uma réplica desse mesmo dado para garantir o acesso ao dispositivo. Frisámos anteriormente que uma das vantagens do recurso a estas técnicas seria, precisamente, a dificuldade de criação de uma réplica. No entanto, com a constante evolução tecnológica e científica, não se descarta a possibilidade da construção de um molde de um dedo com a respectiva impressão

---

[208] Paul/Irvine, 2016: 81.

[209] "*Your fingerprint is one of the best passcodes in the world. It's always with you, and no two are exactly alike…Every fingerprint is unique, so it is rare that even a small section of two separate fingerprints are alike enough to register as a match for Touch ID. The probability of this happening is 1 in 50,000 for one enrolled finger. This is much better than the 1 in 10,000 odds of guessing a typical 4-digit passcode*". Cf. Hustle, 2014: 3. Disponível em: http://rebelpundit.com/biometrics-and-the-constitution-why-fingerprints-are-less-secure-than-passwords/ [consultado em 14.12.2016].

[210] Keenan, 2016: 7.

[211] Feldman, 2003: 110.

[212] Rubens, 2012: 2. Disponível em: http://www.esecurityplanet.com/trends/biometric-authentication-how-it-works.html [consultado em 14.12.2016].

digital[213] ou a utilização de uma fotografia de alta resolução de uma impressão digital para aceder a um smartphone[214].

E como estes dados biométricos consistem em características físicas dos utilizadores, uma das desvantagens fundamentais tem que ver com a sua natureza estática e inalterável. Qualquer característica física de um ser humano é, *a priori*, permanente, pelo que não será viável a alteração ou revogação do modo de acesso ao smartphone[215]. Assim, dada a impossibilidade de revogação do dado biométrico utilizado para aceder ao smartphone, na circunstância de um terceiro ter acesso a esse dado, é criado um risco permanente de acesso às informações armazenadas no dispositivo[216].

No que respeita às considerações físicas sobre a utilização, em particular, de impressões digitais para a encriptação de smartphones, são de apontar algumas desvantagens notórias: este método não funcionará se o utilizador estiver a usar luvas, se o utilizador tiver qualquer tipo de lesão temporária nos dedos ou se, no momento do fornecimento da impressão digital, for detectado algum tipo de humidade ou sujidade que impeça uma leitura bem-sucedida[217].

Uma outra desvantagem destes métodos biométricos de encriptação prende-se com os elevados custos para a sua instalação[218]. No caso concreto dos smartphones, o preço final do aparelho poderá aumentar consideravelmente consoante tenha ou não implementado um sistema de encriptação biométrica.

Por fim, ainda em sede de desvantagens da encriptação biométrica, resta-nos mencionar que, com a divulgação dos atentados praticados contra a privacidade dos utilizadores de dispositivos electrónicos perpetrados pela NSA norte-americana, gerou-se um clima de desconfiança por parte da sociedade em relação à implementação destas novas

---

[213] Paul/Irvine, 2016: 82.
[214] "*For a few German hackers, breaking Apple's much-hyped fingerprint reader seems to have been little more than a one-weekend project. On Sunday, the Berlin-based hacker group known as the Chaos Computer Club - and more specifically a member of the group who goes by the name Starbug - announced that they've managed to crack the iPhone 5s's fingerprint reader just two days after it was released*". Cf. Greenberg, 2013: 1. Disponível em: http://www.forbes.com/sites/andygreenberg/2013/09/22/german-hackers-say-theyve-broken-the-iphones-touchid-fingerprint-reader/#2a8d881167c4 [consultado em 14.12.2016].
[215] Pato/Millett, 2010: 7.
[216] Corcoran/Costache, 2016: 73.
[217] Choong/Franklin/Greene, 2016: 25.
[218] Chu/Rajendran, 2009: 5. Disponível em: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.363.739 [consultado em 14.12.2016].

tecnologias, nomeadamente em smartphones[219]. Assim, os utilizadores de smartphones têm alguma reticência em utilizar este tipo de novas tecnologias, temendo ser alvo de ingerências na sua vida privada por parte do Estado.

Como tivemos oportunidade de esclarecer anteriormente, a nossa investigação irá centrar-se no método de encriptação/desencriptação implementado no iPhone. Assim, depois de analisados os dois métodos de encriptação utilizados pela marca Apple nos seus produtos – a palavra-passe e a biometria - importa agora fazer uma breve referência às particularidades técnicas do seu sistema de encriptação biométrica, o Touch ID.

A técnica da encriptação por impressão digital já existe há alguns anos em diversos dispositivos electrónicos, nomeadamente computadores. No entanto, foi só depois da introdução do Touch ID, em 2013, que a autenticação por impressão digital ganhou notoriedade na área das novas tecnologias[220]. A empresa Apple lançou, em grande parte dos seus produtos (*v.g.* iPhones e iPads), o Touch ID, um leitor de impressões digitais que autoriza o sistema operativo a desbloquear determinadas funcionalidades quando o utilizador toca no sensor, localizado no botão principal do dispositivo. Considerando o facto de que a grande parte dos utilizadores do iPhone não utilizavam a palavra-passe para bloquear o seu smartphone por questões de conveniência, o Touch ID foi criado como uma alternativa menos incómoda[221].

A tecnologia usada no fabrico do Touch ID é uma das formas mais avançadas de *hardware* e *software* alguma vez implementada num smartphone. O sensor consegue captar uma imagem de alta resolução das camadas subepidérmicas da pele localizadas em pequenas secções da impressão digital[222]. O Touch ID tem capacidade para ler diversas impressões digitais, mesmo numa orientação de 360 graus. Após a leitura, é criada uma representação matemática da impressão digital que será comparada às impressões digitais anteriormente registadas no dispositivo. No caso de coincidência entre a impressão digital

[219] Keenan, 2016: 8.
[220] Corcoran/Costache, 2016: 71.
[221] Vogl, 2015: 205.
[222] "*Touch ID then intelligently analyzes this information with a remarkable degree of detail and precision. It categorizes your fingerprint as one of three basic types—arch, loop, or whorl. It also maps out individual details in the ridges that are smaller than the human eye can see and even inspects minor variations in ridge direction caused by pores and edge structures*". Cf. Apple Support – About Touch ID security on iPhone and iPad. Disponível em: https://support.apple.com/en-us/HT204587 [consultado em: 14.12.2016].

fornecida e a impressão digital registada, o dispositivo é desbloqueado automaticamente[223].

É ainda possível que o utilizador do smartphone aumente a segurança do seu dispositivo escolhendo, em simultâneo com a impressão digital, uma palavra-passe composta por 4 ou 6 números, letras ou outros caracteres especiais.

O Touch ID pode ser usado para desbloquear mais rapidamente o dispositivo, prevenir o acesso de terceiros não autorizados[224], instalar novas aplicações e fazer compras através das aplicações instaladas[225].

Caso o iPhone seja furtado ou perdido, é possível desactivar à distância, através da aplicação *Find My iPhone*, a definição que permite a autenticação através do Touch ID.

O Touch ID não armazena fotografias das impressões digitais[226], o que fica registado são apenas representações matemáticas das impressões, ou seja, um longo número, que funciona como uma segunda palavra-passe, composto por 50 a 100 dígitos[227], designado de *biometric hash*[228]. Assim, não será possível que um terceiro consiga reverter este processo de maneira a criar uma imagem da impressão digital através da representação matemática registada.

O registo destas representações fica armazenado no smartphone, mais precisamente, no A7 CPU[229], denominado de "*secure enclave*". A *secure enclave* foi desenvolvida com o propósito de proteger a palavra-passe e os dados biométricos armazenados no smartphone. Os dados biométricos são encriptados e protegidos com uma palavra-chave apenas disponível para a *secure enclave*, que se encontra separada do resto do sistema operativo. Desta forma, nenhuma aplicação nem o próprio sistema iOS (incluindo a iCloud) têm acesso às representações matemáticas das impressões digitais fornecidas.

---

[223] Apple Support – About Touch ID security on iPhone and iPad. Disponível em: https://support.apple.com/en-us/HT204587 [consultado em 15.12.2016].
[224] Whittaker, 2013: 3. Disponível em: http://www.smartsuite.in/iphone-5s-fingerprint-reader-doubling-down-on-identity-a-death-knell-to-zdnet.html [consultado em 15.12.2016].
[225] Tabini, 2014: 2. Disponível em: http://www.macworld.com/article/2455474/open-sesame-how-ios-8-will-unlock-touch-ids-power.html [consultado em 15.12.2016].
[226] Apple Support – About Touch ID security on iPhone and iPad. Disponível em: https://support.apple.com/en-us/HT204587 [consultado em 15.12.2016].
[227] Pagliery, 2016: 2. Disponível em: http://money.cnn.com/2016/05/12/technology/fbi-fingerprint-iphone/ [consultado em 15.12.2016].
[228] Tabini, 2014: 3. Disponível em: http://www.macworld.com/article/2455474/open-sesame-how-ios-8-will-unlock-touch-ids-power.html [consultado em 15.12.2016].
[229] Tarantola, 2013: 1. Disponível em: http://gizmodo.com/stop-worrying-about-the-new-iphones-fingerprint-scanne-1326146704 [consultado em 15.12.2016].

Apesar da activação do Touch ID, podem surgir situações em que é necessário a introdução da palavra-passe para aceder ao smartphone: a) se o dispositivo for reiniciado; b) se a impressão digital não for reconhecida cinco vezes consecutivas; c) se o dispositivo não tiver sido desbloqueado há mais de 48 horas[230]; d) se tiverem sido registadas ou apagadas impressões digitais recentemente; e) se o utilizador tentar aceder às definições do Touch ID.

3. Conclusões intermédias

Atendendo a tudo o que ficou dito durante este capítulo, nomeadamente quanto à constante evolução da tecnologia e ao papel fundamental da informação na sociedade actual, percebe-se a necessidade sentida pelos particulares no sentido de protegerem os seus smartphones. Dada a sua vasta capacidade de armazenamento, estes dispositivos tornaram-se, ao longo do tempo, objecto de curiosidade, tanto para outros particulares como para o Estado, levando a que os seus fabricantes incluíssem, nas suas definições, a encriptação como uma medida de segurança básica. De facto, a encriptação é vista, hoje em dia, como uma tecnologia cuja função primordial é minimizar os riscos de acesso, por parte de terceiros não autorizados, a informações pessoais[231].

Isto posto, não causa estranheza que, não raras vezes, as autoridades judiciárias, no âmbito de uma investigação criminal, depois de apreenderem um smartphone, se deparem com a impossibilidade do acesso aos ficheiros aí armazenados provocada pela sua prévia encriptação. As vantagens do recurso a este tipo de tecnologia para o titular do dispositivo encriptado são, como vimos, inegáveis, no entanto, no caso concreto de estarmos no âmbito de uma investigação criminal e de a encriptação impedir o acesso das autoridades judiciárias a provas potencialmente fundamentais para o processo penal, as vantagens dão lugar a claras desvantagens.

Ao longo deste terceiro capítulo tivemos oportunidade de enunciar as diversas complexidades tecnológicas associadas à encriptação de smartphones. E, são essas mesmas complexidades que diminuem, em larga escala, as possibilidades de as autoridades judiciárias conseguirem apreender eficientemente os ficheiros armazenados num smartphone encriptado sem o auxílio do arguido. É precisamente neste ponto que

[230] O que sucedeu em alguns dos casos enunciados no Capítulo I do presente estudo.
[231] Lowman, 2010: 1. Disponível em: https://www.lowmanio.co.uk/share/The%20Effect%20of%20File%20and%20Disk%20Encryption%20on%20Computer%20Forensics.pdf [consultado em 15.12.2016].

entra em discussão a questão central da nossa investigação, que iremos tratar, em pormenor, no próximo capítulo: a articulação entre a desencriptação de smartphones e o direito do arguido à não-autoincriminação.

CAPÍTULO IV – A DESENCRIPTAÇÃO DE SMARTPHONES PARA OBTENÇÃO DE PROVA E A SUA ARTICULAÇÃO COM O PRINCÍPIO DA NÃO-AUTOINCRIMINAÇÃO

1. Colocação do problema

Actualmente, a encriptação de smartphones é uma tecnologia de livre acesso e facilmente adquirida. No entanto, não raras vezes esta tecnologia é usada pelos piores motivos, como tivemos oportunidade de perceber pela análise dos casos jurisprudenciais norte-americanos que serão objecto do nosso estudo ao longo deste quarto capítulo.

Nestes casos, a utilização da encriptação em smartphones representa um perigo, em especial, para a defesa da segurança nacional e para a persecução da justiça[232]. Isto porque, em abstracto, a possibilidade de ocultar informação de terceiros, nomeadamente do Estado, faz da encriptação um instrumento atractivo para criminosos[233]. De facto, os suspeitos de actividades ilegais como lavagem de dinheiro, fraude, terrorismo, pornografia infantil, homicídio, abuso sexual, entre outros, serão mais facilmente ilibados[234] se as potenciais provas do crime estiverem armazenadas num smartphone encriptado.

Através da encriptação dos smartphones, os criminosos tornam quase impossível o acesso, por parte das entidades judiciárias, ao conteúdo do dispositivo. Durante o processo criminal é comum que as autoridades consigam ter acesso à palavra-passe, seja porque foi escrita num papel ou, porque simplesmente era fácil de adivinhar (*v.g.* data de nascimento do arguido ou um nome de um familiar). No caso de tal não se verificar, existe ainda a possibilidade de desencriptar o smartphone através dos já mencionados *brute-force attacks*[235].

Contudo, ainda que assumindo que as autoridades judiciárias têm todos os meios técnicos necessários para desencriptar o smartphone, surge a questão: será que os custos e tempo

[232] Martins/Marques/Dias, 2004: 70.
[233] Ungberg, 2009: 552. Neste sentido, "[…] a circulação livre desta tecnologia permitirá que qualquer um possa transmitir informações virtualmente indecifráveis para terceiros, construindo desse modo um espaço virtual '*no man's land'*, onde o desenvolvimento e planeamento de actividades criminosas, terroristas e de outras actividades contrárias à garantia da segurança dos Estados fossem livres". Cf. Martins/Marques/Dias, 2004: 71.
[234] Weinberg, 1998: 680.
[235] Sales, 2014: 208.

despendidos no desbloqueio do dispositivo serão justificados atendendo ao facto de que as autoridades não têm qualquer informação sobre o conteúdo do smartphone?[236]

Há ainda que ponderar um outro ponto: mesmo na circunstância de a desencriptação ser bem-sucedida, é possível que a recolha de prova do smartphone não seja célere o suficiente para dar resposta ao crime em questão.

Por estes motivos e tantos outros, muitas das vezes, a única maneira viável de conseguir aceder ao conteúdo do smartphone passa pela colaboração do proprietário (arguido)[237]. Desta forma, as autoridades judiciárias teriam de compelir o arguido a fornecer a palavra-passe ou a sua impressão digital para desencriptar o dispositivo[238].

No entanto, a coacção do arguido no sentido de fornecer tanto a palavra-passe quanto a impressão digital para desencriptar o seu smartphone, onde potencialmente estarão armazenadas provas incriminatórias de um delito que cometeu, levanta preocupações quanto a uma possível violação do brocardo latino *nemo tenetur se ipsum accusare* ou, o princípio de não-autoincriminação.

Para conseguirmos dar resposta a esta problemática mostra-se necessário fazer uma divisão entre duas sub-hipóteses, uma vez que estamos a tratar de dois métodos de encriptação diferenciados: a palavra-passe e a impressão digital. Assim, poderá o arguido ser compelido a fornecer às entidades judiciárias a palavra-passe que desencripta o smartphone sem violar o seu direito à não-autoincriminação? Ou ainda, poderá o arguido ser coagido a fornecer a sua impressão digital com vista a desencriptar o smartphone sem violar o seu direito à não-autoincriminação? Até que ponto será exigível uma colaboração processual do arguido tendo em conta os limites impostos pelo seu estatuto processual?[239]

Para percebermos como o princípio de não-autoincriminação poderá, nestas duas situações, ser ou não violado, torna-se imperativo que façamos *a priori* uma reflexão sobre o brocardo latino *nemo tenetur se ipsum accusare*.

[236] Duong, 2009: 328.
[237] Atwood, 2015: 410.
[238] Gershowitz, 2010: 22. Disponível em: https://papers.ssrn.com/sol3/papers2.cfm?abstract_id=1669403 [consultado em 15.12.2016].
[239] Pinto, 2013: 92.

2. O princípio *nemo tenetur se ipsum accusare*

O princípio *nemo tenetur se ipsum accusare* teve a sua origem no Reino Unido, no séc. XVII, como reacção às práticas inquisitoriais dos tribunais eclesiásticos[240]. Desde então o princípio assistiu a inúmeras mudanças e evoluções, culminando no entendimento de que ao arguido cabe decidir se, como e quando está disposto a contribuir para a sua própria incriminação[241]. Assim, no seu sentido mais profundo, a garantia do *nemo tenetur* visa evitar que o arguido seja transformado em colaborador involuntário das entidades públicas com competências processuais[242], sendo portanto, um princípio estruturante do modelo processual acusatório e do sistema democrático.

Este princípio, ou privilégio, está estreitamente ligado à liberdade de declaração do arguido, que é analisada pela doutrina e pela jurisprudência do Tribunal Constitucional numa dupla dimensão, positiva e negativa. Pela positiva, "abre ao arguido o mais restrito direito de intervenção e declaração em abono da sua defesa e pela negativa, a liberdade de declaração do arguido veda todas as tentativas de obtenção, por meios enganosos ou por coacção, de declarações autoincriminatórias"[243].

A doutrina nacional, e mesmo internacional, defende a ideia de que o princípio *nemo tenetur* implica que ninguém pode ser obrigado a contribuir para estabelecer a sua própria incriminação[244]. Deste modo, de um ponto de vista menos amplo, o princípio pressupõe que ninguém é obrigado a produzir prova ou a praticar actos lesivos à sua própria defesa[245].

Neste sentido vai também a jurisprudência nacional que, no que concerne ao conteúdo deste princípio, vem estabelecer que "o privilégio contra a autoincriminação significa que o arguido não pode ser obrigado, nem deve ser condicionado a contribuir para a sua própria incriminação, isto é, tem o direito a não ceder ou fornecer informações ou

---

[240] Pinto, 2013: 100.
[241] Ramos, 2010: 179.
[242] Silva Dias, 2010: 242.
[243] Costa Andrade, 1992: 120. Neste sentido, Acórdão do Tribunal Constitucional n.º 304/2004, de 5 de Maio de 2004, disponível em: http://www.tribunalconstitucional.pt/tc/acordaos/20040304.html [consultado em 17.01.2017].
[244] Pinto, 2013: 104. Oliveira Silva, 2013: 364. Neves/Correia, 2014: 146. Cruz Bucho, 2013: 18. Disponível em: https://www.trg.pt/ficheiros/estudos/sobre_a_recolha_de_autografos_do_arguido.pdf [consultado em 17.01.2017]. Anastácio, 2010: 205. Haddad, 2003: 37.
[245] Ristori, 2007: 98. Neste sentido vai também Costa Andrade ao referir que "[…] o arguido não pode ser fraudulentamente induzido ou coagido a contribuir para a sua condenação, *i.e.*, a carrear ou oferecer meios de prova contra a sua defesa. Quer no que toca aos factos relevantes para a chamada questão da culpabilidade quer no que respeita aos atinentes à medida da pena". Cf. Costa Andrade, 1992: 121.

elementos (*v.g.*, documentais) que o desfavoreçam, ou a não prestar declarações, sem que do silêncio possam resultar quaisquer consequências negativas ou ilações desfavoráveis no plano da valoração probatória"[246]. Já o Tribunal Constitucional vem afirmar que "o princípio *nemo tenetur se ipsum accusare*, é uma marca irrenunciável do processo penal de estrutura acusatória, visando garantir que o arguido não seja reduzido a mero objecto da actividade estadual de repressão do crime, devendo antes ser-lhe atribuído o papel de verdadeiro sujeito processual, armado com os direitos de defesa e tratado como presumivelmente inocente. Daí que para protecção da autodeterminação do arguido, este deva ter a possibilidade de decidir, no exercício de uma plena liberdade de vontade, qual a posição a tomar perante a matéria que constitui objecto do processo"[247].

O princípio *nemo tenetur se ipsum accusare*, que consubstancia, para Paulo de Sousa Mendes, "um dos pilares do processo penal português"[248], desdobra-se em dois corolários que, embora intimamente relacionados, não se confundem entre si[249]: o princípio contra a autoincriminação em sentido estrito e o direito ao silêncio. O princípio contra a autoincriminação em sentido estrito traduz-se no direito de não cooperar na investigação[250], ou seja, no fornecimento de quaisquer meios de prova susceptíveis de comprometer a presunção de inocência do arguido, coadjuvando a sua incriminação, nomeadamente, através da entrega de documentos ou outros elementos ou através de uma determinada actuação[251]. Já no que concerne ao direito ao silêncio, este abarca apenas a colaboração do arguido na sua incriminação através de declarações sobre os factos que lhe são imputados. Deste modo, como bem refere Maria Fernanda Palma, é sobre a justiça

---

[246] Acórdão do Tribunal da Relação de Coimbra, de 23 de Outubro de 2013, disponível em: http://www.dgsi.pt/jtrc.nsf/c3fb530030ea1c61802568d9005cd5bb/d3a8f7db2f94ad6180257c0f0052958b?OpenDocument [consultado em 17.01.2017].

[247] Cf. Acórdão do Tribunal Constitucional n.º 340/2013, de 17 de Junho de 2013, disponível em: http://www.tribunalconstitucional.pt/tc/acordaos/20130340.html [consultado em 17.01.2017].

[248] Sousa Mendes, 2017: 210.

[249] Martins, 2015: 24. Em sentido contrário, apoiando-se na tese de que o direito ao silêncio e o princípio contra a autoincriminação são sinónimos para descrever uma mesma realidade, pronunciou-se o Tribunal da Relação de Évora, afirmando que "o privilégio contra a autoincriminação ou direito ao silêncio significa que o arguido não pode ser obrigado, nem deve ser condicionado a contribuir para a sua própria incriminação, isto é, tem o direito a não ceder ou fornecer informações ou elementos que o desfavoreçam, ou a não prestar declarações, sem que do silêncio possam resultar quaisquer consequências negativas ou ilações desfavoráveis no plano da valoração probatória". Cf. Acórdão do Tribunal da Relação de Évora, de 30 de Setembro de 2008, disponível em: http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/986b0759b8e0108880257de100574d46?OpenDocument [consultado em 17.01.2017].

[250] Cruz, 2011: 22.

[251] Neves/Correia, 2014: 146.

do Estado que recai o ónus de demonstrar os factos da acusação[252]. O direito ao silêncio é assim o direito de calar, o reconhecimento da liberdade moral do arguido[253]. Por seu turno, Vânia Costa Ramos vem salientar, e bem, que "sem o direito ao silêncio, o arguido seria obrigado a declarar e cooperar sempre que estes actos não revestissem conteúdo autoincriminatório"[254]. A Autora, conjuntamente com Augusto Silva Dias, vai mais longe, chegando a afirmar que o direito ao silêncio é o núcleo duro e quase absoluto do *nemo tenetur*, tanto por razões históricas como pelo regime legal que o acolhe[255].

2.1. Consagração

O princípio *nemo tenetur se ipsum accusare* é consagrado na maioria das constituições dos modernos Estados de Direito. Nos casos de falta de consagração expressa na lei fundamental, acaba por ser reconhecido ao abrigo das suas disposições. Este princípio, ou privilégio, encontra ainda acolhimento em importantes documentos internacionais de protecção dos direitos do Homem, entre os quais a Convenção Europeia dos Direitos do Homem e o Pacto Internacional sobre Direitos Cívicos e Políticos da ONU[256], como princípio essencial do processo penal.

De acordo com a alínea g) do n.º 3 do artigo 14.º do Pacto Internacional sobre Direitos Cívicos e Políticos, "Qualquer pessoa acusada de uma infracção penal terá direito, em plena igualdade, pelo menos às seguintes garantias: g) A não ser forçada a testemunhar contra si própria ou a confessar-se culpada".

Por seu turno, a Convenção Europeia dos Direitos do Homem (CEDH), no seu articulado, não prevê de forma explícita o direito ao silêncio ou o direito à não-autoincriminação. Contudo, segundo o entendimento da jurisprudência do Tribunal Europeu dos Direitos Humanos (TEDH), o princípio *nemo tenetur* constitui um *standard* internacional, que está presente no núcleo da noção de processo equitativo, o qual se destina a proteger o arguido contra o exercício abusivo de poderes coercivos pelas autoridades, a evitar o perigo de adulteração da justiça e, nesse sentido, a assegurar a realização plena do artigo 6.º da Convenção[257]. Segundo aquela jurisprudência, o princípio *nemo tenetur se ipsum*

[252] Palma, 2009: 1. Disponível em: http://www.idpcc.pt/xms/files/Newsletters/Boletim_Ano1_Ed1_Dez08Jan09.pdf [consultado em 17.01.2017].
[253] Queijo, 2012: 233.
[254] Ramos, 2007: 68.
[255] Silva Dias/Ramos, 2009: 20.
[256] Silva, 2007: 59.
[257] Cruz Bucho, 2013: 20.

accusare relaciona-se, em primeira linha, com o respeito pela vontade da pessoa do arguido em permanecer em silêncio e constitui uma decorrência do pressuposto segundo o qual a acusação deverá provar a sua tese contra o acusado sem o recurso a elementos de prova obtidos através de métodos coercivos ou opressivos com desrespeito pela vontade deste[258]. Assim, o direito ao silêncio e o princípio contra a autoincriminação em sentido estrito encontram-se intimamente relacionados com a presunção de inocência consagrada no n.º 2 do artigo 6.º da Convenção Europeia dos Direitos do Homem.

Por conseguinte, por força do disposto nos n.os 1 e 2 do artigo 8.º da Constituição da República Portuguesa, pode sustentar-se que ambos os preceitos vigoram directamente na ordem jurídica interna[259].

Contrariamente ao que sucede com inúmeras Constituições e declarações de direitos de outros países, nomeadamente a Constituição americana (5.ª Emenda)[260], a Constituição espanhola (artigos 17.3 e 24.2)[261] ou a Constituição brasileira (artigo 5.º, inciso LXIII)[262], a Constituição portuguesa não consagra, à semelhança da Lei Fundamental alemã e italiana, o princípio *nemo tenetur se ipsum accusare* de uma forma expressa e directa. Não obstante o princípio *nemo tenetur* – seja na sua vertente de direito ao silêncio do arguido, seja na sua dimensão de princípio contra a autoincriminação em sentido estrito – não estar expressa e directamente plasmado no texto constitucional, a doutrina[263] e a jurisprudência[264] portuguesas, em similitude com a doutrina e jurisprudência alemãs, são unânimes não só quanto à vigência daquele princípio no direito processual penal, como

[258] Cruz Bucho, 2013: 21.
[259] Andrade, 2014: 19.
[260] Estabelece a Quinta Emenda à Constituição dos Estados Unidos da América: "Nenhuma pessoa será obrigada, em qualquer caso criminal, a ser uma testemunha contra si mesma".
[261] No seu artigo 24.2, a Constituição espanhola consagra que todos têm direito "[…] a não declarar contra si mesmo e a não se confessar culpado", assim como no artigo 17.3 se prevê o princípio segundo o qual ninguém será obrigado a fazer declaração que possa resultar em autoincriminação, impondo às autoridades responsáveis a obrigação de prévia informação acerca dos direitos e da acusação que recaem sobre o suspeito.
[262] Prevê o inciso LXIII do artigo 5.º da Constituição brasileira que "o preso será informado de seus direitos, entre os quais o de permanecer calado, sendo-lhe assegurada a assistência da família e de advogado".
[263] Cruz Bucho, 2013: 22. Sousa Mendes, 2010: 125. Pinto, 2013: 105. Catarina Anastácio fala aqui numa "[…] base constitucional (ainda que indirecta ou implícita) deste direito […]". Cf. Anastácio, 2010: 206.
[264] "A Constituição da República Portuguesa não consagra *expressis verbis* este princípio, mas, não obstante essa não consagração expressa, tanto a doutrina como a jurisprudência têm defendido que o *nemo tenetur se ipsum accusare* tem assento constitucional, sendo considerado um direito constitucional do processo penal não escrito". Cf. Acórdão do Tribunal Constitucional n.º 340/2013, de 17 de Junho de 2013, disponível em: http://www.tribunalconstitucional.pt/tc/acordaos/20130340.html: [consultado em 18.01.2017].

quanto à sua natureza constitucional[265]. Fala-se aqui no *nemo tenetur se ipsum accusare* como um verdadeiro "direito constitucional não escrito"[266].

No que à lei processual penal portuguesa diz respeito, este princípio obteve consagração expressa no Código de Processo Penal, na vertente de direito ao silêncio do arguido (artigos 61.º, n.º 1, alínea d), 141.º, n.º 4, alínea a), 343.º, n.º 1, e 345.º, n.º 1, *in fine*)[267]. Assim, a alínea d) do n.º 1 do artigo 61.º estabelece que: "O arguido goza, em especial, em qualquer fase do processo e salvas as excepções da lei, dos direitos de: 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". O direito ao silêncio estende-se mesmo ao próprio suspeito, desde logo porque a pessoa sobre quem recair a suspeita de ter cometido um crime tem direito a ser constituída, a seu pedido, como arguido (n.º 2 do artigo 59.º do CPP). Também a "testemunha não é obrigada a responder a perguntas quando alegar que das respostas resulta a sua responsabilização penal" (n.º 2 do artigo 132.º do CPP)[268]. O direito ao silêncio de que goza o arguido deve ser-lhe comunicado pela autoridade judiciária ou pelo órgão de polícia criminal perante as quais seja obrigado a comparecer (al. h) do n.º 1 do artigo 61.º do CPP), sob pena de as declarações feitas constituírem prova proibida por intromissão na vida privada (n.º 8 do artigo 32.º da CRP, e n.º 3 do artigo 126.º do CPP)[269]. O exercício deste direito ao silêncio não pode ser valorado como indício ou presunção de culpa[270][271].

[265] Figueiredo Dias/Costa Andrade, 2009: 39.
[266] Costa Andrade, 1992: 124.
[267] Como bem refere Costa Andrade, "a lei processual penal portuguesa contém uma malha desenvolvida e articulada de normas através das quais se assenta o princípio *nemo tenetur*". Cf. Costa Andrade, 1992: 126.
[268] Sousa Mendes, 2017: 209-210. Curado, 2012: 262.
[269] Marques da Silva, 2013: 74.
[270] "O conteúdo material do referido princípio (*nemo tenetur*...) é assegurado através da imposição de deveres de esclarecimento ou de advertência às autoridades judiciárias e aos órgãos de polícia criminal [cfr. artigos 58.º, n.º 2; 61.º, n.º 1, alínea g); 141.º, n.º 4 e 343.º, n.º 1], estabelecendo-se a sanção de proibição de valoração, nos termos do artigo 58.º, n.º 4 e da nulidade das provas obtidas mediante tortura, coacção ou ofensa da integridade física ou moral (cfr. artigo 126.º, n.º 1, todos do CPP)". Cf. Acórdão do Tribunal Constitucional n.º 304/2004, de 5 de Maio de 2004, disponível em: http://www.tribunalconstitucional.pt/tc/acordaos/20040304.html [consultado em 18.01.2017]. "[…] o arguido deve ser informado, antes de qualquer interrogatório, de que goza do direito ao silêncio (artigos 141.º, n.º 4, 143.º, n.º 2, 144.º, n.º 1, e 343.º, n.º 1, do CPP), devendo também ser esclarecido de que o seu silêncio não pode ser interpretado desfavoravelmente aos seus interesses, não podendo, por isso, o arguido ser prejudicado por ter exercitado o seu direito a não prestar quaisquer declarações (o silêncio não pode ser interpretado como presunção de culpa). Cf. Acórdão do Tribunal Constitucional n.º 696/95, de 5 de Dezembro de 1995, disponível em: http://www.tribunalconstitucional.pt/tc/acordaos/19950695.html [consultado em 18.01.2017].
[271] Sá, 2004: 187.

Chegados a este ponto, torna-se necessário chamar à colação as duas extensões do direito ao silêncio, consagrado no artigo 61.º do Código de Processo Penal, discutidas na doutrina: a) a extensão minimalista, incidindo apenas sobre as declarações do arguido em sentido estrito e sobre os factos que lhe são imputados; b) a extensão maximalista, abarcando as declarações por meio de documentos, da indicação do lugar onde se encontra o meio de prova, de uma actuação, consubstanciando-se num direito a não ser obrigado a fornecer prova (documental, declarativa, ou outra) da sua culpabilidade[272]. A maioria da doutrina nacional defende a tese de que estamos aqui perante uma variante ampla do direito ao silêncio[273]. Assim, malgrado a redacção do referido artigo 61.º do Código de Processo Penal sugira um direito restrito aos casos em que o arguido é solicitado a prestar declarações verbais, somos da opinião de que uma interpretação teleológica da norma aponta para que a invocação deste direito não esteja dependente dos meios utilizados, mas dos fins que se pretendem alcançar e dos interesses que sejam postos em causa, designadamente o da não-autoincriminação, sob pena de esses expedientes serem utilizados como forma de contornar um direito fundamental dos cidadãos[274]. Desta forma, poderia estar aqui incluído não só o fornecimento da palavra-passe através de declarações orais como também através de declarações escritas ou gestuais[275].

Por fim, resta deixar claro que este direito ao silêncio consagrado no artigo 61.º do Código de Processo Penal não pode ser visto como direito absoluto. Na verdade, este direito do arguido está submetido a algumas restrições no processo penal[276], nomeadamente no que toca à sua identificação pessoal (alínea b) do n.º 3 do artigo 61.º do CPP)[277]. Tanto em sede de primeiro interrogatório judicial (n.º 3 do artigo 141.º do CPP) como em fase de julgamento (artigo 342.º do CPP), o arguido é obrigado a responder com verdade acerca da sua identificação, sob pena de incorrer em crime de desobediência (artigo 349.º do Código Penal) ou falsas declarações (artigo 359.º do Código Penal).

---

[272] Pinto, 2013: 108-109.
[273] Silva Dias, 2010: 244.
[274] Sá, 2004: 188. Neste sentido vai também Augusto Silva Dias quando afirma que "[…] uma compreensão do problema menos legal-positivista e mais sensível à Constituição e aos direitos obriga a considerar que a garantia vigora também perante outros actos comunicativos (orais, escritos, gestuais) através dos quais o suspeito pode contribuir para a sua própria inculpação". Cf. Silva Dias, 2010: 244.
[275] "As manifestações verbais não são as únicas formas em que se apresenta o princípio contra a autoincriminação, pois, através de outras condutas, é possível produzir prova de carácter incriminatório, utilizável contra quem a produziu". Cf. Cruz Bucho, 2013: 30.
[276] Sousa Mendes, 2017: 210.
[277] Curado, 2012: 262-263.

À semelhança do direito ao silêncio, também o princípio contra a autoincriminação em sentido estrito não poderá ser considerado como um direito absoluto[278]. A título de exemplo, podemos mencionar a possibilidade de sujeição a exames, consagrada no artigo 172.º do Código de Processo Penal, como sendo uma clara limitação ao direito de não facultar provas contra si próprio. Voltaremos a este tema mais adiante.

2.2. Fundamentos jurídicos

Actualmente, não é tanto o reconhecimento legal e constitucional do princípio *nemo tenetur se ipsum accusare* que suscita dificuldades, quanto a determinação exacta do seu fundamento e conteúdo.

É usual enquadrar os fundamentos constitucionais do *nemo tenetur* em duas espécies distintas, concebendo-o, alternativamente, como direito material de liberdade (corrente substantiva) ou como garantia processual fundamental (corrente processual)[279].

Segundo a corrente substantiva, defendida pela doutrina maioritária alemã, o fundamento deste princípio estaria enraizado em alguns direitos fundamentais que fundar-se-iam directamente, na dignidade da pessoa humana, proclamada no artigo 1.º da Constituição da República Portuguesa. Ainda dentro desta mesma corrente, outros Autores concebem aquele princípio como reflexo dos direitos à integridade pessoal e ao desenvolvimento da personalidade, vertidos nos artigos 25.º e 26.º da CRP[280].

Por outro lado, segundo a corrente processualista, o direito ao silêncio e à não-autoincriminação teriam a sua fonte jurídico-constitucional nas garantias processuais reconhecidas ao arguido no texto constitucional, designadamente no princípio do processo equitativo e no princípio da presunção de inocência, consagrados, respectivamente, no n.º 4 do artigo 20.º, e nos n.os 2 e 8 do artigo 32.º, ambos da CRP[281].

Não obstante os direitos do arguido, consagrados, nomeadamente, no artigo 61.º do Código de Processo Penal, contribuírem activamente para a protecção de direitos fundamentais como a dignidade da pessoa humana, estamos com Figueiredo Dias e Costa

[278] Sousa Mendes, 2017: 210. Neste sentido, cf. Acórdão do Tribunal Constitucional n.º 696/95, de 5 de Dezembro de 1995, disponível em: http://www.tribunalconstitucional.pt/tc/acordaos/19950695.html [consultado em 18.01.2017]. Cf. Acórdão do Tribunal Constitucional n.º 372/98, de 13 de Maio de 1998, disponível em: http://www.tribunalconstitucional.pt/tc/acordaos/19980372.html [consultado em 18.01.2017].
[279] Oliveira Silva, 2013: 370.
[280] Figueiredo Dias/Costa Andrade, 2009: 40.
[281] Menezes, 2010: 124-125.

Andrade quando defendem que o facto de estes direitos processuais serem "um meio ou forma de concretizar um determinado direito fundamental não implica que este seja o seu fundamento directo e imediato. Desde logo se aponta que o próprio conceito de dignidade humana recobre de forma mediata toda a matéria penal e processual penal de um Estado de Direito"[282]. Assim, apesar de se defender na doutrina portuguesa a corrente processualista, é também aceite que o princípio *nemo tenetur* protege reflexamente os direitos fundamentais referidos pela corrente substantiva[283].

A jurisprudência nacional, nomeadamente, a do Tribunal Constitucional, vem concluir que o princípio *nemo tenetur* configura "uma componente das garantias de defesa asseguradas no artigo 32.º da CRP, cujo objectivo último é a protecção do arguido como sujeito no processo"[284]. Daqui decorre que a posição do Tribunal Constitucional se harmoniza com a posição da doutrina, optando também pela corrente processualista do princípio *nemo tenetur se ipsum accusare*[285].

É assim de concluir que, em Portugal, o entendimento maioritário defende que o princípio *nemo tenetur se ipsum accusare* encontra o seu fundamento imediato nas garantias processuais que a Constituição impõe, no artigo 32.º da Lei Fundamental, cumprindo-se de igual modo a exigência constitucional de um processo penal equitativo, prevista no n.º 4 do artigo 20.º da CRP[286].

No entanto, esta não é uma questão puramente teórica pois, como bem assinala Vânia Costa Ramos, se um direito fundado na dignidade da pessoa humana é "um direito de natureza tendencialmente absoluta", já um direito fundado em garantias processuais poderá ser sujeito a certas limitações"[287]. Assim, não causa estranha afirmar, na decorrência do que já ficou escrito relativamente às limitações do direito ao silêncio e do direito à não-autoincriminação em sentido estrito, que o próprio princípio *nemo tenetur se ipsum accusare* não constitui um princípio absoluto, pelo que comporta restrições justificadas (*v.g.* al. b) do n.º 3 do artigo 61.º e artigo 172.º, ambos do CPP)[288].

---

[282] Figueiredo Dias/Costa Andrade, 2009: 41.
[283] Pinto, 2013: 106.
[284] Cf. Acórdão do Tribunal Constitucional n.º 696/95, de 5 de Dezembro de 1995, disponível em: http://www.tribunalconstitucional.pt/tc/acordaos/19950695.html [consultado em 18.01.2017].
[285] Pinto, 2013: 107.
[286] Figueiredo Dias/Costa Andrade, 2009: 42.
[287] Ramos, 2007: 58 e 73.
[288] Cruz Bucho, 2013: 24.

2.3. Limitações

No processo acusatório, coaduna-se a investigação da verdade material aos pressupostos do Estado de Direito, limitando-a, assim, pela observância escrupulosa dos direitos, liberdades e garantias dos cidadãos. Desta forma, não causa estranheza que se assegure ao arguido a posição de sujeito[289], dotado de um real e efectivo direito de defesa[290].

De facto, o caminho trilhado por este processo penal reformulado, vai no sentido de assegurar ao arguido uma cada vez mais consistente e efectiva condição de sujeito, ao invés de mero meio de prova[291]. No entanto, como já tivemos oportunidade de analisar ao longo da nossa investigação, muitas vezes, o arguido, no seio de uma investigação criminal, acaba por ser sujeito a certas diligências, sendo utilizado como meio de prova[292][293].

Na doutrina, Figueiredo Dias afasta a existência de um dever abstracto de colaboração do arguido[294], na medida em que exige que "a utilização do arguido como meio de prova seja sempre limitada pelo integral respeito da sua vontade", adiantando ainda que "só no exercício de uma plena liberdade da vontade pode o arguido decidir se e como deseja tomar posição perante a matéria que constitui objecto do processo"[295]. Na mesma esteira, mais recentemente, Paulo Pinto de Albuquerque veio defender a ideia de que o arguido

[289] "O arguido é um sujeito processual e, em regra, não pode ser utilizado, contra sua vontade, como fonte de prova contra si mesmo". Cf. Palma, 2009: 1. Disponível em: http://www.idpcc.pt/xms/files/Newsletters/Boletim_Ano1_Ed1_Dez08Jan09.pdf [consultado em 19.01.2017]. Luísa Neto, por seu turno, fala aqui no arguido como o "legislador de si mesmo". Cf. Neto, 2004: 188.

[290] Rodrigues, 2002: 549.

[291] Figueiredo Dias, 1997: 26. Neto, 1997: 184-185.

[292] "Submetido ao processo, às ordens do tribunal e susceptível de sofrer medidas coactivas, ele [o arguido] encontra-se nessa medida certamente numa situação passiva; obrigado a sofrer na sua própria pessoa investigações de prova (os exames) e autor de declarações com valor probatório ele é também meio de prova. Mas nem por isso ele poderá deixar de ser considerado como sujeito do processo". Cf. Castanheira Neves, 1968: 166. Figueiredo Dias segue igualmente este pensamento, defendendo que "Não quer isto dizer que o arguido não possa, em termos demarcados pela lei por forma estrita e expressa, ser objecto de medidas coactivas e constituir, ele próprio, um meio de prova. Quer dizer, sim, que as medidas coactivas e probatórias que sobre ele se exerçam não poderão nunca dirigir-se à extorsão de declarações ou de qualquer forma de autoincriminação […]". Cf. Figueiredo Dias, 2004: 430.

[293] Neste sentido, Roxin afirma que no processo penal alemão se tem debatido sobre o confronto entre a descoberta da verdade e os interesses do arguido: "Em qualquer sistema legal de um Estado de Direito a lei processual penal está obrigada a contrabalançar a investigação criminal e os interesses do arguido, acusado de determinado delito onde a sua privacidade está em causa. O processo penal alemão é um exemplo típico da constante luta entre essas demandas conflituantes. Assim, enquanto a maioria da jurisprudência faz esforços no sentido de reforçar a protecção do arguido, a legislação mais recente revela uma tendência de alcance cada vez maior para a admissão de medidas que interferem com o campo da personalidade". Cf. Roxin, 2009: 87.

[294] Neste sentido, cf. Sousa Mendes, 2007: 609. "[…] o arguido não é um colaborador das autoridades judiciárias e dos OPC para a descoberta da verdade e a realização da justiça!"

[295] Figueiredo Dias, 1997: 27-28.

não tem um "dever de colaboração com o tribunal ou o MP com vista à descoberta da verdade material e à boa decisão da causa (*nemo tenetur se ipsum accusare*), dado o seu direito constitucional ao silêncio (n.º 1 do artigo 32.º da CRP)"[296].

Não obstante a inexistência de um dever de o arguido colaborar com as autoridades, tal não significa que não possa haver derrogações ao princípio *nemo tenetur*, apresentando a doutrina vários exemplos: a) o direito ao silêncio não assiste ao arguido relativamente às perguntas sobre a sua identidade, tendo inclusive o dever de responder a elas com verdade, nos termos da alínea b) do n.º 3 do artigo 61.º do CPP; b) a obrigatoriedade de realizar determinadas perícias e exames (artigos 151.º a 172.º do CPP); c) a obrigatoriedade de sujeição a exames no âmbito de perícias médico-legais quando ordenados pela autoridade judiciária competente, prevista pela Lei n.º 45/2004, de 29 de Agosto[297]; d) a obrigatoriedade de sujeição a diligências de prova, decorrente do consagrado na alínea d) do n.º 3 do artigo 61.º do CPP[298].

No que concerne à jurisprudência, o Tribunal Constitucional já deixou claro que tem sido "reconhecido que o direito à não autoincriminação não tem um carácter absoluto, podendo ser legalmente restringido em determinadas circunstâncias (*v.g.* a obrigatoriedade de realização de determinados exames ou diligências que exijam a colaboração do arguido, mesmo contra a sua vontade)"[299].

Assim, podemos concluir, no seguimento do defendido por Figueiredo Dias, que o arguido pode constituir meio de prova num duplo sentido: a) em sentido material, através das declarações prestadas sobre os factos; b) em sentido formal, na medida em que o seu corpo e o seu estado corporal podem ser objecto de perícias, exames ou outras diligências de prova (artigo 151.º, artigo 172.º e al. d) do n.º 1 do artigo 61.º, todos do CPP) [300].

Chegados a este ponto, e atendendo aos dois métodos de desencriptação do smartphone - a palavra-passe e a impressão digital -, podemos afirmar que a acção de fornecimento da palavra-passe às autoridades judiciárias seria, sem margem para dúvidas, reconduzível à conduta de prestação de declarações sobre os factos (al. d) do n.º 1 do artigo 61.º do CPP). Contrariamente, no que diz respeito à desencriptação do smartphone através da impressão

[296] Albuquerque, 2011: 48 e 183.
[297] Figueiredo Dias/Costa Andrade, 2009: 44-45.
[298] Marques da Silva, 2010: 318.
[299] Cf. Acórdão do Tribunal Constitucional n.º 340/2013, de 17 de Junho de 2013, disponível em: http://www.tribunalconstitucional.pt/tc/acordaos/20130340.html [consultado em 19.01.2017].
[300] Figueiredo Dias, 2004: 438-439.

digital, não podemos defender que esta acção poderá ser reconduzida a uma qualquer prestação de declaração. Assim, resta-nos saber: será a desencriptação através da impressão digital uma perícia, um exame, uma outra diligência de prova, ou nenhuma das anteriores?

Para que possamos responder com clareza a esta questão, iremos, no próximo ponto, fazer uma breve análise ao regime das perícias e exames (artigos 151.º a 172.º do CPP) e às diligências de prova (al. d) do n.º 3 do artigo 61.º do CPP).

3. A sujeição a perícias, exames e diligências de prova e a sua articulação com o princípio *nemo tenetur se ipsum accusare*

Como já tivemos oportunidade de enfatizar anteriormente, o facto de o arguido ser considerado um sujeito do processo penal, não significa que não possa, em determinados termos demarcados pela lei por forma estrita e expressa, constituir ele próprio um meio de prova. Desta forma, sobre o arguido recai o dever de se sujeitar a diligências de prova especificadas na lei e ordenadas e efectuadas por entidade competente (al. d) do n.º 3 do artigo 61.º do CPP), considerando-se como tais as diligências de prova que não forem proibidas por lei e que sejam necessárias para a descoberta da verdade e a realização da justiça[301].

Não obstante este dever de sujeição que recai sobre o arguido, o mesmo não significa que o arguido não se possa opor à realização dessas diligências quando forem manifestamente ilegais, *v.g.*, por atentatórias de direitos fundamentais, e de nessa medida recorrer aos meios que a lei lhe confere, nomeadamente o de recurso judicial. O que a alínea d) do n.º 3 do artigo 61.º do Código de Processo Penal prevê é que, pressupondo que o meio de prova seja legal, o arguido deve sujeitar-se à diligência[302]. Assim, a obrigação que impende sobre o arguido de se sujeitar a diligências de prova tem de ser temperada com o direito fundamental da não-autoincriminação, porque ele não pode ser objecto de prova, instrumento abusivo da sua própria condenação ou de qualquer forma obrigado a contribuir para estabelecer a sua própria culpabilidade[303].

A sujeição coerciva do arguido a diligências de prova tem carácter excepcional, na estrita medida em que se mostrem ineficazes outros meios de prova, devendo observar-se quanto

[301] Garrett, 2007: 15.
[302] Monte, 2006: 254-255.
[303] Garrett, 2007: 17.

à sua utilização os mesmos princípios que regem a aplicação da medida de coacção da prisão preventiva[304].

Algumas diligências de prova a que o arguido pode ser sujeito estão expressamente previstas no Código de Processo Penal, nomeadamente, a perícia (artigo 151.º e seguintes do CPP) e o exame (artigo 171.º e seguintes do CPP).

O Código de Processo Penal enquadrou a perícia no âmbito dos meios de prova, referindo no seu artigo 151.º que "a prova pericial tem lugar quando a percepção ou apreciação dos factos exigirem especiais conhecimentos técnicos, científicos ou artísticos". A perícia surge, assim, como um meio de prova auxiliar, facultando à entidade responsável pela decisão a proferir, elementos de que esta careça e que sejam necessários à percepção ou apreciação dos factos[305].

No que à doutrina diz respeito, no entender de Germano Marques da Silva, "a qualificação que melhor cabe à perícia é efectivamente a de meio de prova pessoal", sendo o seu objecto "a percepção dos factos ou a sua valoração", uma vez que "o perito pode descobrir meios de prova, recorrendo a métodos científicos únicos a permitirem a sua apreensão ou pode exigir-se ao perito não a descoberta dos factos probatórios, mas apenas a sua apreciação"[306]. Na mesma esteira, Manuel Andrade defende a ideia de que a perícia "traduz-se na percepção, por meio de pessoas idóneas para tal efeito designadas, de quaisquer factos presentes, quando não possa ser directa e exclusivamente realizada pelo juiz, por necessitar de conhecimentos científicos ou técnicos especiais, ou por motivos de decoro ou de respeito pela sensibilidade (legítima susceptibilidade) das pessoas em quem se verificam tais factos; ou na apreciação de quaisquer factos (na determinação das ilações que deles se possam tirar acerca doutros factos), caso dependa de conhecimentos daquela ordem, isto é, de regras de experiência que não fazem parte da cultura geral ou experiência comum que pode e deve presumir-se no juiz, como na generalidade das pessoas instruídas e experimentadas"[307].

[304] Monte, 2006: 252. Garrett, 2007: 16.
[305] Cf. Parecer do Conselho Consultivo da Procuradoria Geral da República, P000642006, de 2 de Novembro de 2006, disponível em: http://www.ministeriopublico.pt/iframe/pareceres-do-conselho-consultivo-da-pgr [consultado em 23.01.2017].
[306] Marques da Silva, 2011: 197-198.
[307] Andrade, 1979: 261.

Em sentido inverso, o exame é um meio de obtenção de prova (e não um meio de prova, como a perícia) destinado a recolher vestígios materiais de factos com relevância penal, em ordem à determinação das circunstâncias da prática e da respectiva autoria[308].

No mesmo sentido vai a lei quando aponta que os exames têm por finalidade inspeccionar "os vestígios que possa ter deixado o crime, e todos os indícios relativos ao modo e ao lugar onde foi praticado, às pessoas que o cometeram ou sobre as quais foi cometido" (n.º 1 do artigo 171.º do CPP)[309].

O exame visa a detecção de vestígios, a perícia visa a avaliação desses mesmos vestígios (*v.g.* dactiloscopia[310]).

Um ponto fundamental a ter em consideração em matéria de sujeição a exames tem que ver com a sua obrigatoriedade (n.º 1 do artigo 172.º do CPP). Este princípio expressa-se na possibilidade de a autoridade judiciária competente compelir o arguido à observância de tais obrigações, ainda que condicionadas (no caso de exame susceptível de ofender o pudor das pessoas) ao respeito pela intimidade e dignidade da pessoa a examinar, não se permitindo assistentes, além da própria autoridade judiciária ou de pessoa de confiança do visado que este venha a indicar (n.º 3 do artigo 172.º do CPP).

Contrariamente às perícias, os exames não supõem a existência de especiais conhecimentos técnicos, científicos ou artísticos. No entanto, a mera detecção (e não avaliação) de vestígios que exija especiais conhecimentos técnicos, científicos ou artísticos é ainda um exame. Assim também, a avaliação de vestígios que não exija especiais conhecimentos técnicos, científicos ou artísticos, isto é, que apenas exija conhecimentos comuns, não é uma perícia, mas um exame[311].

Figueiredo Dias fala aqui de uma dupla natureza dos exames, visto que são "[…] por um lado, meios de prova, enquanto neles se faça avultar o juízo que se emite sobre as qualidades ou características de uma pessoa, *i.e.*, enquanto neles se tenha primacialmente em vista a sua mais ou menos acentuada natureza de inspecção ou perícia; na medida,

---

[308] Simas Santos/Leal-Henriques/Simas Santos, 2010: 226-227.
[309] Cf. Acórdão do Tribunal da Relação de Lisboa, de 3 de Março de 2016, disponível em: http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/36f34b50b321b89980257f6f004d5fc6?OpenDocument [consultado em 23.01.2017].
[310] A dactiloscopia assenta na comparação das marcas digitais colhidas directamente dos objectos por técnicas cada vez mais apuradas, com as impressões digitais constantes dos ficheiros policiais, para o estabelecimento da coincidência (*match*) das respectivas formas, as quais são absolutamente originais em cada ser humano. Cf. Oliveira, 2008: 134-135.
[311] Albuquerque, 2011: 434.

porém, em que o objecto do exame seja uma pessoa, que assim se vê constrangida a sofrer ou a suportar uma actividade de investigação sobre si mesma, o exame constitui um verdadeiro meio de coacção processual"[312].

Depois de analisadas as figuras da diligência de prova, perícia e exame, podemos concluir que a recolha de impressões digitais[313] é um exame[314]. Isto porque a sua detecção e avaliação não supõe a existência de especiais conhecimentos técnicos, científicos ou artísticos, sendo apenas exigíveis conhecimentos comuns ao nível da anatomia humana.

Não obstante o que foi dito até agora sobre diligências de prova, perícias e exames e, nomeadamente, sobre o facto de a recolha de impressões digitais ser um exame, surge-nos a questão: em caso de necessidade de desencriptação por impressão digital de um smartphone (no caso concreto da marca Apple), seria esta recolha de impressões digitais (exame) suficiente para o seu desbloqueio?

A esta pergunta teremos de responder negativamente. Tal como deixamos claro no Capítulo III do presente estudo, e atendendo ao caso concreto do iPhone, a tecnologia usada no fabrico do Touch ID é uma das formas mais avançadas de *hardware* e *software* alguma vez implementada num smartphone. O sensor consegue captar uma imagem de alta resolução das camadas subepidérmicas da pele localizadas em pequenas secções da impressão digital, impossibilitando assim que uma réplica da impressão digital do arguido seja eficaz para a sua desencriptação.

Desta forma, a única maneira eficiente de desencriptar o smartphone seria através da coacção do arguido no sentido de colocar o seu dedo no sensor. Mas, neste caso, estaremos perante uma perícia ou um exame?

Ora, o acto (compelido) de colocar o dedo no sensor de um smartphone não pode ser considerado, pelo que analisámos anteriormente, nem uma perícia, nem um exame, nem uma declaração verbal (*v.g.* fornecimento da palavra-passe), mas sim uma outra diligência

[312] Figueiredo Dias, 2004: 438-439.
[313] As impressões digitais são consideradas como um vestígio morfológico. Neste sentido, cf. Ferreira, 2014: 81. "Os vestígios que podem ser detectados ou até mesmo avaliados em sede de exame podem ser classificados como físicos ou materiais (materialmente individualizáveis) ou psíquicos ou imateriais (condutas comportamentais, psíquicas ou de personalidade). Os vestígios físicos podem ser divididos em: orgânicos ou biológicos (saliva, sémen, sangue, urina, secreções, unhas, plantas, insectos, estupefacientes, entre outros); não orgânicos ou não biológicos (instrumentos, fragmentos, solos, tintas, vidros, gases, explosivos, venenos, papel, documentos, entre outros); morfológicos (impressões digitais, palmares e plantares, pegadas, rastos, marcas de objectos, vestígios balísticos, entre outros)".
[314] Albuquerque, 2011: 435.

de prova (al. d) do n.º 3 do artigo 61.º do CPP)[315], relativamente à qual não cabe invocar o direito ao silêncio (al. d) do n.º 1 do artigo 61.º do CPP).

Chegados a este ponto, resta-nos concluir que, ao passo que o fornecimento da palavra-passe para a desencriptação de smartphone se reconduz a um acto comunicativo ou declarativo (al. d) do n.º 1 do artigo 61.º do CPP), a desencriptação do smartphone através da colocação do dedo no sensor para a leitura da impressão digital será uma diligência de prova (al. d) do n.º 3 do artigo 61.º do CPP). E, como já deixamos claro nas páginas anteriores, a área de abrangência do princípio *nemo tenetur se ipsum accusare* não se restringe às declarações orais – nomeadamente ao fornecimento de palavra-passe - proferidas pelo arguido.

No entanto, conforme assinala Costa Andrade, importa reconhecer que existe uma "zona de fronteira e concorrência entre o estatuto do arguido como sujeito processual e o seu estatuto como objecto de medidas de coacção ou meios de prova. Nesta zona cinzenta deparam-se, não raramente, situações em que não é fácil decidir: quando se está ainda no âmbito […]" de uma diligência de prova admissível mesmo se coactivamente imposta; "[…] ou quando, inversamente, se invade já o campo da inadmissível autoincriminação coerciva"[316]. Assim, a legitimidade destas diligências depende da questão de saber se a sua realização ainda é compatível com o estatuto de sujeito processual do arguido ou se traduz antes uma degradação deste à condição de objecto do processo[317].

É ainda de ressalvar que, atendendo ao facto de que o próprio direito ao silêncio, conferido ao arguido em sede de processo criminal, não é absoluto, ou seja, pode ser limitado, podemos afirmar também que o próprio fornecimento de palavra-passe (declaração) para a desencriptação de smartphone pode gerar algumas dúvidas, nomeadamente quanto à questão de saber até que ponto está ou não violado o princípio contra a autoincriminação nesta situação.

Por conseguinte, coloca-se a pergunta: de que critério ou critérios deve, então, o intérprete socorrer-se para aquilatar se a revelação da palavra-passe ou a desencriptação por leitura

[315] Em sentido semelhante, mas relativamente à recolha de autógrafos, Cruz Bucho afirma que "[…] num caso de recolha de autógrafos não estamos perante declarações verbais do arguido, mas sim perante uma diligência de prova relativamente à qual não cabe invocar o direito ao silêncio". Cf. Cruz Bucho, 2013: 34.
[316] Costa Andrade, 1992: 127.
[317] Silva Dias/Ramos, 2009: 21-22.

da impressão digital do arguido se encontram ou não abrangidos pelo princípio *nemo tenetur se ipsum accusare*?

Para respondermos a esta questão, analisaremos no próximo ponto os critérios apresentados pela doutrina e jurisprudência nacionais e internacionais.

4. Critérios para a determinação de violação do princípio *nemo tenetur se ipsum accusare*

A delimitação da área de tutela do *nemo tenetur se ipsum accusare* é, como se intui, tarefa revestida da maior dificuldade e, simultaneamente, do mais significativo relevo. Para o efeito, impõe-se a definição de um critério apto a discernir, nas zonas críticas de fronteira, entre a colaboração coercivamente imposta proibida e a colaboração coercivamente imposta permitida[318].

Tanto a doutrina quanto a jurisprudência, nacionais e internacionais, têm admitido diferentes critérios para a determinação da violação do princípio *nemo tenetur se ipsum accusare*. Analisaremos de seguida os três critérios defendidos.

4.1. Critério da dependência e independência da vontade do arguido

Segundo o critério da dependência e independência da vontade do arguido, estariam fora do princípio *nemo tenetur se ipsum accusare* prestações pessoais exigidas sobre ameaça de sanção, mas independentes da vontade do sujeito, que não passam por uma colaboração espiritual da sua parte[319].

Este critério foi defendido inúmeras vezes pelo Tribunal Europeu dos Direitos Humanos (TEDH), sendo que o caso emblemático que lhe deu origem foi o caso Saunders v. Reino Unido[320]. Ernest Saunders, administrador executivo da sociedade *Guinness PLC*, foi condenado, no sistema judicial britânico, a cinco anos de prisão por conspiração no crime de falsificação de balanço (*false accounting*) e noutros crimes patrimoniais comuns (*thefts*), todos relacionados com uma oferta pública de aquisição sobre a *Distillers Company PLC*, em competição com a *Argyll Group PLC*. O Tribunal Europeu dos Direitos Humanos teve de decidir sobre a queixa de Saunders, fundada no facto de terem

[318] Oliveira Silva, 2013: 375-376.
[319] Cruz Bucho, 2013: 35.
[320] Acórdão Saunders v. Reino Unido, de 17 de Dezembro de 1996, disponível em: http://hudoc.echr.coe.int/webservices/content/pdf/001-58009?TID=thkbhnilzk [consultado em 25.01.2017].

sido usadas como prova num processo-crime subsequente as declarações que ele prestara sob coerção (*i.e.*, sob cominação de desobediência), em procedimento de investigação administrativo, aos inspectores do Ministério do Comércio e Indústria britânico, o que violaria o seu direito à não-autoincriminação, implicitamente consagrado nos n.os 1 e 2 do artigo 6.º da CEDH[321].

O TEDH começou por enunciar os corolários do processo equitativo (artigo 6.º da CEDH) – o direito ao silêncio e a prerrogativa contra a autoincriminação – prosseguindo na sua argumentação[322] afirmando que "[…] o direito de não contribuir para a sua própria incriminação, em especial, pressupõe que, em matéria penal, a acusação deve procurar provar a sua argumentação sem recorrer a elementos de prova obtidos mediante medidas coercivas ou opressivas, desrespeitando a vontade do arguido. Neste sentido, este direito está intimamente ligado ao princípio da presunção da inocência consagrado no parágrafo 2.º do artigo 6.º da Convenção"[323]. O douto Tribunal acrescenta ainda – numa fórmula que se tornou clássica, pois perde-se a conta às vezes em que já tem sido citada – que, tal como é comummente entendido na generalidade dos sistemas jurídicos das Partes contratantes da Convenção, o direito à não-autoincriminação não abrange a utilização, em quaisquer processos penais, de elementos susceptíveis de serem obtidos do acusado através do exercício de poderes compulsivos, contando que a respectiva existência seja "independente da vontade do suspeito"[324], tais como documentos apreendidos em buscas,

---

[321] Sousa Mendes, 2017: 212.

[322] Ramos, 2007: 94.

[323] "*The Court recalls that, although not specifically mentioned in Article 6 of the Convention (art. 6), the right to silence and the right not to incriminate oneself are generally recognised international standards which lie at the heart of the notion of a fair procedure under Article 6 (art. 6). Their rationale lies, inter alia, in the protection of the accused against improper compulsion by the authorities thereby contributing to the avoidance of miscarriages of justice and to the fulfilment of the aims of Article 6 (art. 6) (see the above-mentioned John Murray judgment, p. 49, para. 45, and the above-mentioned Funke judgment, p. 22, para. 44). The right not to incriminate oneself, in particular, presupposes that the prosecution in a criminal case seek to prove their case against the accused without resort to evidence obtained through methods of coercion or oppression in defiance of the will of the accused. In this sense the right is closely linked to the presumption of innocence contained in Article 6 para. 2 of the Convention (art. 6-2)*". Cf. parágrafo 68 do Acórdão Saunders v. Reino Unido, de 17 de Dezembro de 1996, disponível em: http://hudoc.echr.coe.int/webservices/content/pdf/001-58009?TID=thkbhnilzk [consultado em 25.01.2017].

[324] "*The right not to incriminate oneself is primarily concerned, however, with respecting the will of an accused person to remain silent. As commonly understood in the legal systems of the Contracting Parties to the Convention and elsewhere, it does not extend to the use in criminal proceedings of material which may be obtained from the accused through the use of compulsory powers but which has an existence independent of the will of the suspect such as, inter alia, documents acquired pursuant to a warrant, breath, blood and urine samples and bodily tissue for the purpose of DNA testing*". Cf. parágrafo 69 do Acórdão Saunders v. Reino Unido, de 17 de Dezembro de 1996, disponível em: http://hudoc.echr.coe.int/webservices/content/pdf/001-58009?TID=thkbhnilzk [consultado em 25.01.2017].

amostras de sangue ou de urina, e tecidos corporais para testes de ADN[325]. É evidente, portanto, que os reconhecimentos ou intervenções sobre o corpo humano com fins de investigação penal, não estão protegidos pelo direito ao silêncio, à não-autoincriminação ou a não se confessar culpado[326].

O Tribunal decidiu, por conseguinte, que o princípio do processo equitativo, tal como previsto no n.º 1 do artigo 6.º da CEDH, tinha sido violado. À conta do *obter dictum* sobre as provas existentes independentemente da vontade do acusado[327], o presente acórdão tornar-se-ia o caso de referência para a defesa do critério da dependência e independência da vontade do arguido.

Este critério voltou a ser utilizado nos casos Quinn v. Irlanda[328], P.G. et J.H. v. Reino Unido[329], Shannon v. Reino Unido[330] e reafirmado no importante caso Jalloh v. Alemanha[331]. Neste último caso, o TEDH procedeu à delimitação do campo de aplicação do princípio da não-autoincriminação consagrado no artigo 6.º da Convenção, considerando que o mesmo, apesar de se relacionar em primeira linha com o respeito pela vontade do acusado em permanecer em silêncio em face de perguntas que lhe são colocadas e de não ser compelido a prestar declarações, abrange ainda outros casos em que a coacção tenha sido exercida pelas autoridades sobre o acusado para obter prova[332]. Os casos ainda abrangidos pelo âmbito de incidência do princípio da não-autoincriminação correspondem, segundo o TEDH, às hipóteses de intimação para entrega, através de prendimentos coercivos, de prova documental potencialmente autoincriminatória, não se estendendo já ao material susceptível de ser obtido do acusado através do exercício de poderes compulsivos mas cuja existência é independente da

[325] Costa, 2011: 156.
[326] Rodrigues, 2008: 197-198.
[327] Sousa Mendes, 2017: 214.
[328] Acórdão Quinn v. Irlanda, de 21 de Dezembro de 2000, disponível em: http://hudoc.echr.coe.int/eng#{"itemid":["001-59098"]} [consultado em 25.01.2017].
[329] Acórdão P.G. e J.H. v. Reino Unido, de 25 de Setembro de 2001, disponível em: http://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=002-5500&filename=002-5500.pdf&TID=ihgdqbxnfi [consultado em 25.01.2017].
[330] Acórdão Shannon v. Reino Unido, de 4 de Outubro de 2005, disponível em: http://hudoc.echr.coe.int/webservices/content/pdf/001-70364?TID=ihgdqbxnfi [consultado em 25.01.2017].
[331] Acórdão Jalloh v. Alemanha, de 11 de Julho de 2006, disponível em: https://wcd.coe.int/ViewDoc.jsp?p=&id=1018815&Site=COE&direct=true [consultado em 25.01.2017].
[332] Costa, 2011: 156. Ashworth, 2008: 773.

vontade do suspeito, tal como documentos apreendidos em buscas, amostras de sangue ou urina e tecidos corporais para testes de ADN[333].

No que concerne à jurisprudência nacional, também o Tribunal Constitucional perfilhou, em tempos, este entendimento, ao sublinhar, no seu Acórdão n.º 155/2007, que entende "[…] que o direito à não-autoincriminação se refere ao respeito pela vontade do arguido em não prestar declarações, não abrangendo […] o uso, em processo penal, de elementos que se tenham obtido do arguido por meio de poderes coercivos, mas que existam independentemente da vontade do sujeito, como é o caso, por exemplo e para o que agora nos importa considerar, da colheita de saliva para efeitos de realização de análises de ADN"[334]. O Tribunal da Relação de Évora acrescenta ainda que: "Na essência, o privilégio contra a autoincriminação está associado a um depoimento e não a uma prova de natureza física, mas abrange a obrigatoriedade de apresentação de documentação incriminadora"[335].

É também este o critério adoptado maioritariamente pela doutrina e jurisprudência norte-americanas, como já tivemos oportunidade de mencionar no Capítulo I da presente investigação. No entanto, a adopção deste critério em território norte-americano faz-se em termos ligeiramente diferentes aos defendidos pelo Tribunal Europeu dos Direitos Humanos.

A construção largamente dominante no contexto jurídico norte-americano assenta, como vimos anteriormente, na dicotomia entre os elementos probatórios de tipo declarativo (*testimonial*) ou comunicativo (*communicative*) e os elementos probatórios físicos, circunscrevendo-se às provas da primeira espécie a operatividade do privilégio contra a autoincriminação[336].

---

[333] Criticando a distinção entre declarações orais e os elementos de prova enunciados com base no critério da sua existência independente da vontade do arguido, cf. Silva Dias/Ramos, 2009: 24.

[334] Acórdão do Tribunal Constitucional n.º 155/2007, de 2 de Março de 2007, disponível em: http://www.tribunalconstitucional.pt/tc/acordaos/20070155.html [consultado em 25.01.2017]. Neste sentido vão também o Acórdão do Tribunal da Relação de Évora, de 15 de Novembro de 2011, disponível em: http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/3475e69cdc8de87380257de10056f84a?OpenDocument [consultado 25.01.2017] e o Acórdão do Tribunal da Relação de Évora, de 21 de Abril de 2015, disponível em: http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/21398dcfc4605f1980257e43003306a9?OpenDocument [consultado em 25.01.2017].

[335] Acórdão do Tribunal da Relação de Évora, de 11 de Outubro de 2011, disponível em: http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/3693bad042ba17bb80257de10056f62e?OpenDocument [consultado em 25.01.2017].

[336] Oliveira Silva, 2013: 376.

Apesar da *ratio* do critério ser a mesma, o sistema jurídico norte-americano não faz menção aos elementos probatórios "dependentes da vontade do arguido", fazendo, ao invés, referência aos elementos probatórios que pressuponham o recurso ao "conteúdo da mente do arguido"[337].

Em última análise, podemos concluir que são meramente duas expressões distintas - mas integralmente interligadas - que culminam no mesmo entendimento: nenhuma prova incriminatória que dependa, de alguma maneira, inteiramente do arguido (da sua mente/vontade) pode ser compelida. Quanto à interligação ou, se preferirmos, à subordinação entre as duas expressões, – dependência da vontade do arguido e revelação do conteúdo da sua mente – fica claro que é necessário que se faça uso da vontade para que alguém possa revelar, ainda que coercivamente, qualquer conteúdo da sua mente.

Assim, segundo este critério, a recolha coerciva de um elemento probatório inteiramente dependente, de alguma maneira, do arguido (da sua mente/vontade), será violadora do princípio contra a autoincriminação. Por outro lado, se essa recolha de prova não estiver dependente, de alguma maneira, do arguido (da sua mente/vontade), podemos concluir pela não violação do princípio *nemo tenetur*.

Chegados a este ponto, resta-nos então apurar se a revelação coagida da palavra-passe ou a desencriptação do smartphone através da leitura da impressão digital do arguido são ou não condutas violadoras do princípio *nemo tenetur* com base neste critério da dependência e independência da vontade do arguido.

No que concerne ao fornecimento coagido de palavra-passe para desencriptação de um smartphone, a doutrina norte-americana tende a fazer uma analogia entre a palavra-passe e uma combinação de um cofre[338], defendendo que o fornecimento da palavra-passe será um elemento probatório declarativo (*testimonial*)[339].

---

[337] Mesquita, 2011: 560.

[338] "*A passphrase is more analogous to a combination to a safe in the sense that both exist only in the mind of the individual*". Cf. Duong, 2009: 349-350.

[339] "*A combination metaphor to a safe more accurately captures a password's testimonial nature, because a combination is something that is in one's mind"*. Cf. Kiok, 2015: 77. Neste sentido vão também Wiseman, 2014: 29. Disponível em: https://works.bepress.com/timothy_wiseman/2/ [consultado em 26.01.2017]. Thompson II/Jaikaran, 2016: 12. Engel, 2012: 107-108. Mohan/Villasenor, 2012: 24-25. Porém, existe alguma doutrina, ainda que claramente minoritária, que defende a ideia de que, mesmo contra a vontade do arguido, a própria revelação pode ser legalmente compelida. Cf. Terzian, 2014: 305. Na esteira do defendido pela maioria da doutrina norte-americana, também a jurisprudência parece ir no mesmo sentido: "*forcing the Defendant to reveal the password… requires Defendant to communicate 'knowlegde'*". Cf. United States v. Kirschner, 2010. Disponível em: https://www.ravellaw.com/opinions/789d10be33066b73e4377a26bf5c574a [consultado em 26.01.2017];

O arguido, ao fornecer, sob coacção, a palavra-passe que desencripta o seu smartphone, seja pela via oral, escrita ou gestual, estará, necessariamente, a fazer uso da sua vontade. Ou seja, para o fornecimento da palavra-passe o arguido tem de revelar o conteúdo da sua mente, e essa revelação está, como já adiantámos anteriormente, totalmente condicionada pela sua vontade em auxiliar ou não a investigação[340].

Assim, não podemos caracterizar esta conduta de revelação da palavra-passe, seja de que modo for, como um qualquer acto físico independente da vontade do arguido[341]. Isto porque, seria impossível para as autoridades judiciárias forçarem o arguido a divulgar algo sobre o qual tenha conhecimento[342].

Já no que diz respeito à desencriptação do smartphone através da colocação do dedo do arguido no sensor para a leitura da sua impressão digital o resultado é díspar. Se, por um lado, podíamos fazer uma analogia entre a divulgação da palavra-passe e a divulgação de uma combinação de um cofre, por outro, podemos aqui falar, segundo o entendimento da doutrina norte-americana, numa analogia entre a desencriptação de um smartphone através da leitura da impressão digital do arguido e a entrega de uma chave de um cofre[343].

Contrariamente ao fornecimento de palavra-passe, a desencriptação do smartphone através da leitura da impressão digital do arguido configura um acto inteiramente físico, que compara apenas a impressão digital lida com a impressão digital armazenada no dispositivo[344]. O acto de colocar o dedo no sensor do smartphone para possibilitar a sua desencriptação não exige qualquer tipo de divulgação do conteúdo da mente do arguido[345]. E, uma vez que as entidades judiciárias podem simplesmente agarrar no dedo

---

"*[…] the production was testimonial because the decryption password require the appellant to use 'the contents of the mind' to produce information that could be incriminating*". Cf. Fisher v. United States, 1976. Disponível em: https://supreme.justia.com/cases/federal/us/425/391/case.html [consultado em 26.01.2017].

[340] Wiseman, 2015: 548-549.

[341] Bales, 2012: 1302-1303.

[342] Hustle, 2014: 2. Disponível em: http://rebelpundit.com/biometrics-and-the-constitution-why-fingerprints-are-less-secure-than-passwords/ [consultado em 26.01.2017]. "*[…] using a decryption password requires sufficiently great mental use […]*." Cf. Terzian, 2015: 1136.

[343] Thompson II/Jaikaran, 2016: 14.

[344] Sales, 2014: 222-223.

[345] Goldman, 2015: 218. Neste sentido vão também Silver, 2012: 814. Wilson, 2015: 28-29. Na esteira do defendido pela doutrina, também a jurisprudência norte-americana vem afirmar que: "*[…] fingerprints are not deemed testimonial and therefore not subject to Fifth Amendment protection. […] a fingerprint can be compelled even though it is being used to open the cell phone. The passcode is more like a combination to a safe and the fingerprint is more like a key*". Cf. Commonwealth of Virginia v. David Charles Baust, 2014. Disponível em: https://consumermediallc.files.wordpress.com/2014/11/245515028-fingerprint-unlock-ruling.pdf [consultado em 26.01.2017]. Pode ser consultado no Anexo I da presente Dissertação. Cf. State of Minnesota v. Matthew Vaughn Diamond, 2017. Disponível em: http://mn.gov/law-library-

do arguido e colocá-lo no sensor, não podemos, semelhantemente, falar numa dependência da sua vontade.

Assim, sendo a desencriptação do smartphone através da leitura da impressão digital do arguido um acto físico independente da sua vontade, podemos admitir que não haverá aqui, segundo este critério, uma violação do princípio *nemo tenetur se ipsum accusare*. Em sentido inverso, o fornecimento da palavra-passe, sendo um acto que depende obrigatoriamente da vontade do arguido, será violador, segundo este critério, do princípio contra a autoincriminação, se for compelido pelas autoridades judiciárias.

Não obstante o que ficou dito sobre o critério da dependência e independência da vontade do arguido, defendido tanto pelo Tribunal Europeu dos Direitos Humanos como pela jurisprudência e doutrina maioritária norte-americanas, várias críticas surgem contra esta tese.

De facto, não partilhamos desta linha argumentativa – frágil no nosso entender -, defendida várias vezes pelo Tribunal Constitucional português, de que "o direito à não-autoincriminação se refere ao respeito pela vontade do arguido em não prestar declarações, não abrangendo […] o uso, em processo penal, de elementos que se tenham obtido do arguido por meio de poderes coercivos, mas que existam independentemente da vontade do sujeito"[346].

Esta concepção altamente restritiva do conceito do *nemo tenetur se ipsum accusare* permite que o arguido seja o objecto de prova em todas as situações nas quais não se exija a prestação de declarações. O princípio ficaria cingido às declarações orais, coincidindo praticamente com o direito ao silêncio[347]. E, limitar o princípio ao direito ao silêncio é desprovê-lo de todo o seu conteúdo e alcance prático[348].

Por outro lado, parece irrefutável que as declarações orais não são o único meio através do qual alguém se pode autoincriminar, já que não se vê como alguém que é alvo de uma qualquer ingerência corporal não estará a contribuir para a sua autoincriminação, sobretudo se a prova, a final, apenas vier a assentar em tal meio de prova que, de outro

stat/archive/ctappub/2017/OPa152075-011717.pdf [consultado em 26.01.2017]. Pode ser consultado no Anexo II da presente Dissertação.

[346] Acórdão do Tribunal Constitucional n.º 155/2007, de 2 de Março de 2007, disponível em: http://www.tribunalconstitucional.pt/tc/acordaos/20070155.html [consultado em 31.01.2017].

[347] Silva Dias/Ramos, 2009: 24.

[348] Cruz, 2011: 71.

modo, não existiria. Do que se trata é de se colocar a "falar o corpo" quando o titular desse corpo pretende calar[349].

Posto isto, analisadas que estão as críticas relativas a este critério, passaremos à apreciação de um segundo critério defendido pela doutrina e jurisprudência nacionais e internacionais.

4.2. Critério da conduta activa e tolerância passiva

O segundo critério, adoptado pelo Tribunal Constitucional alemão e pela generalidade da doutrina alemã, assenta na distinção entre conduta activa e tolerância passiva. De acordo com este critério, ninguém poderá ser coactivamente obrigado a contribuir activamente para a sua própria condenação em processo criminal[350] - seja declarando contra si mesmo, seja realizando algum outro tipo de actividade que contribua para a investigação e comprovação do crime imputado.

No panorama jurídico alemão, a doutrina tradicional e (ainda) dominante aponta como critério delimitador do princípio *nemo tenetur* a "qualidade da conduta" (*"Handlungsqualität"*) esperada do arguido, distinguindo entre os meros deveres de tolerância passiva ("*passive Duldungspflichten*") e as obrigações de colaboração activa (*"aktive Mitwirkungspflichten"*)[351]. A colaboração activa será, segundo esta doutrina tradicional, inexigível ao arguido, existindo um direito de oposição à colaboração activa (*Mitwirkungsverweigerungsrecht*), porquanto esta seria violadora do princípio *nemo tenetur se ipsum accusare*[352].

Nesta esteira de ideias, se ao arguido se impusesse a colaboração mediante uma conduta activa, tal seria susceptível de ferir o princípio contra a autoincriminação; se, ao invés, se lhe impusesse meramente que tolerasse uma determinada actividade, não haveria qualquer colisão com o direito à não-autoincriminação que lhe assiste, não configurando assim uma manifestação inadmissível de autoincriminação[353].

A referida diferenciação fenomenológica assenta na premissa filosófica de que a liberdade de vontade constitui a expressão mais nuclear da personalidade humana, por

[349] Rodrigues, 2008: 198.
[350] Acórdão do Tribunal Constitucional n.º 340/2013, de 17 de Junho de 2013, disponível em: http://www.tribunalconstitucional.pt/tc/acordaos/20130340.html [consultado em 31.01.2017].
[351] Oliveira Silva, 2013: 376-377.
[352] Pinto, 2013: 97.
[353] Agostinho, 2014: 112.

contraposição com a existência física/corpórea. E tem como certa a ideia de que a autonomia pessoal é mais severamente atingida se o arguido for forçado a colaborar com o Estado na própria perseguição criminal sob a forma de uma acção positiva, do que nos casos em que o seu corpo é simplesmente manipulado pelas autoridades, impondo-se-lhe o dever de tolerar a intervenção (mas já não a de coadjuvar)[354].

Claus Roxin, defensor desta teoria, adianta que o arguido não tem o dever de auxiliar as autoridades judiciárias de forma activa, no entanto, deve tolerar não apenas as investigações relativas à sua vida privada, mas também as intervenções físicas sobre o seu corpo, que podem facilmente consubstanciar uma contribuição decisiva para a prova da sua culpabilidade[355].

É de notar que o Tribunal da Relação do Porto, num acórdão relativamente recente, parece acolher esta distinção[356]. Neste caso jurisprudencial estaria em causa a legitimidade da recusa do arguido em se sujeitar à recolha de autógrafos, e a legitimidade da cominação dessa recusa com o crime de desobediência. No acórdão recorrido, o Tribunal de 1.ª instância afasta categoricamente toda a colaboração qualificada como activa. O acórdão do Tribunal da Relação do Porto acaba por confirmar o acórdão recorrido, mas é mais comedido do que o Tribunal de 1.ª instância, temperando o argumento da colaboração activa com o princípio da legalidade[357].

Fazendo apelo a este segundo critério, importa agora perceber se o fornecimento da palavra-passe e a desencriptação através da impressão digital seriam ou não condutas violadoras do princípio contra a autoincriminação.

As coisas são particularmente óbvias quando se trata de obter, por coacção, declarações incriminadoras do arguido[358]. Assim, segundo o critério da conduta activa e tolerância passiva, o arguido não poderá ser compelido a revelar a palavra-passe que desencripta o seu smartphone, essencial para os investigadores criminais terem rápido acesso à

[354] Oliveira Silva, 2015: 575-576.
[355] Cf. Roxin, 2009: 98.
[356] "Mesmo que o recorrente não concorde, não podemos esquecer que aqui, a recolha de autógrafos implica uma acção positiva do arguido (contra a sua vontade), que não se confunde com "o mero tolerar passivo da actividade de terceiro", *v.g.* que decorre da execução de decisão de juiz a "compelir" à sujeição a exame, tal como hoje se prevê expressamente nos n.os 1 e 2 do artigo 172.º do CPP (estabelecendo-se ainda que é correspondentemente aplicável o disposto no nº 2 do artigo 154.º e nos nos 5 e 6 do artigo 156.º do mesmo código)". Cf. Acórdão da Relação do Porto, de 28 de Janeiro de 2009, disponível em: http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/f861aadc84da529a8025754e0054040e?OpenDocument [consultado em 31.01.2017].
[357] Pinto, 2013: 97-98.
[358] Costa Andrade, 1992: 128.

informação nele contida, por ser ilegitimamente obrigado a colaborar ou a contribuir activamente para a sua incriminação[359].

Quanto à desencriptação do smartphone através da leitura da impressão digital do arguido, a situação é mais dúbia. Isto porque, como frisámos anteriormente, o arguido pode, por sua livre vontade, colocar o dedo no sensor para permitir a leitura da sua impressão digital, possibilitando assim a desencriptação do dispositivo. No entanto, o mesmo arguido pode optar por se opor a colocar o dedo no sensor, restando às autoridades a alternativa de forçarem a desencriptação do smartphone através da colocação coactiva do seu dedo no sensor. E, se por um lado podemos classificar a primeira conduta como uma conduta activa, por outro, podemos qualificar a segunda como uma conduta passiva.

A desencriptação do smartphone através da leitura da impressão digital do arguido é um exemplo típico de uma das críticas feitas a este critério da conduta activa e tolerância passiva, um critério que está longe de concitar um aplauso pacífico entre Autores e tribunais. É certo que "fazer" é diferente de "deixar fazer", que o direito (nomeadamente o direito penal) valora de modo diferente condutas activas e condutas omissivas. No entanto, este critério de averiguação da conformidade com o princípio *nemo tenetur* manifesta-se insatisfatório[360].

Na verdade, este segundo critério tem sido qualificado como simplista e de difícil aplicação prática[361] pela dificuldade em diferenciar, sob o prisma fenomenológico, entre actos de colaboração activa e meros estados passivos de tolerância[362].

Acompanhamos Wolfslast quando afirma que "não se é apenas instrumento da própria condenação quando se colabora mediante uma conduta activa, querida e livre, mas também quando […] contra vontade, uma pessoa tem de tolerar que o próprio corpo seja utilizado como meio de prova"[363]. De resto, acrescenta, será difícil discernir porque é que a dignidade humana do arguido só é atingida quando forçado a uma acção e não já quando compelido a ter de tolerar uma acção. O tormento, a humilhação de ter de ser instrumento contra si próprio podem, em caso de passividade forçada e verificadas certas circunstâncias, ser maiores do que em caso de colaboração activa[364].

[359] Haddad, 2003: 42-43.
[360] Fidalgo, 2006: 141.
[361] Cruz Bucho, 2013: 46. Pinto, 2013: 98.
[362] Oliveira Silva, 2015: 580.
[363] Wolfslast, 1987: 103.
[364] Wolfslast, 1987: 104.

Como bem refere Sandra Oliveira e Silva, "a distinção conceitual-positivista entre acção e omissão é inadequada para estabelecer valorações jurídicas distintas. Em causa estão conceitos intercambiáveis de acordo com a conclusão pretendida pelo intérprete. E ainda que se pudesse obter um consenso sobre o sentido a adoptar em cada caso, não deixa de ser possível interpretar indistintamente determinados comportamentos como acção ou omissão e as correspondentes obrigações como importando uma colaboração activa ou uma simples tolerância passiva"[365].

No que concerne às inconsistências deste critério no plano teórico, importa voltar a mencionar a ideia de que o *nemo tenetur* pretende preservar o arguido do "trilema" da escolha entre três males, poupá-lo à experiência degradante de ser obrigado a colocar nas mãos das autoridades de perseguição criminal o material probatório para a sua incriminação[366]. Acreditamos, na esteira do defendido por Sandra Oliveira e Silva, que é difícil discernir as razões pelas quais o sentimento de humilhação só se manifesta se o arguido for obrigado a entregar o material incriminador pelos seus próprios meios e não também nas hipóteses em que as informações são extraídas à força do seu corpo[367], nomeadamente através da utilização da sua impressão digital para desencriptar um smartphone onde estarão armazenadas informações íntimas e possivelmente incriminatórias. Quer no caso de uma conduta activa, quer no caso de tolerância passiva, o arguido tem plena consciência de ser obrigado a contribuir contra a sua vontade para a obtenção de provas incriminatórias.

Também a jurisprudência nacional se tem pronunciado, ainda que em pouca escala, sobre este critério defendido pela doutrina e jurisprudência alemãs. O Tribunal Constitucional, no seu acórdão n.º 155/2007, refere-se, a propósito da colheita de saliva para efeitos de realização de análises de ADN, que esta, "independentemente de não requerer apenas um comportamento passivo, não se pode catalogar como obrigação de autoincriminação"[368]. Esta expressão parece apontar para a conclusão de que o critério conduta activa/tolerância passiva não tem relevância no sistema jurídico nacional, na medida em que o douto Tribunal aceita a existência de um caso de colaboração activa do arguido, não o afastando imediata e categoricamente depois de o qualificar como tal[369]. Mais recentemente, o

[365] Oliveira Silva, 2015: 583-584.
[366] Costa Andrade, 2014: 143-144.
[367] Oliveira Silva, 2015: 590.
[368] Acórdão do Tribunal Constitucional n.º 155/2007, de 2 de Março de 2007, disponível em: http://www.tribunalconstitucional.pt/tc/acordaos/20070155.html [consultado em 01.02.2017].
[369] Pinto, 2013: 99.

Supremo Tribunal de Justiça, no seu acórdão n.º 14/2014, veio destacar a difícil praticabilidade deste critério "por nem sempre ser viável e nem visível a distinção entre as duas formas procedimentais, por ser demasiado simplista, não conducente a resultados seguros, sequer aceitáveis"[370]. O Supremo Tribunal atesta ainda que "na verdade, parece evidente que mesmo em casos havidos classicamente de tolerância passiva não deixa de coexistir uma participação activa, como é o caso da sujeição a recolha de sangue, saliva, urina, corte de cabelo, de tecidos corporais, álcool no sangue a partir do ar expirado ou do sangue etc., em que sem a colaboração (necessariamente activa) do arguido expondo voluntariamente o seu corpo fica comprometido o resultado a alcançar"[371].

Em conclusão, podemos afirmar que, dadas as dificuldades de aplicação, fragilidades e inconsistências do critério da conduta activa e tolerância passiva, este não poderá ser considerado como um método viável para traçar a linha de fronteira entre a colaboração admissível e a inadmissível. Por esse motivo, estas dificuldades têm conduzido a doutrina e jurisprudência nacionais ao esboço de um terceiro critério de delimitação e ao progressivo abandono do binómio actividade/passividade.

4.3. Critério da ponderação de bens

A doutrina e jurisprudência constitucional portuguesas têm vindo a adoptar o critério da ponderação de bens para delimitar a área de tutela do *nemo tenetur se ipsum accusare*. Sem embargo, antes de procedermos à análise deste critério, impera que se estabeleça *a priori* uma distinção relativa à natureza dos direitos fundamentais ou, mais rigorosamente, à natureza das normas de direitos fundamentais que possam entrar em conflito.

4.3.1. A distinção entre normas-regras e normas-princípios

Grande parte da doutrina, nacional e internacional, defende a distinção nítida entre regras e princípios. Distinção, segundo Alexy, sem a qual não poderia existir uma teoria adequada dos limites dos direitos fundamentais, nem uma teoria satisfatória da colisão entre direitos fundamentais, nem tão pouco uma teoria suficiente acerca do papel desempenhado por estes direitos no sistema jurídico[372]. Esta construção foi globalmente

[370] Acórdão do Supremo Tribunal de Justiça n.º 14/2014, de 21 de Outubro de 2014, disponível em: https://dre.pt/application/file/58512485 [consultado em 01.02.2017].
[371] Acórdão do Supremo Tribunal de Justiça n.º 14/2014, de 21 de Outubro de 2014, disponível em: https://dre.pt/application/file/58512485 [consultado em 01.02.2017].
[372] Alexy, 2008: 63.

desenvolvida, na década de oitenta, por Alexy, inspirado no pensamento de Dworkin e nas suas distinções entre "*rules*" e "*principles*".

Segundo Dworkin, a distinção lógica entre regras e princípios manifesta-se na diferente forma de aplicação e de colisão que, por sua vez, se funda na seguinte diferença essencial: enquanto que a dimensão fundamental das regras é a da validade, a dos princípios é o peso[373]. Assim, um conflito de regras seria decidido através da dimensão determinante da validade, implicando a eliminação na ordem jurídica da regra contrária inválida, ao passo que, uma colisão de princípios, diferentemente, seria decidida em função do peso relativo que cada um deles apresenta no caso concreto (*dimension of weight*), implicando a cedência do princípio mais fraco nesse caso, sem a sua exclusão da ordem jurídica[374].

Para Alexy, as regras são normas que exigem algo de modo definitivo, são comandos definitivos. Se uma regra é válida e estão reunidas as condições para a sua aplicação, então deve ser feito exactamente o que ela exige. Se isso for feito, a regra é cumprida, se isso não for feito, a regra é violada[375]. Pelo contrário, os princípios são mandados de optimização. Como tal, eles exigem que algo seja feito na máxima extensão possível de acordo com as possibilidades de facto e de direito existentes[376].

Neste sentido, a diferença entre regras e princípios permanece, para Alexy, tal como para Dworkin, uma diferença qualitativa e não gradativa, sendo qualquer norma ou uma regra ou um princípio[377].

Já na doutrina nacional, Jorge Reis Novais, afirma que a diferença entre regras e princípios é determinada pelo método de aplicação, que seria a ponderação nos princípios e a subsunção nas regras[378].

De acordo com estas distinções entre normas-regras e normas-princípios, facilmente se depreende que o *nemo tenetur se ipsum accusare* seria qualificado como um princípio e não uma regra. E, apresentando este direito fundamental não escrito a natureza de princípio, o *nemo tenetur*, como temos vindo a reiterar ao longo da nossa investigação,

[373] Dworkin, 1977: 35.
[374] Dworkin, 1977: 22-26.
[375] Alexy, 2014: 818-819.
[376] Alexy, 2014: 819.
[377] Alexy, 2008: 68. Contra esta ideia vai Jorge Reis Novais, ao afirmar que um direito fundamental pode ser simultaneamente uma regra e um princípio, dando como exemplo o direito à vida. "[…] o direito à vida constitucionalmente reconhecido pode ser fundamentalmente considerado como regra, como princípio ou simultaneamente regra e princípio […]". Cf. Reis Novais, 2010: 352.
[378] Reis Novais, 2010: 347-348.

não será absoluto, podendo ser alvo de colisões com outros princípios. Segundo Alexy, quando dois princípios entram em colisão um deles terá obrigatoriamente que ceder perante o outro. No entanto, isto não significa, como se referiu anteriormente, que se tenha de considerar inválido o princípio alvo de cedência[379].

Efectivamente, os defensores dos direitos fundamentais como princípios partem desta distinção entre regras e princípios para afirmarem que a determinação do grau adequado de satisfação ou de realização de um princípio, relativamente aos mandados de outros princípios, é conseguida através da ponderação[380]. Ou seja, apresentando as normas constitucionais de direitos fundamentais a natureza de princípios, isso significa que os direitos nelas sustentados só se convertem em direitos definitivos depois de passarem pelo crivo do critério da ponderação com os princípios opostos nas circunstâncias do caso concreto[381]. O critério da ponderação será assim a forma específica de aplicação aos princípios.

Depois de feita a distinção entre normas-regras e normas-princípios e o seu método de resolução em caso de conflito, passaremos agora à análise do critério da ponderação.

4.3.2. A ponderação enquanto critério de resolução de conflitos entre direitos fundamentais

Sendo o princípio *nemo tenetur* sujeito a restrições, não causa estranheza afirmar que o processo penal é foco permanente de tensões entre o dever de eficácia que é exigido aos responsáveis pela investigação criminal e as garantias de defesa que cabem a todos os arguidos. É, assim, neste âmbito, que assume relevância a ponderação deste amplo direito dos arguidos em não colaborar para a autoincriminação, quando em confronto com outros valores como a eficácia da investigação criminal e a tutela efectiva da justiça[382].

Augusto Silva Dias e Vânia Costa Ramos são dois Autores que perfilham este critério como sendo o correcto para a delimitação entre a coacção permitida e a coacção proibida. Segundo os Autores, "sempre que o suspeito (ou arguido) seja induzido ou coagido, por forma mais ou menos activa ou mais ou menos intelectualmente elaborada, a colaborar

[379] Alexy, 2008: 70.
[380] Alexy, 2014: 819. Contra este entendimento vai Vieira de Andrade, ao defender que "[…] a limitação de direitos fundamentais, associada ao método da ponderação e da harmonização, toma um sentido muito amplo, que tende a consumir na colisão de direitos ou de direitos e valores, além dos casos de harmonização, a declaração de limites imanentes e a restrição legislativa". Cf. Vieira de Andrade, 2016: 266-267.
[381] Reis Novais, 2010: 339.
[382] Neves/Correia, 2014: 146.

na sua inculpação, cai-se na esfera de protecção do *nemo tenetur*"[383]. No entanto, estando-se perante um princípio de natureza não absoluta, existe a necessidade de encontrar um ponto de equilíbrio entre as garantias de defesa do arguido e os interesses da investigação. Com efeito, a descoberta da verdade e a correcta realização da justiça criminal ficariam seriamente comprometidas caso fossem eliminadas todas as possibilidades de utilização de elementos probatórios provenientes da esfera do arguido ou obtidos com a sua colaboração[384]. Para os Autores citados, e para a maioria da doutrina nacional[385], o referido ponto de equilíbrio é dado pela ideia de concordância prática fundada na ponderação de interesses conflituantes[386]. "Porque nenhum princípio pode pretender, na sua globalidade, vigência absoluta", são legítimas as restrições ao *nemo tenetur* impostas pela necessidade de salvaguarda de um interesse ou direito concretamente prevalecente, como será o da máxima eficácia da administração da justiça na perseguição dos crimes mais graves[387].

De facto, ter um direito fundamental significa, na sua dimensão subjectiva, ter uma posição forte de garantia que vincula directamente as entidades públicas, no sentido de que estas não podem dispor ou intervir livremente sobre ela sem que estejam preenchidos requisitos constitucionais escritos[388]. Porém, dada a necessidade de essas posições serem compatibilizadas com outros bens, a ponderação dos bens em conflito parece ser o melhor procedimento, ao invés de um critério *all or nothing*[389].

Neste caso, quando os poderes constituídos procedem à harmonização ou compatibilização de bens, não procedem à mera declaração de limites já existentes, mas determinam, de uma maneira geral constitutivamente, de entre várias hipóteses de solução ao seu dispor, o *se*, o *como* e o *quanto* da eventual cedência (restrição) dos direitos

[383] Silva Dias/Ramos, 2009: 29.
[384] Oliveira Silva, 2015: 617.
[385] "A doutrina portuguesa vem aceitando a concepção de Dworkin e de Alexy segundo a qual o *Dasein* dos princípios é em colisão com outros e o modo de dirimir essa colisão é, não através de um critério *all or nothing*, mas por meio de uma compatibilização ou concordância prática que visa aplicar todos os princípios colidentes, harmonizando-os entre si na situação concreta". Cf. Silva Dias/Ramos, 2009: 23.
[386] Neste sentido Gomes Canotilho e Vital Moreira defendem que "a restrição de direitos fundamentais implica necessariamente uma relação de conciliação com outros direitos ou interesses constitucionais e exige necessariamente uma tarefa de ponderação ou de concordância prática dos direitos ou interesses em conflito". Cf. Canotilho/Moreira, 1991: 134.
[387] Silva Dias/Ramos, 2009: 34. "O grau dessa restrição depende da importância constitucional dos direitos ou interesses públicos colidentes, mas nunca pode ir ao ponto de aniquilar o conteúdo essencial de qualquer deles (v. n.º 3 do artigo 18.º da CRP)". Cf. Silva Dias, 2010: 246.
[388] Reis Novais, 2010: 570.
[389] Silva Dias/Ramos, 2009: 23.

fundamentais[390]. Desta forma, não devemos falar aqui, contrariamente ao defendido pela teoria interna dos limites dos direitos fundamentais, em limites imanentes. Os direitos de terceiros ou outros bens constitucionais que colidam com os direitos fundamentais não são os seus limites, ou seja, não excluem, *a priori*, qualquer exercício de direito fundamental que eventualmente afecte esses bens. O que se passa, como bem defende Jorge Reis Novais, é que, "tendo os direitos fundamentais uma validade condicionada à cedência perante valores que apresentem, no caso concreto, um maior peso, pode acontecer que, por força da sua colisão com esses bens, os interesses […] jusfundamentalmente protegidos tenham que ceder"[391]. Efectivamente, quando um princípio, direito ou garantia, é superior a outro de acordo com critérios de relevância constitucional e não é possível na situação concreta salvaguardar alguns aspectos do princípio inferior, nesse caso, é permitido o sacrifício deste último[392].

Sem embargo, cumpre deixar claro que a colisão dos mesmos bens num outro caso concreto pode ser resolvida num sentido ou numa medida de restrição completamente diferentes, seja pela novidade das circunstâncias envolventes seja pela diversidade das específicas modalidades, áreas ou recortes dos interesses e dos bens em colisão.

No fundo, como já referimos anteriormente, todo o problema dos limites dos direitos fundamentais em Estado de Direito gira em torno de duas exigências de sentido potencialmente divergente: de um lado, as necessidades de protecção privilegiada e qualidade das liberdades individuais e, de outro, a satisfação, por parte do Estado, das necessidades de vida em comunidade politicamente organizada e, em particular, a garantia dos direitos fundamentais dos outros e a realização dos bens constitucionais.

4.3.3. Os limites aos limites dos direitos fundamentais

Atendendo ao facto de que o conflito entre estas duas exigências resolver-se-à, segundo o critério da ponderação, através de uma harmonização ou compatibilização de bens, cumpre agora deixar claro que esta ponderação de bens, na medida em que irá restringir obrigatoriamente um ou ambos os direitos fundamentais, terá de observar, recorrendo à terminologia germânica, os chamados limites aos limites dos direitos fundamentais.

[390] Reis Novais, 2010: 570-571.
[391] Reis Novais, 2010: 572. Neste sentido, Alexy vem defender a ideia de que a solução para a colisão consiste na fixação de uma relação de precedência condicionada entre os princípios em conflito. Por sua vez, a determinação desta relação de precedência condicionada, atendendo ao caso concreto, passa por indicar em que condições um princípio tem prevalência sobre o outro. Cf. Alexy, 2008: 73.
[392] Silva Dias/Ramos, 2009: 23-24.

No caso português, por força da aplicação dos n.os 2 e 3 do artigo 18.º da Constituição da República Portuguesa, toda e qualquer restrição a direitos fundamentais, nomeadamente ao princípio *nemo tenetur se ipsum accusare*, terá de obedecer aos seguintes requisitos: a) deve estar prevista em lei formal (n.º 2, 1.ª parte); b) deve ter como objectivo a salvaguarda de outro direito ou interesse constitucionalmente protegido (n.º 2, *in fine*); c) deve obedecer ao princípio da proporcionalidade em sentido amplo – adequação, necessidade e proporcionalidade em sentido estrito (n.º 2, 2.ª parte)[393]; d) não deve aniquilar o direito em causa atingindo o conteúdo essencial do respectivo preceito (n.º 3, *in fine*)[394].

Além da verificação destes requisitos materiais, a validade das restrições a direitos, liberdades e garantias depende ainda, nos termos do n.º 3 do artigo 18.º da Lei Fundamental, de dois requisitos formais: a) deve ser geral e abstracta (n.º 3, 1.ª parte); b) e, não deve ter efeito retroactivo (n.º 3, 2.ª parte).

Verificados estes requisitos deverá considerar-se jurídico-constitucionalmente admissível a restrição daquelas garantias processuais mesmo em matéria criminal.

Entendimento semelhante é defendido pela jurisprudência nacional[395]. O Tribunal Constitucional, no seu acórdão n.º 155/2007, relativo à recolha de saliva através de zaragatoa bucal, veio atestar que "[…] não proibindo a Constituição, em absoluto, a possibilidade de restrição legal aos direitos, liberdades e garantias, submete-a, contudo, a múltiplos e apertados pressupostos (formais e materiais) de validade. Da vasta jurisprudência constitucional sobre a matéria decorre, em síntese, que qualquer restrição de direitos, liberdades e garantias só é constitucionalmente legítima se (i) for autorizada pela Constituição (artigo 18.º, nº 2, 1ª parte) (ii) estiver suficientemente sustentada em lei da Assembleia da República ou em decreto-lei autorizado (artigo 18.º, nº 2, 1ª parte e

[393] Figueiredo Dias/Costa Andrade, 2009: 45. Neste sentido vai também Vânia Costa Ramos, quando defende a ideia de que "o *nemo tenetur* não é, todavia, um princípio absoluto, subtraído a ponderação. Poderá ser limitado para protecção de outros direitos, liberdades ou garantias da mesma natureza e segundo critérios de adequação e de proporcionalidade, em conformidade com o n.º 2 do artigo 18.º da Constituição da República Portuguesa". Cf. Ramos, 2010: 180.

[394] Gomes Canotilho/Moreira, 2014: 388. Miranda, 2006: 96-97. Moniz, 2009: 149. Gomes Canotilho, 2016: 451.

[395] O próprio Tribunal Europeu dos Direitos Humanos, no caso Jalloh v. Alemanha, parece adoptar um critério de ponderação de bens quando afirma que "Para determinar se o direito à não-autoincriminação do queixoso foi violado, o Tribunal, por sua vez, terá de considerar os seguintes factores: a natureza e o grau de coerção empregado para obter as provas, a importância do interesse público na investigação e punição da infracção em apreço, a existência de garantias relevantes no processo e a utilização prevista dos meios de prova obtidos dessa forma". Cf. Acórdão Jalloh v. Alemanha, de 11 de Julho de 2006, disponível em: https://wcd.coe.int/ViewDoc.jsp?p=&id=1018815&Site=COE&direct=true [consultado em 02.02.2017].

artigo 165.º, nº 1, alínea b), (iii) visar a salvaguarda de outro direito ou interesse constitucionalmente protegido (artigo 18.º, nº 2, *in fine*); (iv) for necessária a essa salvaguarda, adequada para o efeito e proporcional a esse objectivo (artigo 18.º, nº 2, 2ª parte); (v) tiver carácter geral e abstracto, não tiver efeito retroactivo e não diminuir a extensão e o alcance do conteúdo essencial dos preceitos constitucionais (artigo 18.º, nº 3, da Constituição)"[396].

Por sua vez, o Tribunal da Relação do Porto, também em sede de apreciação da legitimidade do uso de zaragatoa bucal para a recolha de ADN, e defendendo o recurso ao critério da ponderação de bens, veio esclarecer que "[…] não existirá desproporcionalidade na utilização de tais métodos invasivos do corpo da pessoa (mas não lesivos da integridade física), da sua liberdade e privacidade, como único meio para a obtenção de prova em situações (tal qual a do presente caso) de extrema gravidade dos factos perpetrados, com base numa ponderação de todas as circunstâncias a efectuar por um juiz imparcial que não tem a seu cargo ou sob o seu domínio a investigação do processo […]"[397].

4.3.3.1. Exigência de lei formal

No que concerne ao primeiro requisito apresentado, cumpre deixar claro que o *princípio nemo tenetur se ipsum accusare*, assim como todos os direitos fundamentais, só pode ser restringido por lei[398]. Esta reserva material de lei tem duas dimensões principais: a primeira (dimensão negativa) significa que as matérias reservadas à lei não podem ser reguladas por outras fontes diferentes da lei; a segunda (dimensão positiva) significa que deve ser a lei a estabelecer efectivamente (com suficiente grau de certeza, precisão e densidade) o regime jurídico das matérias em questão[399].

---

[396] Acórdão do Tribunal Constitucional n.º 155/2007, de 2 de Março de 2007, disponível em: http://www.tribunalconstitucional.pt/tc/acordaos/20070155.html [consultado em 02.02.2017].

[397] Acórdão do Tribunal da Relação do Porto, de 10 de Dezembro de 2008, disponível em: http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/673fcb5dc0168da6802575220056a553?OpenDocument [consultado em 02.02.2017]. Também em sede de processos contra-ordenacionais, o Tribunal da Relação de Lisboa veio atestar que dada "[…] a necessidade de compatibilizar os diversos direitos, princípios e interesses constitucionalmente protegidos, caberá verificar se, no caso dos processos contra-ordenacionais investigados, instruídos e decididos pelo Instituto Nacional de Aviação Civil, existem razões que determinem a supressão ou a mera restrição do direito à não-autoincriminação, sempre em obediência ao princípio da proporcionalidade (cfr. n.º 2 do artigo 18.º da CRP)". Cf. Acórdão do Tribunal da Relação de Lisboa, de 17 de Abril de 2012, disponível em: http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/849980283d233cfd802579e6004e401f?OpenDocument [consultado em 02.02.2017].

[398] Gomes Canotilho, 2016: 453.

[399] Alexandrino, 2015: 128.

Este requisito constitucional das restrições está patente na problemática regra enunciada no n.º 2 do artigo 18.º da Constituição da República Portuguesa, segundo a qual a lei só pode restringir os direitos, liberdades e garantias nos casos expressamente previstos na Constituição. Sendo que o princípio *nemo tenetur* configura, como frisámos anteriormente, uma componente das garantias de defesa do arguido, asseguradas no artigo 32.º da CRP, cujo objectivo último é a sua protecção como sujeito no processo, parece claro que nos encontramos aqui perante uma restrição de direitos, liberdades e garantias.

Sobre o sentido e a função a reconhecer a essa singular cláusula da Lei Fundamental portuguesa, existem pelo menos três grupos de orientações na doutrina: a) as teses defensoras da relevância absoluta; b) as teses defensoras da relevância relativa; c) e as teses defensoras da irrelevância jurídica.

O primeiro grupo de orientações, defendido por Vieira de Andrade, pretende levar a sério a proibição constante dessa regra constitucional. Para este Autor, o n.º 2 do referido artigo estabelece categoricamente a figura das restrições legislativas. Assim, as restrições, nomeadamente ao princípio contra a autoincriminação, só seriam permitidas, entre nós, nos casos e para os efeitos em que fossem expressamente previstas pelos preceitos constitucionais relativos a esses direitos[400].

Uma segunda corrente doutrinária relativiza o sentido da proibição, fazendo-o, no entanto, de formas muito distintas, podendo designadamente considerar-se dois grupos, consoante persista uma ideia de resolver a dificuldade no quadro da norma ou de fugir a essa dificuldade[401]. Assim: a) para muitos Autores, da interpretação sistemática da Constituição decorreria a necessidade de admitir, ao lado das restrições expressamente autorizadas, restrições implícitas, restrições implicitamente autorizadas[402]; b) por outro lado, têm constituído exemplos de orientações centrífugas o recurso à figura dos limites imanentes *a priori*, o recurso ao n.º 2 do artigo 29.º da Declaração Universal dos Direitos do Homem, o recurso à transferência de limites ou a introdução da distinção, com imediatos efeitos de regime, entre restrição e condicionamento (limitação)[403].

[400] Vieira de Andrade, 2016: 271-273.
[401] Alexandrino, 2015: 131.
[402] Alexandrino, 2006: 445-448.
[403] Acórdão do Tribunal Constitucional n.º 155/2007, de 2 de Março de 2007, disponível em: http://www.tribunalconstitucional.pt/tc/acordaos/20070155.html [consultado em 10.02.2017].

Por fim, uma terceira tese, defendida por Jorge Reis Novais, vem afirmar que a regra enunciada no n.º 2 do artigo 18.º da Constituição não pode ser levada a sério. Estamos com o Autor, quando defende que o legislador constituinte português proclamou (no artigo 18.º) uma regra que não tem correspondência na natureza das coisas[404], pois é da natureza dos direitos fundamentais que estes entrem em colisão uns com os outros. Em segundo plano, adianta o Autor, se é verdade que os direitos, liberdades e garantias são trunfos, eles podem ser batidos por trunfos mais altos[405]. O Autor conclui com a defesa de que a consagração, na revisão constitucional de 1997, de uma liberdade geral de acção abrangente tem necessariamente como contrapartida o reconhecimento da possibilidade da sua limitação da forma mais ampla possível[406]. Efectivamente, se todas as restrições, nomeadamente ao princípio *nemo tenetur*, tivessem de ser previstas expressamente no texto constitucional, este haveria de conter muitos milhares de artigos[407].

Desta forma, defendemos a ideia de que uma restrição válida ao princípio *nemo tenetur se ipsum accusare* não necessita de constar expressamente na Constituição da República Portuguesa, mas antes de ser admitida dentro da unidade desta.

4.3.3.2. Necessidade de salvaguarda de outro direito ou interesse constitucionalmente protegido

O segundo requisito material para a restrição legítima de direitos, liberdades e garantias consiste em que ela só se pode justificar para salvaguardar um outro direito ou interesse constitucionalmente protegido (n.º 2 do artigo 18.º da CRP). Este requisito significa fundamentalmente que o sacrifício, ainda que parcial, de um direito fundamental, não pode ser arbitrário, gratuito ou desmotivado[408].

Não há consenso na doutrina quanto à necessidade de estatura constitucional do outro direito ou interesse que justifica a restrição.

Por um lado, Gomes Canotilho e Vital Moreira defendem que é vedada ao legislador a possibilidade de justificar a restrição de direitos, liberdades e garantias por eventual colisão com outros direitos ou bens tutelados apenas a nível infraconstitucional. Para estes

[404] Reis Novais, 2010: 581 e 587.
[405] Reis Novais, 2006: 52.
[406] Reis Novais, 2010: 591.
[407] Martinez, 1992: 33.
[408] Gomes Canotilho/Moreira, 2014: 391.

Autores torna-se necessário "que o interesse, cuja salvaguarda se invoca para restringir um dos direitos, liberdades ou garantias, tenha no texto constitucional suficiente e adequada expressão" (*v.g.* património cultural, defesa nacional, ordem constitucional democrática, segurança pública, saúde pública, entre outros)[409].

Por outro lado, Jorge Reis Novais, com quem concordamos, reitera que qualquer valor digno de protecção jurídica pode fundamentar uma restrição aos direitos fundamentais, uma vez que indagar do fundamento da restrição através de uma distinção de hierarquia meramente formal de bens pode mascarar aquilo que está realmente em causa – saber se os direitos fundamentais podem ser restringidos em função da protecção de bens de estatura infraconstitucional, mas que no caso concreto apresente um valor ou peso superior ao dos direitos fundamentais que se pretende restringir[410]. Defende o Autor que mesmo direitos ou interesses não consagrados na Lei Fundamental podem restringir direitos fundamentais. Será, ainda segundo o Autor, o peso concreto e material dos princípios opostos que determinará a preferência relativa no caso concreto, independentemente do nível constitucional ou infraconstitucional da garantia jurídica, que é só mais um entre os diversos factores que devem ser considerados na ponderação[411].

4.3.3.3. Princípio da proporcionalidade em sentido amplo

Decorre do n.º 2 do artigo 18.º da Constituição da República Portuguesa, que as restrições aos direitos, liberdades e garantias têm de ser necessárias para a salvaguarda de outros direitos ou interesses constitucionalmente protegidos e têm de limitar-se ao necessário para esse fim[412]. Assim, para além de ter de constar em lei autorizada, com carácter geral e abstracto, a ordem restritiva (nomeadamente, a ordem de desencriptação de smartphones) tem, ainda, que ser adequada, ou seja, apropriada aos fins que se propõe atingir, necessária, na medida em que só é admissível quando for impossível utilizar outro meio menos oneroso, e proporcional em relação aos resultados obtidos[413].

---

[409] Gomes Canotilho/Moreira, 2014: 392.
[410] Reis Novais, 2010: 602-603.
[411] Reis Novais, 2010: 604.
[412] Alexandrino, 2015: 134.
[413] Correia, 1999a: 59. Em sentido semelhante, "as restrições estão sujeitas ao princípio da proporcionalidade – só podem ser estabelecidas quando os fins, os interesses e os valores constitucionais só através deles possam ser protegidos, devem, em cada caso, realizar esses fins e não outros e devem corresponder à medida, à justa medida, também em cada caso concreto". Cf. Miranda, 2006: 97. "O valor constitucional dos preceitos relativos aos direitos fundamentais só é efectivamente garantido se se exigir que a eventual restrição seja adequada e justificada pela necessidade de proteger ou promover um bem constitucionalmente valioso e só na proporção dessa necessidade". Cf. Vieira de Andrade, 2016: 287. "[…]

Apesar de a Constituição, no seu artigo 18.º, não fazer menção expressa à proporcionalidade como parâmetro de controlo, a doutrina portuguesa fez formalmente do princípio da proporcionalidade o núcleo central dos requisitos materiais exigidos às restrições de direitos fundamentais[414].

O texto constitucional faz, ainda que implicitamente, referência ao princípio da proporcionalidade em sentido amplo, que estabelece um limite constitucional à liberdade de conformação do legislador[415]. O princípio da proporcionalidade em sentido amplo constitui um verdadeiro super conceito (*Oberbegriff*), super conceito esse que tem sido tradicionalmente decomposto em três subprincípios (corolários, máximas ou dimensões): a) o da adequação (ou idoneidade); b) o da necessidade (indispensabilidade ou do meio menos restritivo); c) o da proporcionalidade em sentido estrito (ou da justa medida)[416].

O primeiro subprincípio, da adequação ou idoneidade, significa que as medidas restritivas devem ser aptas ou idóneas para realizar o fim prosseguido pela restrição. Ou seja, este subprincípio exige que a medida restritiva em causa seja considerada, através de um juízo de prognose[417], apta a realizar o fim visado com a restrição ou contribua para o alcançar[418]. Para que se apure a existência de inconstitucionalidade será necessário que o responsável pela restrição pudesse ter previsto tal inaptidão no momento em que a decidiu ou a actuou. O controlo da adequação acaba por ser, segundo Jorge Reis Novais, um controlo *ex ante*, incidindo sobre a prognose realizada pelos poderes públicos responsáveis pela criação ou concretização da restrição a direitos fundamentais[419]. Desta forma, viola-se este corolário sempre que, tendo em conta os conhecimentos empíricos e científicos disponíveis no momento da aprovação da medida, esta se revele inapta para atingir o fim visado: será naturalmente inapta se os efeitos dessa medida se revelarem

---

as restrições de direitos fundamentais carecem também de justificação, não podendo legitimar-se senão pela necessidade de salvaguardar outros direitos ou interesses constitucionalmente protegidos e não podendo ultrapassar a medida necessária para o efeito (n.º 2 do artigo 18.º). É a consagração expressa do chamado princípio da proporcionalidade, que proíbe, nomeadamente, as restrições desnecessárias, inaptas ou excessivas de direitos fundamentais. Os direitos fundamentais só podem ser restringidos quando tal se torne indispensável, e no mínimo necessário, para salvaguardar outros direitos ou interesses constitucionalmente protegidos". Cf. Gomes Canotilho/Moreira, 1991: 133-134.

414 Reis Novais, 2010: 729-730.

415 "A Constituição, ao autorizar a lei a restringir direitos, liberdades e garantias, de forma a permitir ao legislador a realização de uma tarefa de concordância prática justificada pela defesa de outros bens ou direitos constitucionalmente protegidos, impõe uma clara vinculação ao exercício dos poderes discricionários do legislador". Cf. Gomes Canotilho, 2016: 457.

416 Alexandrino, 2015: 135.

417 Rodrigues, 2009b: 216.

418 Reis Novais, 2010: 731.

419 Reis Novais, 2010: 739.

indiferentes ou contrários à realização do fim em vista[420]. É ainda de referir que a aptidão deve ser aferida não no sentido de uma exigência que só se considera cumprida quando o meio realiza integral ou plenamente o fim visado, mas bastando-se, antes, com uma aproximação sensível, ainda que parcelar, do fim pretendido[421]. Relativamente aos fins, pressupõe-se que os mesmos sejam legítimos e, além disso, que sejam jurídica e materialmente possíveis.

O segundo corolário, da necessidade, indispensabilidade ou do meio menos restritivo, que constitui, sem dúvida, o teste mais complexo, exigente e decisivo, significa que se deve recorrer ao meio menos restritivo para atingir o fim em vista[422]. Isto é, o princípio da necessidade impõe que se recorra, para atingir esse fim, ao meio necessário, exigível ou indispensável, no sentido do meio mais suave ou menos restritivo que precise de ser utilizado para atingir o fim em vista[423]. A indispensabilidade afere-se então pela comparação entre os prejuízos provocados por esse meio e os prejuízos que seriam provocados pela utilização de um meio alternativo menos agressivo. Por sua vez, a desnecessidade da agressão afere-se em relação aos prejuízos provocados pela medida restritiva, avaliados em função de critérios materiais, espaciais, temporais ou pessoais e tendo em conta, não apenas o direito fundamental directamente atingido, como qualquer outra afectação desvantajosa da liberdade, dos direitos fundamentais ou de outros interesses juridicamente relevantes do mesmo titular ou de outros afectados[424]. O teste é complexo desde logo porque é função de múltiplas variáveis, nomeadamente: do tipo concreto de afectação, da agressividade do meio, da medida da eficácia dos vários meios ou da existência de outros efeitos colaterais[425].

Por fim, o terceiro e último subprincípio, o da proporcionalidade em sentido estrito ou da justa medida, visa apurar o equilíbrio na relação entre a importância do fim visado e a gravidade do sacrifício imposto. Na verdade, uma medida pode ser adequada e necessária

[420] Gomes Canotilho, 2016: 457.
[421] Reis Novais, 2010: 738. Qualquer exigência de plena realização do fim seria impossível de ser atingida pelo legislador aquando da realização da medida, uma vez que não há como saber *a priori* se a medida irá efectivamente realizar o fim, motivo pelo qual basta que a medida seja adequada para fomentar o fim.
[422] Alexandrino, 2015: 136.
[423] Neste sentido vai também a jurisprudência do Supremo Tribunal de Justiça, ao afirmar que "ainda que se considere a medida idónea, esta deve ser necessária, ou seja, perante medidas que oferecem idêntica idoneidade, deve escolher-se a que ofereça o menor potencial de prejuízo para o visado, mesmo que exija mais tempo para a sua realização, obrigando a utilizar outros meios de obtenção de prova […]". Cf. Acórdão do Supremo Tribunal de Justiça n.º 14/2014, de 21 de Outubro de 2014, disponível em: https://dre.pt/application/file/58512485 [consultado em 16.02.2017].
[424] Reis Novais, 2010: 741.
[425] Gomes Canotilho, 2016: 458.

e ao mesmo tempo afectar de forma excessiva, intolerável ou desproporcionada o direito em questão[426]. Este corolário está relacionado com a ideia de pesar, de sopesar, de ponderar as vantagens e desvantagens presentes num determinado cenário de restrição. Segundo Alexy, o subprincípio da proporcionalidade em sentido estrito corresponde a uma máxima que pode ser designada como "Lei da Ponderação". Esta máxima defende que quanto maior for o grau de não realização ou de afectação de um princípio, maior deve ser a importância da realização do princípio colidente[427]. De facto, aqui já não é a ponderação entre bens que está em análise, mas antes a medida restritiva que foi concretamente adoptada no seguimento daquela ponderação e, mais precisamente, o controlo da proporcionalidade dessa medida restritiva. E, neste controlo de proporcionalidade em sentido estrito, aquilo que se avalia, que se compara ou que se põe em relação, são os sacrifícios (custos) impostos ao direito fundamental contrapostos aos benefícios (vantagens) produzidos na obtenção do fim visado com a restrição[428]. Se a adopção de uma medida restritiva adoptada introduz na ordem jurídica um benefício marginal mínimo para o fim visado, mas produz, simultaneamente, um acréscimo significativo de sacrifício na liberdade, na autonomia ou no bem-estar, então a ponderação dessas grandezas com as que resultam das medidas alternativas actualmente em vigor pode revelar uma relação claramente desproporcionada e, daí, a inconstitucionalidade da nova medida[429].

Por fim, quanto à concretização jurisprudencial, pode afirmar-se que o princípio da proporcionalidade em sentido amplo, ou princípio da proibição do excesso, é talvez o cânone mais utilizado pelos tribunais portugueses. O Tribunal da Relação de Lisboa chega mesmo a afimar, no seu acórdão de 3 de Março de 2016, que o princípio da proporcionalidade em sentido amplo configura-se "como a trave mestra de legitimação do "*ius puniendi*" estatal e de toda a restrição de direitos fundamentais"[430]. O douto tribunal dissocia ainda, de uma forma clara, as três dimensões do princípio: adequação,

[426] Alexandrino, 2015: 137.
[427] Alexy, 2014: 821.
[428] Reis Novais, 2012: 128.
[429] Reis Novais, 2012: 131.
[430] Acórdão do Tribunal da Relação de Lisboa, de 3 de Março de 2016, disponível em: http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/36f34b50b321b89980257f6f004d5fc6?OpenDocument [consultado em 16.02.2017].

necessidade e proporcionalidade (*stricto sensu*), aplicando cada uma delas ao caso concreto[431].

4.3.3.4. Garantia do conteúdo essencial

O último requisito material da legitimidade das restrições a direitos fundamentais consiste na ideia de que existe um núcleo essencial dos direitos, liberdades e garantias que não pode, em caso algum, ser violado. Mesmo nos casos em que o legislador está constitucionalmente autorizado a editar normas restritivas, ele permanece vinculado à salvaguarda do núcleo essencial dos direitos[432].

Esta garantia do núcleo/conteúdo essencial dos direitos fundamentais, apesar de ser uma criação especificamente alemã, encontrou um eco generalizado na doutrina e jurisprudência constitucionais de vários outros países, incluindo mesmo uma recepção constitucional expressa, como aconteceu entre nós (n.º 3 do artigo 18.º da Constituição da República Portuguesa). Efectivamente, na doutrina alemã, cuja Constituição contém uma cláusula semelhante, que inspirou a nossa, aparecem dois tipos de teorias atinentes à natureza do conteúdo essencial, habitualmente designadas como teorias absolutas e teorias relativas.

Para as teorias absolutas, o núcleo essencial consistiria num conteúdo normativo irrestringível, abstractamente fixado[433]. Desta forma, podemos afirmar que a teoria absoluta é, assim, uma perspectiva ontológico-substancialista que entende o conteúdo essencial como grandeza estática e intemporal. Independentemente do interesse ou bem que justifique a restrição e da importância relativa da sua realização, esta teoria considera que há, em cada direito fundamental, uma zona, esfera ou âmbito nuclear intocável[434] que, sob pena de desnaturação ou perda do seu sentido útil, em caso algum poderá ser

---

[431] "O princípio da idoneidade […] traduz-se na ideia de que se exige uma relação de adequação entre o meio usado e o fim perseguido. […] o princípio da necessidade e da mínima intervenção implica a necessária utilização de outros meios menos lesivos para os direitos fundamentais, quando isso se afigure possível. […] o princípio da proporcionalidade em sentido estrito ou da adequação ao fim, exige uma ponderação do interesse em conflito segundo um critério de justiça material, […] implica uma ponderação entre os interesses individuais que se vão constranger, e os interesses que se pretendem defender". Cf. Acórdão do Tribunal da Relação de Lisboa, de 3 de Março de 2016, disponível em: http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/36f34b50b321b89980257f6f004d5fc6?OpenDocument [consultado em 16.02.2017].

[432] Gomes Canotilho, 2016: 458.

[433] Gomes Canotilho, 2016: 459.

[434] Neste sentido vai Robert Alexy, ao afimar que, segundo as teorias absolutas, existe um núcleo essencial em todos os direitos fundamentais que, em nenhum caso, pode ser afectado. Cf. Alexy, 2008: 259.

afectada[435]. Segundo alguns Autores, o núcleo essencial corresponderia à projecção da dignidade humana em cada direito e seria afectado sempre que o indivíduo se tornasse objecto do acontecer estadual, para outros, significaria uma certa medida de valor social global que teria sempre de sobrar depois da restrição, para outros ainda, seria constituído pelos elementos típicos que conferem carácter ao direito[436].

Por seu turno, as teorias relativas reconduzem o conteúdo essencial aos princípios da exigibilidade e da proporcionalidade: a restrição só seria legítima quando (se) fosse exigida para a realização de bens jurídicos que devessem ser considerados (no caso) como mais valiosos e só na medida em que essa exigência se imponha ao direito fundamental[437]. Assim, não é a gravidade ou intensidade da lesão, a relevância da justificação ou o tipo de prejuízo na liberdade que determinam, por si só, a activação da garantia do núcleo essencial. O que está em causa é, segundo Jorge Reis Novais, a natureza da relação que se estabelece entre os bens em confronto e entre o fim prosseguido com a restrição e o meio utilizado, considerando-se que há violação do conteúdo essencial dos direitos fundamentais quando se verifica um excesso, uma desproporcionalidade, uma desnecessidade, independentemente do muito ou pouco que reste do direito fundamental após a incidência da restrição[438]. Donde facilmente se conclui que, para a teoria relativa, a garantia do conteúdo essencial se identifica com o princípio da proporcionalidade em sentido amplo/proibição do excesso num quadro de ponderação de bens.

Estamos com Gomes Canotilho e Vital Moreira, que defendem uma solução intermédia, uma teoria mista, segundo a qual a questão do conteúdo essencial de um direito não se pode equacionar senão em confronto com outro bem, mas, nos termos da Constituição, nunca essa ponderação poderá conduzir à aniquilação de qualquer direito fundamental[439]. A garantia do conteúdo essencial deve servir como um "*plus*" em relação ao princípio da proporcionalidade. Ou, como sustenta Jorge Miranda, deverá funcionar como barreira última e efectiva contra o abuso do poder, que não pode ser violada em qualquer hipótese[440].

---

[435] Reis Novais, 2010: 782.
[436] Vieira de Andrade, 2016: 282-283.
[437] Vieira de Andrade, 2016: 283.
[438] Reis Novais, 2010: 781.
[439] Gomes Canotilho/Moreira, 2014: 395.
[440] Miranda, 2014: 315. Nesta linha de pensamento, Gomes Canotilho e Vital Moreira, reiteram que a garantia do conteúdo essencial é uma baliza última de defesa dos direitos, liberdades e garantias, delimitando um núcleo que, em nenhum caso, deverá ser invadido. Cf. Gomes Canotilho/Moreira, 2014: 396.

Em termos práticos, pode dizer-se que o requisito da proporcionalidade, mencionado no ponto anterior, é uma terceira aproximação (depois da exigência da legalidade e da necessidade de salvaguarda de outro direito ou interesse constitucionalmente protegido), dado que a existência de uma restrição arbitrária, desproporcionada, é um índice relativamente seguro da ofensa do núcleo essencial. Sem embargo, independentemente de haver ou não uma desproporcionalidade na restrição, há que salvaguardar sempre a extensão do núcleo essencial.

Desta forma, apoiamo-nos no recurso a uma teoria mista sustentada pelos Autores, a um tempo relativa e absoluta: "relativa, porque a própria delimitação do núcleo essencial dos direitos, liberdades e garantias tem de articular-se com a necessidade de protecção de outros bens ou direitos constitucionalmente garantidos; absoluta, porque, em última análise, para não existir aniquilação do núcleo essencial, é necessário que haja sempre um resto substancial de direito, liberdade e garantia, que assegure a sua utilidade constitucional"[441].

O conteúdo inatacável dos preceitos relativos aos direitos, liberdades e garantias começa, assim, onde acaba a possibilidade e legitimidade da sua restrição[442].

4.3.3.5. Requisitos formais: generalidade, abstracção e não retroactividade

Segundo o primeiro requisito formal - lei geral e abstracta -, a restrição de um qualquer direito fundamental deve ser aplicável a um número indeterminado ou indeterminável de pessoas (proibição de leis individuais) e não pode ter como objecto um caso concreto, ou melhor, deve regular um número indeterminado ou indeterminável de casos (proibição de leis concretas)[443]. Estes dois requisitos são cumulativos.

Note-se que não basta que as leis sejam formalmente ou aparentemente gerais e abstractas. Importa que o sejam material e realmente, sendo ilegítimas as leis individuais e/ou concretas camufladas em forma geral e abstracta[444].

Ainda assim, apesar de não estar expressamente referido, Vieira de Andrade esclarece que deve ainda considerar-se que a restrição ao princípio *nemo tenetur*, ou a qualquer outro princípio, "em função da reserva de lei formal, tem de apresentar uma densidade

[441] Gomes Canotilho/Moreira, 2014: 395.
[442] Vieira de Andrade, 2016: 287.
[443] Gomes Canotilho, 2016: 454.
[444] Gomes Canotilho/Moreira, 2014: 393.

suficiente, isto é, um certo grau de determinação do seu conteúdo, pelo menos no essencial, não sendo legítimo que se deixe à Administração espaços significativos de regulação ou de decisão […]"[445].

O segundo requisito formal das restrições de direitos, liberdades e garantias está relacionado com o respeito pelo princípio da não retroactividade. Desta forma, qualquer restrição a direitos fundamentais não pode, portanto, aplicar-se a situações ou actos passados, mas antes e apenas aos verificados ou praticados após a sua entrada em vigor[446]. Este princípio da não retroactividade não é um princípio constitucional irrestritamente válido na ordem jurídica portuguesa, mas é-o, sem quaisquer excepções, no que respeita a restrições de direitos, liberdades e garantias ou de direitos análogos (n.º 3 do artigo 18.º e artigo 17.º da Constituição da Repúblcica Portuguesa)[447].

A proibição incide, segundo Gomes Canotilho e Vital Moreira, sobre a chamada retroactividade autêntica, em que as leis restritivas de direitos afectam posições jusfundamentais já estabelecidas no passado ou, mesmo, esgotadas[448]. Ela abrangerá também alguns casos de retrospectividade ou de retroactividade inautêntica sempre que as medidas legislativas se revelarem arbitrárias, inesperadas, desproporcionadas ou afectarem posições jusfundamentais dos particulares de forma excessivamente gravosa e imprópria.

A razão de ser deste requisito está, ainda segundo o entendimento dos referidos Autores, intimamente ligada à ideia de protecção da confiança e da segurança dos cidadãos, defendendo-os contra o perigo de verem atribuir aos seus actos passados ou às situações transactas efeitos jurídicos com que razoavelmente não podiam contar[449]. Por seu turno, Jorge Reis Novais, defende aqui a ideia de que a proibição de restrições a direitos fundamentais de carácter retroactivo decorre do princípio da protecção da confiança[450].

Por fim, em jeito de conclusão desta problemática dos limites aos limites, cumpre deixar claro que, pela nossa parte, não rejeitamos a possibilidade de poder haver casos de colaboração do arguido. Concluímos pela existência de uma tipicidade dos casos de colaboração do arguido, mas admitimos que uma lei formal possa impor novos casos de

[445] Vieira de Andrade, 2016: 290-291.
[446] Gomes Canotilho/Moreira, 2014: 394.
[447] Gomes Canotilho, 2016: 456.
[448] Gomes Canotilho/Moreira, 2014: 394.
[449] Gomes Canotilho/Moreira, 2014: 395.
[450] Reis Novais, 2010: 816-817.

colaboração, contando que se respeitem os n.os 2 e 3 do artigo 18.º da Constituição da República Portuguesa[451]. Assim, o ponto é que haja uma lei formal que exija a colaboração, que esta seja necessária, adequada e proporcional em sentido estrito, que não afecte o núcleo essencial do direito fundamental restringido e que seja uma restrição de carácter geral, abstracto e não retroactivo.

4.3.4. Críticas ao critério de ponderação de bens

Depois de analisado o critério da ponderação como método de resolução de conflitos entre direitos fundamentais, cumpre agora trazer à colação as várias críticas apresentadas pela doutrina a este critério. Independemente da concordância ou não com esta metodologia, não podem deixar de se reconhecer os perigos do recurso à ponderação de bens neste contexto.

Considerando o entendimento de parte da doutrina, diremos que os argumentos avançados contra o recurso à metodologia da ponderação de interesses são, ainda que genericamente: a ausência de linhas seguras que regulem ou orientem a solução dos casos de direitos fundamentais, a imprevisibilidade associada a essa desregulação, a manipulabilidade do método e as consequentes ameaças para uma protecção adequada das posições jusfundamentais dos particulares protegidas pelas normas constitucionais[452].

No que ao princípio *nemo tenetur* diz respeito, segundo o entendimento de Sandra Oliveira e Silva, a solução da ponderação acaba por enfraquecer a consistência da sua tutela jurídica, uma vez que o juízo de ponderação do legislador ou do aplicador não é balizado de forma cuidadosa por parâmetros materiais objectivos extraídos das próprias normas constitucionais[453]. Para a Autora, à ponderação de bens caberá, em rigor, delimitar o âmbito normativo de cada direito fundamental, vale dizer, determinar o *quid* protegido pelas normas que os consagram. Desta forma, o recurso à metodologia da ponderação acabaria por gerar riscos de subjectivismo e arbitrariedade na decisão, passando de um Estado-de-Direito para um Estado-de-Ponderação[454].

A ponderação é vista, assim, como um método de esvaziamento do âmbito de protecção dos direitos fundamentais, onde tudo é deixado em aberto à relativização e à

[451] Pinto, 2013: 111.
[452] "[…] dir-se-ia que a vantagem prática da ponderação de bens é a de que pode ser utilizada para justificar qualquer decisão, tanto a admissibilidade da restrição como exactamente o contrário; a desvantagem é a de que toda a gente de apercebe disso…". Cf. Reis Novais, 2010: 694.
[453] Oliveira Silva, 2015: 617-619.
[454] Oliveira Silva, 2015: 620.

arbitrariedade. Efectivamente, segundo este entendimento, o critério da ponderação, por não delimitar parâmetros materiais objectivos extraídos do texto da lei que permitam a comparação dos bens constitucionais em conflito e por rejeitar a existência de uma ordem constitucional de valores, acaba por converter-se numa simples fórmula vazia insusceptível de produzir resultados seguros.

Em síntese, pela junção dos argumentos acima mencionados, a ponderação é altamente criticada por pautar-se num intenso subjectivismo, não possuindo mecanismos de prevenção ao arbítrio, nem tampouco consistência metodológica.

Da nossa parte, se bem que reconhecendo a pertinência das críticas dirigidas à ponderação de bens, delas não nos permitimos inferir a rejeição do método, mas tão só a importância dos riscos da sua utilização. De resto, como grande parte dos Autores tidos como adeptos da ponderação de bens, consideramos que o recurso a essa metodologia é inevitável, na medida em que, sendo o procedimento que intuitivamente corresponde ao sentimento comum de justiça na resolução de conflitos de bens ou de interesses, não é possível prescindir da sua utilização nem encontrar qualquer outro método que o substituía com proveito sempre que se trate de determinar uma relação de prevalência num contexto de colisão entre direitos, liberdades e garantias[455]. Explicaremos de seguida o porquê desta nossa posição através da contestação das críticas apresentadas.

Uma das críticas apresentadas contra a ponderação de bens prende-se com a ausência de critérios que regulem ou orientem a solução dos conflitos entre direitos fundamentais. Sem embargo, e apesar de a Constituição não fornecer critérios definidos para a resolução de cada conflito em concreto, cremos que da Lei Fundamental podemos deduzir critérios e parâmetros de valoração objectivos que, vinculando os resultados da ponderação, a tornem verificável, previsível e escrutinável e impeçam que esse procedimento se converta numa decisão valorativa subjectiva e irrefutável do julgador.

Senão, leiam-se os números 2 e 3 do artigo 18.º da Constituição da República Portuguesa, que consagram a necessidade de as restrições, fundamentadas essencialmente em decisões de ponderação de bens, observarem os limites aos limites dos direitos fundamentais aplicáveis a quaisquer restrições. Desde logo, de acordo com a chamada lei da ponderação de Alexy, a intensidade do prejuízo sofrido por um dos bens deve ser compensada pelo peso relativo do bem que a justifica, dependendo, a decisão de

[455] Reis Novais, 2010: 640-641.

prevalência, do alcance que venha a atingir a restrição que a concretiza. Assim, a medida concreta do recuo ou da cedência que um bem em colisão tem que suportar num caso concreto é condicionada pelos limites aos limites que a nossa Constituição consagra explicitamente, e que, de resto, deveriam ser sempre observados, já que, grosso modo, correspondem a exigências que o princípio do Estado de Direito coloca a quaisquer actuações restritivas da liberdade[456].

Uma decisão de ponderação terá sempre de observar, como mencionado anteriormente, os princípios da reserva de lei, da necessidade de salvaguarda de outro direito ou interesse constitucionalmente protegido, da proporcionalidade em sentido amplo e da protecção do núcleo essencial dos direitos fundamentais, bem como os requisitos formais da generalidade, abstracção e não retroactividade (n^{os} 2 e 3 do artigo 18.º da CRP), traçando, desta forma, fronteiras claramente discerníveis do âmbito de protecção de cada direito fundamental restringido, evitando a subjectividade.

Logo, sendo certo que a ponderação de bens não pode deixar de observar estes critérios constitucionais que regem a actuação dos poderes constituídos, no caso das situações de restrição de direitos fundamentais, aquele perigo de falta de parâmetros materiais objectivos para a resolução de conflitos deixa de fazer sentido. Não haverá, na generalidade dos casos, uma inobservância ou dissolução de critérios constitucionais exclusivamente pelo facto de se ter recorrido à metodologia da ponderação de bens como forma de solucionar a colisão que envolva um direito fundamental consagrado sem reservas[457].

Quanto à questão da rejeição de uma ordem constitucional de valores, cumpre deixar claro que, a ponderação de bens, utilizada no domínio das restrições aos direitos fundamentais, raramente surge limitada à avaliação do peso relativo de dois bens ou interesses numa dada situação, antecipada ou verificada, de colisão. Para além desse factor, ela envolve simultaneamente, como já tivemos oportunidade de referir em sede de análise ao princípio da proporcionalidade em sentido amplo, uma valoração das vantagens e desvantagens que a restrição de determinado direito fundamental inevitavelmente provoca, bem como a ponderação das vantagens e desvantagens de um meio alternativo menos agressivo/restritivo.

[456] Reis Novais, 2010: 723-724.
[457] Reis Novais, 2010: 696.

Assim, de nada serve, para os fins em causa, proceder a uma hierarquização abstracta entre dois direitos fundamentais. Para demonstrar esta desnecessidade de hierarquização, Jorge Reis Novais dá o exemplo do conflito entre a liberdade religiosa e a saúde pública, quando o exercício da primeira arrasta consigo o perigo de uma propagação de epidemia. Aqui, o conflito em questão não é, segundo o Autor, entre aqueles dois bens em abstracto, mas sim entre, de um lado, "uma manifestação parcelar, substituível, eventualmente adiável de uma forma particular de culto religioso por parte de alguns cidadãos e, de outro, as ameaças, mais ou menos remotas, intensas, reais ou aparentes que impendem sobre a saúde de outros ou dos mesmos cidadãos" [458]. Por conseguinte, mesmo que essa hierarquização fosse constitucionalmente possível, ela de nada adiantaria sobre a prevalência de um ou de outro bem, uma vez que deve sempre assistir-se a uma valoração ponderada das vantagens e desvantagens da restrição em determinado caso concreto.

Do ponto de vista da jurisprudência internacional, cumpre ainda deixar claro que o próprio Tribunal Europeu dos Direitos Humanos, deparando-se com uma situação de restrição a direitos fundamentais, recorre sistematicamente à metodologia da ponderação de bens (e não apenas ao critério da dependência/independência da vontade do arguido). E, também aqui, a ponderação é necessariamente fundada sobre uma elaboração dogmática genérica acerca do sentido das "exigências da sociedade democrática" e não constitucionalmente pré-determinadas por qualquer hipotética ordem de valores[459].

Desta feita, podemos concluir que a crítica à ponderação baseada na falta de parâmetros materiais objectivos e a resultante tentativa de criar critérios rígidos e pré-definidos *a priori* para a resolução de conflitos entre direitos fundamentais, defendidas pelas estratégias absolutistas, falham por culminarem em duas situações alternativas: a) em soluções abstractas inadequadas, não realistas e, até, pura e simplesmente inaplicáveis; b) ou, em contrapartida, em soluções baseadas, de facto, em ponderações, mas que, não sendo assumidas enquanto tal, não podem, consequentemente, ser sujeitas ao controlo e à crítica. Por este motivo, somos da opinião de que nunca será possível prescindir do reconhecimento de uma margem de apreciação que permita, mediante procedimentos de

[458] Reis Novais, 2010: 701.
[459] Reis Novais, 2010: 707.

ponderação e respeitando os critérios impostos constitucionalmente, dar resposta a um caso concreto de conflito entre direitos fundamentais[460].

Por fim, no que respeita à questão da arbitrariedade na decisão derivada da circunstância de ser o juiz a proceder à ponderação de bens, cumpre esclarecer que mais importante que discutir se os tribunais podem proceder a ponderações é considerar a forma como essas ponderações se devem processar num quadro de necessária garantia de previsibilidade, estabilidade e igualdade. Para assegurar a redução da discricionariedade judicial nos procedimentos de ponderação, os juízes devem atender aos critérios impostos constitucionalmente nos já mencionados n.os 2 e 3 do artigo 18.º da Lei Fundamental. Desta forma, o método da ponderação de bens, mediante a intervenção de condicionantes jurídico-constitucionais, pode escapar a um decisionismo casuístico. É que, diz-se, na ausência de critérios jurídicos objectivos e precisos, susceptíveis de se imporem vinculativamente aos procedimentos de valoração e ponderação de bens, é a vontade subjectiva do julgador que acaba por prevalecer, com o inconveniente de essa prevalência se estabelecer com o sacrifício da decisão de quem fora eleito para proceder à ponderação dos interesses subjacentes às colisões em causa[461].

Pelos motivos enunciados, acreditamos que a ponderação de bens constitui, assim, a chave da solução do problema das restrições a direitos fundamentais. E, optando pelo critério da ponderação de bens como o método ideal para a delimitação da área de tutela do princípio *nemo tenetur se ipsum accusare*, resta-nos averiguar se, com base neste critério, a revelação da palavra-passe e a leitura da impressão digital do arguido para desencriptação de smartphones estão ou não sob o âmbito de protecção desse princípio.

[460] Cumpre salientar, neste âmbito, que o próprio direito à vida não se pode considerar isento de valoração e ponderações no caso concreto. Jorge Reis Novais dá o exemplo do conflito entre o direito à vida e a segurança do Estado, defendendo que, apesar de o direito à vida ter uma preferência ética relativamente a este último, no caso concreto em que um grupo de terroristas rapta um empresário e ameaça, com toda a verosimilhança, matá-lo caso o Estado não satisfaça as suas exigências, a solução seria ou prescindir do controlo ou aderir a um controlo de constitucionalidade essencialmente concretizado e dependente de valoração e ponderação de bens. Não há, segundo o Autor, alternativas à ponderação de bens que se traduzam em acréscimo de racionalidade, de segurança jurídica e, sobretudo, de protecção efectiva dos direitos fundamentais. Cf. Reis Novais, 2010: 719.
[461] Reis Novais, 2010: 697-698.

5. Aplicabilidade do princípio *nemo tenetur se ipsum accusare* na desencriptação de smartphones para obtenção de prova em processo penal

Depois de feita a apreciação dos casos jurisprudenciais de desencriptação de smartphones com o auxílio do arguido nos Estados Unidos da América, a análise sobre o acesso e apreensão dos seus conteúdos no ordenamento jurídico português, a encriptação destes dispositivos e a possibilidade de violação do princípio *nemo tenetur se ipsum accusare* nos casos de desencriptação compelida dos mesmos, chegamos à derradeira questão da nossa investigação: tendo como referência os casos apresentados no Capítulo I e, recorrendo à legislação, doutrina e jurisprudência portuguesas, seriam estas desencriptações de smartphones, através da revelação da palavra-passe ou da leitura da impressão digital do arguido, violadoras do princípio de não-autoincriminação?

Já foi salientado diversas vezes durante o nosso estudo que o princípio *nemo tenetur se ipsum accusare* não é absoluto, pelo que pode ser restringido, quer na sua vertente de direito ao silêncio do arguido, quer na sua dimensão de princípio contra a autoincriminação. A título de exemplo, podemos chamar à colação as restrições a este princípio que têm sido assumidas pelo legislador, sempre por via da intervenção dos limites aos limites, com previsão constitucional expressa nos n.^{os} 2 e 3 do artigo 18.º da Lei Fundamental, nomeadamente: a) a obrigação do arguido responder com verdade às perguntas sobre a sua identidade (al. b) do n.º 3 do artigo 61.º do CPP); b) a obrigatoriedade de realizar determinados exames, por exemplo de alcoolemia ou de substâncias psicotrópicas (artigos 152.º e 153.º do Código da Estrada) ou exames de ADN para fins de investigação criminal (n.º 1 do artigo 8.º da Lei n.º 5/2008, de 12 de Fevereiro, e artigo 172.º do CPP).

No caso concreto de desencriptação de smartphones para obtenção de prova em processo penal, este princípio entrará em confronto com outros valores, nomeadamente, com a persecução da justiça e a descoberta da verdade material.

Como referido anteriormente, segundo o critério da ponderação de bens, são legítimas as restrições ao princípio *nemo tenetur se ipsum accusare* que observem os seguintes requisitos: a) devem estar previstas em lei formal; b) devem ter como objectivo a salvaguarda de outro direito ou interesse constitucionalmente protegido; c) devem obedecer ao princípio da proporcionalidade em sentido amplo – adequação, necessidade e proporcionalidade em sentido estrito; d) não devem aniquilar o direito em causa

atingindo o conteúdo essencial do respectivo preceito. Além da verificação destes requisitos materiais, todas as restrições ao *nemo tenetur* devem ainda observar dois requisitos de ordem formal: a) generalidade e abstracção; b) não retroactividade.

Tendo como referência os casos norte-americanos apresentados no Capítulo I, relativos à ordem de desencriptação dirigida ao arguido no sentido de revelar a sua palavra-passe ou de permitir a leitura da sua impressão digital, veremos de seguida se estes critérios estão ou não respeitados nesses casos. Por questões de ordem prática, faremos uma divisão entre o primeiro e o segundo método de desbloqueio do dispositivo.

5.1. Desencriptação de smartphones através da revelação da palavra-passe

Para podermos aferir da legitimidade da ordem de desencriptação de um smartphone através da revelação da palavra-passe pelo arguido, cumpre analisar se esta ordem está prevista em lei formal, se tem como objectivo a salvaguarda de outro direito ou interesse constitucionalmente protegido, se obedece ao princípio da proporcionalidade em sentido amplo, se não aniquila o *nemo tenetur* atingindo o seu conteúdo essencial e, por fim, se respeita os requisitos formais (n.os 2 e 3 do artigo 18.º da CRP). Começaremos pela análise do primeiro requisito, onde indagaremos sobre a existência de um comando legal que obrigue o arguido à desencriptação de smartphones através da revelação da palavra-passe.

Até 2009 não havia nenhuma solução legislativa acerca da questão concreta acima colocada. No entanto, como foi referido no Capítulo II da presente investigação, em 2009 foi aprovada a Lei do Cibercrime, o que nos leva a perguntar se perante esta lei se passou a consagrar a possibilidade – alargada – de as autoridades judiciárias exigirem do arguido o fornecimento da palavra-passe do seu smartphone.

Um dos meios de obtenção de prova previstos na Lei do Cibercrime é a injunção para apresentação ou concessão do acesso a dados, prevista no artigo 14.º, analisado *supra*. Esta norma consagra que as autoridades judiciárias podem ordenar, a quem tenha a disponibilidade ou o controlo de dados informáticos específicos e que se encontrem armazenados num determinado sistema informático (*v.g.* smartphone), que os comunique ao processo ou que permita o acesso aos mesmos. Prevê ainda este artigo que quem não actuar segundo as imposições previstas pode ser punido pelo crime de desobediência, previsto pelo artigo 348.º do Código Penal.

Ora, impõe-se saber se esta medida pode ter por alvo o arguido, já que isso implicaria uma clara opção do legislador em restringir o princípio contra a autoincriminação em detrimento da eficácia da investigação criminal. E, como atestámos em sede de acesso ao conteúdo dos smartphones, a resposta é negativa: o legislador ponderou bem os interesses e direitos aqui em conflito, tomando a opção clara de salvaguardar o direito à não-autoincriminação, ao consagrar no n.º 5 do artigo 14.º, que a injunção para apresentação ou concessão do acesso a dados não pode ser dirigida a suspeitos ou a arguidos no processo em que for determinada a própria medida[462]. Desta forma, fica vedada às autoridades judiciárias – através do mecanismo do artigo 14.º da Lei do Cibercrime - a possibilidade de compelirem o arguido a revelar a palavra-passe do seu dispositivo electrónico.

Entendem-se e aplaudem-se as excepções formuladas, sendo que, no que particularmente respeita à protecção do arguido, parece ser esta a única forma de não impor uma colaboração deste na recolha de prova da sua eventual incriminação.

Ademais, a já mencionada alínea d) do n.º 1 do artigo 61.º do Código de Processo Penal, referente aos direitos e deveres processuais do arguido, consagra o direito ao silêncio deste sujeito processual, enfatizando assim a possibilidade de o arguido manter em segredo a palavra-passe que permite o acesso ao seu dispositivo electrónico.

Desta forma, podemos concluir que, na legislação nacional, parece não constar uma norma que permita às autoridades judiciárias compelir o arguido a revelar a palavra-passe.

Contrariamente ao que acontece no ordenamento jurídico português, no Reino Unido, a criminalização da recusa em fornecer a palavra-passe encontra-se prevista, e é punida, pelo artigo 53.º da *Regulation of Investigatory Powers Act 2000* (RIPA)[463], sendo que a

[462] Neves/Correia, 2014: 147-148. Também na Holanda, o Código de Processo Penal prevê, na secção 2 do seu artigo 125K que "*an order can be given to provide access of a secured computer and/or to decrypt relevant data*". Esta ordem pode ser dada a qualquer pessoa que tenha acesso à informação necessária para desencriptar o dispositivo, à excepção do suspeito e arguido. Cf. Vordoglou, 2016: 17. Disponível em: https://repository.ihu.edu.gr/xmlui/bitstream/handle/11544/14539/Dissertation-Final-1104130034-Vordoglou.pdf?sequence=1 [consultado em 10.02.2017]. Koops, 2010: 607.

[463] Dispõe o artigo 53.º da RIPA, sob a epígrafe de "*Failure to comply with a notice"*: *"(1) A person to whom a section 49 notice has been given is guilty of an offence if he knowingly fails, in accordance with the notice, to make the disclosure required by virtue of the giving of the notice. (2) In proceedings against any person for an offence under this section, if it is shown that that person was in possession of a key to any protected information at any time before the time of the giving of the section 49 notice, that person shall be taken for the purposes of those proceedings to have continued to be in possession of that key at all subsequent times, unless it is shown that the key was not in his possession after the giving of the notice and before the time by which he was required to disclose it. […] (5) A person guilty of an offence under this section shall be liable - (a) on conviction on indictment, to imprisonment for a term not exceeding* ***[****the*

notificação para ceder qualquer palavra-passe é consagrada no artigo 49.º da referida legislação[464]. Assim, se após a notificação para fornecer uma palavra-passe o arguido optar por não o fazer, a punição aplicável corresponde a uma pena de prisão compreendida entre 2 a 5 anos[465]. Atendendo ao caso concreto, a eventual recusa do arguido em cumprir a ordem de desencriptação do smartphone que lhe é dirigida pela autoridade competente será livremente apreciada pelo tribunal[466]. Por outro lado, se o arguido actuar em conformidade com a ordem de desencriptação, também os dados descodificados serão, de uma perspectiva probatória, livremente ponderados e tomados em consideração na decisão a proferir[467].

Já no ordenamento jurídico belga, a criminalização da recusa em revelar palavras-passe pode desencadear a aplicação de uma pena de prisão compreendida entre os 6 a 12 meses ou, ainda, uma pena de multa. De facto, o juiz pode ordenar que o arguido revele a palavra-passe do seu smartphone quando considere que a mesma é essencial para a descoberta da verdade material[468].

---

*appropriate maximum term**]** or to a fine, or to both; (b) on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum, or to both. (5A) In subsection (5) 'the appropriate maximum term' means - (a) in a national security case **[**or a child indecency case**]**, five years; and (b) in any other case, two years. (5B) In subsection (5A) 'a national security case' means a case in which the grounds specified in the notice to which the offence relates as the grounds for imposing a disclosure requirement were or included a belief that the imposition of the requirement was necessary in the interests of national security] […]".*

[464] Dispõe o artigo 49.º do RIPA sob a epígrafe de "*Nothing requiring disclosure": "(1) This section applies where any protected information: (a) has come into the possession of any person by means of the exercise of a statutory power to seize, detain, inspect, search or otherwise to interfere with documents or other property, or is likely to do so; […] (2) If any person with the appropriate permission under Schedule 2 believes, on reasonable grounds— (a) that a key to the protected information is in the possession of any person, (b) that the imposition of a disclosure requirement in respect of the protected information is— […] (ii) necessary for the purpose of securing the effective exercise or proper performance by any public authority of any statutory power or statutory duty. […] the person with that permission may, by notice to the person whom he believes to have possession of the key, impose a disclosure requirement in respect of the protected information. (3) A disclosure requirement in respect of any protected information is necessary on grounds falling within this subsection if it is necessary— (a) in the interests of national security; (b) for the purpose of preventing or detecting crime; or (c) in the interests of the economic well-being of the United Kingdom […]".*

[465] Atwood, 2015: 431.

[466] Palfreyman, 2009: 362-370. Lowman, 2010: 3-4. Disponível em: https://www.lowmanio.co.uk/share/The%20Effect%20of%20File%20and%20Disk%20Encryption%20on%20Computer%20Forensics.pdf [consultado em 10.02.2017].

[467] Andrade, 2014: 33.

[468] Dispõe o artigo 88.º do Código Processual Penal belga (Code D'Instruction Criminelle): "*§ 1er. Lorsque le juge d'instruction ordonne une recherche dans un système informatique ou une partie de celuici, cette recherche peut être étendue vers un système informatique ou une partie de celui-ci qui se trouve dans un autre lieu que celui où la recherche est effectuée: - si cette extension est nécessaire pour la manifestation de la vérité à l'égard de l'infraction qui fait l'objet de la recherche, et - si d'autres mesures seraient disproportionnées, ou s'il existe un risque que, sans cette extension, des éléments de preuve soient perdus. § 2. L'extension de la recherche dans un système informatique ne peut pas excéder les systèmes informatiques ou les parties de tels systèmes auxquels les personnes autorisées à utiliser le système*

Se até ao ano de 2000 nenhum país tinha legislado a criminalização, ou mesmo a simples obrigação de fornecer uma palavra-passe quando tal lhe fosse ordenado, desde esse ano temos assistido ao movimento segundo o qual vários ordenamentos jurídicos introduziram normas atinentes à desencriptação de dados[469].

Ora, atendendo ao facto de que, na legislação nacional, não podemos encontrar nenhum comando legal que regule esta matéria, o julgador, aplicando directamente os preceitos constitucionais, devidamente interpretados e concretizados, terá de concluir que é ilegítima, e violadora do princípio *nemo tenetur se ipsum accusare*, qualquer ordem de desencriptação de smartphones através da revelação da palavra-passe diriga ao arguido pelas autoridades judiciárias[470].

De facto, estamos com Vânia Costa Ramos, quando centra a discussão na existência ou inexistência de uma obrigação imposta por lei e na específica relação que se impõe entre o Estado e a pessoa. Segundo a Autora, se sobre o cidadão impende um dever específico de submissão ao controlo das autoridades (*v.g.* exames de alcoolemia, substâncias

informatique qui fait l'objet de la mesure ont spécifiquement accès. § 3. En ce qui concerne les données recueillies par l'extension de la recherche dans un système informatique, qui sont utiles pour les mêmes finalités que celles prévues pour la saisie, les règles prévues à l'article 39bis s'appliquent. Le juge d'instruction informe le responsable du système informatique, sauf si son identité ou son adresse ne peuvent être raisonnablement retrouvées. Lorsqu'il s'avère que ces données ne se trouvent pas sur le territoire du Royaume, elles peuvent seulement être copiées. Dans ce cas, le juge d'instruction, par l'intermédiaire du ministère public, communique sans délai cette information au ministère de la Justice, qui en informe les autorités compétentes de l'état concerné, si celui-ci peut raisonnablement être déterminé. § 4. L'article 89bis est applicable à l'extension de la recherche dans un système informatique". Por seu turno, o art.º *88quater* dispõe o seguinte*: "§ 1er. Le juge d'instruction ou un officier de police judiciaire auxiliaire du procureur du Roi délégué par lui, peut ordonner aux personnes dont il presume qu'elles ont une connaissance particulière du système informatique qui fait l'objet de la recherche ou des services qui permettent de protéger ou de crypter des données qui sont stockées, traitées ou transmises par un système informatique, de fournir des informations sur le fonctionnement de ce système et sur la manière d'y accéder ou d'accéder aux données qui sont stockées, traitées ou transmises par un tel système, dans une forme compréhensible. Le juge d'instruction mentionne les circonstances propres à l'affaire justifiant la mesure dans une ordonnance motivée qu'il transmet au procureur du Roi. § 2. Le juge d'instruction peut ordonner à toute personne appropriée de mettre en fonctionnement ellemême le système informatique ou, selon le cas, de rechercher, rendre accessibles, copier, rendre inaccessibles ou retirer les données pertinentes qui sont stockées, traitées ou transmises par ce système, dans la forme qu'il aura demandée. Ces personnes sont tenues d'y donner suite, dans la mesure de leurs moyens. L'ordonnance vises à l'alinéa 1er, ne peut être prise à l'égard de l'inculpé et à l'égard des personnes visées à l'article 156. § 3. Celui qui refuse de fournir la collaboration ordonnée aux §§ 1er et 2 ou qui fait obstacle à la recherche dans le système informatique, est puni d'un emprisonnement de six mois à un an et d'une amende de vingt-six francs à vingt mille francs ou d'une de ces peines seulement. § 4. Toute personne qui, du chef de sa fonction, a connaissance de la mesure ou y prête son concours, est tenue de garder le secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal. § 5. L'Etat est civilement responsable pour le dommage causé de façon non intentionnelle par les personnes requises à un système informatique ou aux données qui sont stockées, traitées ou transmises par un tel système".*

[469] Andrade, 2014: 35.

[470] Dias, 2005: 211. "[…] não havendo entre nós nenhuma norma habilitante, dificilmente se poderão superar os constrangimentos processuais penais decorrentes do princípio *nemo tenetur se ipsum accusare*. O arguido não pode ser forçado a contribuir para a sua própria condenação". Cf. Correia, 2014: 59.

psicotrópicas, ou exames de ADN), qualquer restrição do *nemo tenetur* é válida; se, pelo contrário, impender unicamente um dever genérico, não será possível obrigar o arguido a colaborar. Em suma, "as restrições ao *nemo tenetur* situam-se num campo de verificação do cumprimento de obrigações impostas por lei"[471].

Assim sendo, cremos que do enquadramento legal português decorre que a colaboração do arguido é a excepção (e não a regra), só havendo colaboração exigível ao arguido na medida em que haja uma lei formal nesse sentido (que excepcione concretamente o princípio *nemo tenetur se ipsum accusare*)[472].

Apesar da falta de uma lei formal que regule a desencriptação de smartphones através da revelação da palavra-passe por parte do arguido, analisaremos, ainda que sumariamente e, sob pena de tratarmos a questão em maior detalhe mais à frente na nossa investigação, os restantes requisitos.

Desta feita, se o primeiro requisito das restrições a direitos fundamentais fosse validamente preenchido através da consagração de uma lei formal que previsse a obrigação de o arguido revelar a palavra-passe do seu smartphone, o segundo requisito – a necessidade de a restrição ao *nemo tenetur* ter como objectivo a salvaguarda de um outro direito ou interesse constitucionalmente protegido – não parece levantar dúvidas de maior. Na circunstância de as autoridades judiciárias forçarem o arguido a desencriptar o seu smartphone através da revelação da sua palavra-passe para, desta forma, obterem o acesso ao seu conteúdo, salta à vista que interesse as primeiras pretendem alcançar: a realização da justiça e a busca pela verdade material. Tal interesse é claramente protegido dentro da unidade da Constituição, impedindo, assim, um sacrifício arbitrário, gratuito e desmotivado do princípio *nemo tenetur se ipsum accusare*.

No que concerne à questão de saber se as ordens de desencriptação de smartphones dirigidas aos arguidos através da revelação da palavra-passe enunciadas no Capítulo I respeitam o princípio da proporcionalidade em sentido amplo, posicionamo-nos a favor da sua clara desproporcionalidade, em violação do princípio *nemo tenetur se ipsum accusare*. Sem embargo, sob pena de nos adiantármos nesta matéria, remetemos para a análise deste princípio em sede de desencriptação de smartphones através da leitura da impressão digital do arguido.

[471] Ramos, 2007: 90.
[472] Pinto, 2013: 111.

Queda-nos ainda referir que, pela nossa parte, qualquer ordem de desencriptação de smartphones através da revelação da palavra-passe dirigida ao arguido não respeita o quarto e último requisito material das restrições a direitos fundamentais vertido no n.º 3 do artigo 18.º da Constituição da República Portuguesa – a garantia do conteúdo essencial do direito restringido. Como mencionado anteriormente, este requisito consagra a ideia de que existe um núcleo essencial dos direitos fundamentais que não pode, em caso algum, ser violado. Sendo o último requisito material das restrições a direitos, liberdades e garantias, este pressuposto funciona como uma barreira final e efectiva contra o abuso do poder. De acordo com uma teoria mista, por nós defendida, este núcleo essencial do *nemo tenetur* terá de articular-se com a necessidade de protecção do interesse pela persecução da justiça e pela busca da verdade material, sendo que não poderá ser alvo de uma qualquer aniquilação.

Nesta linha de raciocínio, estamos com Catarina Anastácio, quando defende que o núcleo essencial deste princípio é aniquilado nas situações em que alguém é "coagido a emitir declarações autoincriminatórias, a declarar a sua culpabilidade, a admitir a sua participação numa infracção, uma vez que tal admissão, a verificar-se, deverá ser sempre um acto totalmente livre e consciente"[473]. Por conseguinte, atendendo ao facto de que o arguido, ao acatar uma qualquer ordem de desencriptação do seu smartphone através da revelação da sua palavra-passe, estará a emitir declarações autoincriminatórias, outra não poderá ser a conclusão senão a de que esta medida é claramente violadora do requisito da garantia do núcleo essencial do direito fundamental restringido, consagrado na parte final do n.º 3 do artigo 18.º da Lei Fundamental.

Perante um caso de conflito entre dois direitos fundamentais, e depois de valoradas todas as circunstâncias do caso concreto, dever-se-á concluir pela prevalência de um direito sobre o outro. No entanto, o sacrifício deste último em caso algum poderá jusitificar a aniquilação do conteúdo essencial de qualquer um dos direitos.

Por fim, quanto aos requisitos formais das restrições a direitos fundamentais – generalidade, abstracção e não retroactividade -, atendendo ao facto de que a ordem de desencriptação de smartphones através da revelação de palavra-passe dirigida ao arguido não tem consagração em lei formal deixa de ser pertinente a análise destes critérios.

[473] Anastácio, 2010: 217.

Em jeito de conclusão, contra a revelação coactiva da palavra-passe poder-se-á alegar o seguinte: a) não está prevista na lei qualquer obrigatoriedade de fornecimento da palavra-passe por parte do arguido; b) o acesso ao smartphone encriptado é possível através de tentativas de adivinhar a palavra-passe, uma vez que muitos utilizadores optam por palavras-passe fáceis de decifrar; c) o arguido tem direito ao silêncio de acordo com a alínea d) do n.º 1 do artigo 61.º do Código de Processo Penal; d) a palavra-passe pode ser considerada como incriminatória, uma vez que a demonstração do seu conhecimento prova, ainda que implicitamente[474], determinados factos, nomeadamente, que o arguido será responsável pelos conteúdos encriptados que estejam armazenados no smartphone, porquanto ele terá acesso e controlo sobre os mesmos[475]; e) a palavra-passe pode ser ainda incriminatória noutro sentido: será incriminatória, de modo indirecto, na medida em que faculta o acesso a dados incriminatórios[476], os quais, sem a colaboração do arguido, nunca seriam acedidos e nunca fundamentariam, por isso mesmo, a sua responsabilidade penal[477].

Depois de confirmada a violação, de acordo com ordenamento jurídico nacional, do princípio *nemo tenetur* nos casos em que as autoridades judiciárias dirigem ao arguido uma ordem de desencriptação do seu smartphone através da revelação da palavra-passe, resta-nos apenas aferir da legitimidade da desencriptação do smartphone através da leitura da impressão digital do arguido.

---

474 *"[…] the entry of the passphrase is testimonial because it implicity communicates facts, namely that the defendant knows the passphrase, has control over the smartphone files, and believes he can access the smartphone's contents"*. Cf. Pfefferkorn, 2009: 11. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1883697&download=yes [consultado em 13.02.2017].

475 *"[…] disclosing the passphrase […] implicity involves statements of fact by admitting that the evidence exists, is in the person's possession or control, and is authentic. By entering a passphrase, the person will implicity admit the fact that he or she knows the passphrase, it is within his or her control, and the passphrase is authentic in the sense that it is what the person believes the government wants. In this case, the act of disclosing a passphrase will lead to the inference that the contents decrypted were created and in the control of that person, which may be highly incriminating […]*". Cf. Duong, 2009: 349. *"When a defendant is compelled to enter a password into his smartphone, the act of decryption necessarily implies statements of fact that could prove to be incriminatory"*. Cf. Winkler, 2014: 46.

476 "O princípio contra a autoincriminação abrange acções verbais ou físicas capazes de contribuir para a própria condenação e, encurtando razões, o arguido não pode ser condicionado a contribuir para a sua incriminação através da prestação de qualquer tipo de declarações, nomeadamente, […] fornecendo um código […]". Cf. Haddad, 2003: 20-21.

477 Pinto, 2013: 112-115.

5.2. Desencriptação de smartphones através da leitura da impressão digital do arguido

Para aferir da legitimidade da desencriptação de smartphones para a obtenção de prova em processo penal através da leitura da impressão digital do arguido, com base nos casos norte-americanos anteriormente apresentados, cumpre, à semelhança do que foi feito em sede de desencriptação através da revelação da palavra-passe, aferir se estas ordens estão previstas em lei formal, se têm como objectivo a salvaguarda de outro direito ou interesse constitucionalmente protegido, se obedecem ao princípio da proporcionalidade em sentido amplo, se não aniquilam o *nemo tenetur* atingindo o seu conteúdo essencial e, por fim, se respeitam os requisitos formais (n.os 2 e 3 do artigo 18.º da CRP). Começaremos pelo primeiro requisito.

Quanto à questão da exigência de lei formal, vale o que ficou dito no ponto anterior. Assim, a legitimidade da restrição ao princípio *nemo tenetur se ipsum accusare* está dependente da sua consagração na legislação nacional (bastando que seja admitida dentro da unidade da Constituição).

Queda-nos, então, apurar sobre a existência de uma norma que obrigue o arguido a colocar o seu dedo no sensor do smartphone para que a leitura da sua impressão digital possibilite o acesso das autoridades judiciárias ao conteúdo do seu dispositivo.

Como ficou assente no Capítulo II da nossa investigação, o acto de colocar o dedo no sensor do smartphone para permitir a leitura da impressão digital do arguido não pode ser considerado nem uma perícia, nem um exame, mas sim uma outra diligência de prova.

A alínea d) do n.º 3 do artigo 61.º do Código de Processo Penal regula que, sobre o arguido, recaem, em especial, os deveres de "sujeitar-se a diligências de prova e a medidas de coacção e garantia patrimonial especificadas na lei e ordenadas e efectuadas por entidade competente". De facto, como realçámos anteriormente, não obstante a inexistência de um dever de o arguido colaborar com as autoridades, tal não significa que não possa haver derrogações ao princípio *nemo tenetur*[478]. Neste caso concreto de desencriptação de smartphones através da leitura da impressão digital, o arguido acaba

[478] Marques da Silva, 2010: 318.

por constituir um meio de prova em sentido formal, na medida em que o seu corpo e o seu estado corporal podem ser objecto de diligências de prova[479].

No que à jurisprudência diz respeito, o Supremo Tribunal de Justiça, no seu acórdão n.º 14/2014, veio realçar o disposto na alínea d) do n.º 3 do artigo 61.º do CPP, afirmando que "o estatuto processual do arguido não é incompatível com a sujeição a diligências de prova ou meios de as obter, posto que esses deveres não afectem direitos fundamentais processuais, integrantes do seu direito de defesa"[480].

Poderíamos assim concluir que, de acordo com o entendimento da doutrina citada e da jurisprudência do Supremo Tribunal de Justiça, a desencriptação de smartphones através da leitura da impressão digital do arguido teria consagração na alínea d) do n.º 3 do artigo 61.º do Código de Processo Penal, podendo o arguido ser legitimamente compelido a tal.

Efectivamente, o arguido tem o dever de se sujeitar a diligências de prova, devendo, no entanto, entender-se que este dever não abrange todo e qualquer tipo de prova (artigo 125.º do CPP), mas apenas as diligências de prova que estejam "especificadas na lei", sendo que a desencriptação de smartphones através da leitura da impressão digital não se mostra, como tal, normativamente especificada. Se todos os casos de recusa de submissão a diligências de prova devessem merecer a censura típica do crime de desobediência, o legislador tê-lo-ia previsto expressamente naquele segmento normativo (al. d) do n.º 3 do artigo 61.º), bastando para tanto acrescentar à sua respectiva previsão a expressão: "sob cominação de incorrer no crime de desobediência em caso de recusa ou não cumprimento"[481]. Deve ainda ter-se em conta que, na esteira do defendido por Germano Marques da Silva, não obstante o dever de sujeição a diligências de prova, o arguido não tem a obrigação de fornecer provas que o incriminem[482].

O Código de Processo Penal actualmente em vigor desde 1987 (e com as alterações entretanto introduzidas), consagrou expressamente o direito ao silêncio do arguido, mas não consagrou expressamente a possibilidade de desencriptação de smartphones através da leitura da sua impressão digital. Pelo contrário, a Lei do Cibercrime, de 15 de Setembro de 2009, veio estabelecer no n.º 5 do seu artigo 14.º, que o suspeito e o arguido não podem

[479] Figueiredo Dias, 2004: 438-439.
[480] Acórdão do Supremo Tribunal de Justiça n.º 14/2014, de 21 de Outubro de 2014, disponível em: https://dre.pt/application/file/58512485 [consultado em 15.02.2017].
[481] Acórdão do Supremo Tribunal de Justiça n.º 14/2014, de 21 de Outubro de 2014, disponível em: https://dre.pt/application/file/58512485 [consultado em 15.02.2017].
[482] Marques da Silva, 2013: 76.

ser compelidos pelas autoridades judiciárias a permitir o acesso ao conteúdo do seu dispositivo electrónico.

Assim, estamos com Helena Moniz, quando defende no seu voto de vencida ao Acórdão do Supremo Tribunal de Justiça n.º 14/2014, que "a submissão do arguido a diligências de prova, nos termos da al. d) do n.º 3 do artigo 61.º do CPP, apenas se impõe quando estejam "especificadas na lei", sem o que não pode aquela restrição às garantias do arguido ser-lhe imposta quando o arguido é utilizado como meio de prova contra si próprio […]"[483].

Como deixámos claro no ponto anterior, também Vania Costa Ramos parece seguir este entendimento, com o qual concordamos inteiramente. Segundo a Autora, se sobre o arguido impende unicamente um dever genérico (*v.g.* dever de sujeição a diligências de prova – al. d) do n.º 3 do artigo 61.º do CPP), não será possível obrigar o arguido a colaborar[484]. Para que se possa aqui falar de uma obrigação de colaboração por parte do arguido, é necessário que se esteja perante um dever específico de submissão ao controlo das autoridades[485], como é o caso, a título de exemplo, dos exames de alcoolemia e substâncias psicotrópicas (artigos 152.º e 153.º do Código da Estrada) e exames de ADN para fins de investigação criminal (n.º 1 do artigo 8.º da Lei n.º 5/2008, de 12 de Fevereiro, e artigo 172.º do CPP). Igualmente, Vieira de Andrade vem defender a ideia de que uma qualquer restrição ao princípio da não-autoincriminação, em função da exigência de lei formal, deve "[…] apresentar uma densidade suficiente, isto é, um certo grau de determinação do seu conteúdo, pelo menos no essencial, não sendo legítimo que se deixe à Administração espaços significativos de regulação ou de decisão […]"[486].

---

[483] Voto de Vencida de Helena Moniz ao Acórdão do Supremo Tribunal de Justiça n.º 14/2014, de 21 de Outubro de 2014, disponível em: https://dre.pt/application/file/58512485 [consultado em 15.02.2017]. Em sentido contrário, o Supremo Tribunal de Justiça, no referido acórdão, veio defender o entendimento de que uma leitura e interpretação restritiva da alínea d) do n.º 3 do artigo 61.º do Código de Processo Penal, no sentido de que as deligências de prova necessitariam de estar "especificadas na lei", constituiria um golpe profundo na investigação criminal, posto que salvaguardaria o arguido das diligências de prova, meios de prova ou de obtenção de prova. Cf. Acórdão do Supremo Tribunal de Justiça n.º 14/2014, de 21 de Outubro de 2014, disponível em: https://dre.pt/application/file/58512485 [consultado em 15.02.2017].

[484] Ramos, 2007: 90.

[485] Neste sentido vai também Catarina Andrade, ao afimar, em sede de desencriptação de dispositivos electrónicos, que não se pode defender a ideia de que o arguido é obrigado a cooperar com as autoridades ao abrigo de um dever genérico de colaboração. "Pese embora a importância da descoberta da verdade material, não pode o legislador permitir que a mesma opere como derrogação absoluta dos princípios constitucionalmente consagrados e desenvolvidos em sede processual penal. Como tal, […] não podemos considerar que a questão controvertida se encontra resolvida através da aplicação de um dever geral de colaboração do arguido, porquanto o mesmo não é aceite pelo ordenamento jurídico português". Cf. Andrade, 2014: 29.

[486] Vieira de Andrade, 2016: 290-291.

Assim, a sujeição do arguido a colocar o dedo no sensor do smartphone para permitir o acesso ao dispositivo, contra a sua vontade, enquanto limitação ao princípio *nemo tenetur se ipsum accusare*, só deverá ser possível após a consagração legal desse dever específico. Considerando-se que aquela limitação não está legalmente prevista, não podemos entender que possa ser ordenada pelas autoridades judiciárias. De facto, ainda que não exista legislação que preveja uma obrigação de o arguido desencriptar o seu smartphone através da leitura da impressão digital, suprir esta omissão legislativa através da subversão do regime processual penal consagrado não pode configurar-se como admissível. O simples facto de determinada matéria não se achar prevista e regulada na lei não indicia, de *per si*, a existência de uma lacuna legal que careça de ser integrada, nos termos do disposto no artigo 10.º do Código Civil. Na expressão impressiva de Oliveira Ascensão, "lacuna não é tudo o que não está na lei"[487].

E, mesmo que o julgador interprete a norma constante da alínea d) do n.º 3 do artigo 61.º como uma obrigação de o arguido desencriptar o dispositivo através da leitura da sua impressão digital, resta saber se esta ordem respeita os restantes limites aos limites dos direitos fundamentais consagrados nos n.os 2 e 3 do artigo 18.º da Lei Fundamental.

Analisado que está o primeiro requisito da exigência de lei formal, passaremos à verificação do segundo requisito – necessidade de salvaguarda de outro direito ou interesse constitucionalmente protegido.

À semelhança do que ficou dito no ponto anterior, também no caso concreto de uma ordem de desencriptação de smartphones através da leitura da impressão digital dirigida ao arguido pelas autoridades judiciárias, não existem dúvidas quanto ao interesse das últimas: a persecução da justiça e a descoberta da verdade material. Interesse esse que, como já enfatizámos anteriormente, é claramente protegido dentro da unidade da Constituição, impedindo assim um sacrifício arbitrário, gratuito e desmotivado do princípio *nemo tenetur se ipsum accusare*.

Passando à averiguação do terceiro limite aos limites dos direitos fundamentais, cumpre salientar que a ordem de desencriptação de smartphones, agora através da leitura da impressão digital do arguido, não pode dispensar o escrutínio do princípio da proporcionalidade em sentido amplo ou, para alguns, princípio da proibição do excesso. Por esse motivo, analisaremos, de seguida, se, nos casos norte-americanos, tendo agora

[487] Ascensão, 1997: 918.

por base a legislação nacional, os corolários da adequação, necessidade e proporcionalidade em sentido estrito estão ou não preenchidos.

O subprincípio da adequação, como vimos anteriormente, exige que a ordem restritiva em causa seja apta a realizar o fim visado com a restrição ou contribua para o alcançar. Ora, a ordem restritiva nos casos norte-americanos apresentados é precisamente a ordem dada ao arguido, pelas autoridades judiciárias, no sentido de desencriptar o seu smarpthone através da leitura da sua impressão digital. Já o fim visado com essa restrição prende-se com a realização da justiça e a busca pela verdade material.

Sabendo, de antemão, que este corolário não é devidamente cumprido sempre que a ordem restritiva se revele inapta para atingir esse fim, ou seja, sempre que os efeitos dessa medida se revelarem indiferentes ou contrários à realização do fim em vista, cumpre perceber quais são os potenciais efeitos que aquelas ordens de desencriptação de smartphones através da leitura da impressão digital do arguido podem causar.

A ordem de desencriptação do smartphone, seja através de que método for, é sempre emitida com o propósito de aceder ao conteúdo do dispositivo. Assim, as autoridades judiciárias, numa tentativa de proceder à apreensão de provas incriminatórias que possam estar armazenadas no smartphone, solicitam a colaboração do arguido.

Ora, *a priori*, as autoridades judiciárias não têm, na maioria das vezes (ou, até mesmo, na totalidade), conhecimentos bastantes para garantir que no smartphone estarão armazenadas provas de determinado delito. Por esse motivo, depois de conseguirem aceder ao dispositivo, através da leitura da impressão digital do arguido, estas entidades podem encontrar provas suficientes para relacionar o arguido ao crime em questão ou, pelo contrário, podem encontrar apenas informações, ficheiros e dados pessoais do arguido que em nada o relacionem com o delito. E, neste último caso, se o smartphone não contiver qualquer informação pertinente para a investigação do crime, parece-nos óbvio que o fim visado – a persecução da justiça e a busca pela verdade material – fica claramente comprometido. No entanto, ficou esclarecido anteriormente que este subprincípio da adequação exige que a medida restritiva seja considerada apta a realizar o fim visado com a restrição ou contribua para o alcançar, mas através de um juízo de prognose. Ou seja, só poderemos falar aqui numa inconstitucionalidade desta ordem de desencriptação se, tendo em conta os conhecimentos empíricos e científicos disponíveis

no momento da aprovação da medida, esta se revele inapta a contribuir para a persecução da justiça e descoberta da verdade material.

Assim, podemos concluir que os efeitos desta medida restritiva ao princípio *nemo tenetur* – desencriptação do smartphone através da leitura da impressão digital do arguido – revelam-se, desta forma, aptos à realização da justiça e descoberta da verdade, desde que, à data da aprovação da medida, e de acordo com os conhecimentos das autoridades judiciárias, haja a possibilidade (ainda que reduzida) de o dispositivo conter provas autoincriminatórias.

Desta feita, outra não poderá ser a conclusão se não a de que todas as ordens de desencriptação apresentadas no Capítulo I (no caso Baust, Diamond e Paytsar – no caso do mandado de 9 de Maio de 2016 não temos informações suficientes quanto à finalidade da medida) respeitaram o subprincípio da adequação, uma vez que à data da sua aprovação, e de acordo com os conhecimentos empíricos disponíveis na altura, havia, em todos os casos, a possibilidade de os dispositivos electrónicos armazenarem provas incriminatórias (relativas à ofensa à integridade física, ao furto e ao roubo de identidade, respectivamente).

De facto, casos em que uma medida retritiva de um direito fundamental é declarada inconstitucional devido à sua inadequação são raros. Normalmente, os meios restritivos adoptados atingem o seu objectivo até certo grau. Isto é suficiente para superar o teste da adequação[488].

Completamente diferente é o que se passa com o segundo subprincípio da proporcionalidade em sentido amplo, ou seja, a necessidade. Este subprincípio exige que se recorra, para atingir determinado fim, ao meio necessário, exigível ou indispensável, no sentido do meio mais suave ou menos restritivo que precise de ser utilizado para atingir o fim em vista. Para tal, é necessário que se faça a comparação entre os prejuízos provocados pela desencriptação compelida e os prejuízos que seriam provocados pela utilização de um meio alternativo.

Como foi oportunamente referido, o smartphone tem, actualmente, capacidade para armazenar uma vasta quantidade de informação, nomeadamente: agenda de contactos; informação de calendário; mensagens escritas; registo de chamadas feitas e recebidas; e-

[488] Alexy, 2014: 820.

mail; fotografias; gravações áudio e vídeo; mensagens de multimédia; mensagens instantâneas; histórico de navegação na internet; documentos electrónicos; dados relacionados com as redes sociais; dados relacionados com aplicações; informação sobre localizações geográficas, entre outras. Por esse motivo, compreende-se que o acesso a este dispositivo acarreta, simultaneamente, o acesso a informação protegida pelo direito à reserva sobre a intimidade da vida privada.

Com a desencriptação do smartphone através da leitura da impressão digital do arguido, as autoridades judiciárias passam a ter domínio sobre vários ficheiros electrónicos de carácter pessoal e íntimo. Assim, estamos aqui claramente perante não só uma grave violação do princípio contra a autoincriminação, como também uma grave violação do direito do arguido à reserva da intimidade da vida privada[489], um direito fundamental consagrado no texto constitucional, no n.º 1 do artigo 26.º. Posto isto, queda-nos perceber se estes prejuízos causados pela desencriptação são superiores aos prejuízos que poderiam ser provocados por um meio de obtenção de prova alternativo.

Acreditamos, independentemente do crime perpretado (*v.g.* crime de ofensa à integridade física, furto, roubo de identidade), que outros meios de prova e meios de obtenção de prova poderiam ser menos lesivos do que a desencriptação.

Mesmo que as autoridades judiciárias tivessem a convicção plena de que no smartphone estariam armazenadas provas que relacionavam o arguido com o crime em questão, outros meios alternativos como os exames, as perícias, as revistas e buscas ou as apreensões, seriam menos lesivos, tanto em relação ao princípio *nemo tenetur*, quanto ao direito à reserva sobre a intimidade da vida privada, do que a desencriptação compelida do dispositivo. Tendo em consideração o caso de David Baust, apresentado no Capítulo I da presente investigação, vários podiam ser os meios de prova utilizados para provar a ofensa à integridade física da vítima de uma forma menos lesiva para os direitos fundamentais do arguido do que a ordem de desencriptação do smartphone (independentemente do método utilizado). Nomeadamente, uma perícia médico-legal, um exame realizado ao local do crime ou uma busca. No caso de Matthew Diamond, o arguido, suspeito de furto, foi ordenado a desencriptar o seu smartphone através da leitura da sua impressão digital,

[489] Como deixámos claro anteriormente, a desnecessidade da agressão afere-se em relação aos prejuízos provocados pela medida restritiva, avaliados em função de critérios materiais, espaciais, temporais ou pessoais e tendo em conta, não apenas o direito fundamental directamente atingido, como qualquer outra afectação desvantajosa da liberdade, dos direitos fundamentais ou de outros interesses juridicamente relevantes do mesmo titular ou de outros afectados.

no entanto, acreditamos que a recolha de imagens de vídeo-vigilância que comprovariam o seu envolvimento na venda das peças furtadas, uma busca à sua residência e a comparação das pegadas encontradas no local com os seus sapatos, seriam medidas muito menos lesivas do seu privilégio contra a autoincriminação e do seu direito à reserva da intimidade da vida privada. Quanto ao caso Paytsar, acreditamos que, também aqui, uma busca à sua residência seria um meio de obtenção de prova menos lesivo e até mais eficaz para a investigação do crime de roubo de identidade do que a ordem de desencriptação. Por fim, no caso do mandado de 9 de Maio de 2016, apesar de não termos conhecimento sobre os motivos que levaram à elaboração do mandado, acreditamos que a ordem de desencriptação é desnecessária e extremamente lesiva das garantias de defesa dos proprietários dos smartphones, em comparação com a mera busca ao local e revista dos sujeitos aí presentes.

Nestes quatro casos em análise, mesmo que se venha a alegar uma diferente intensidade na prossecução do fim optando por estes meios menos lesivos, acreditamos que a persecução da justiça e a descoberta da verdade material não ficariam, de modo algum, prejudicadas, até porque os meios apresentados conduziriam ao mesmo fim a que a desencriptação do smartphone possivelmente levaria e, segundo nossa opinião, com uma maior eficácia.

Deste modo, defendemos a ideia de que o subprincípio da necessidade não se encontra devidamente preenchido nos casos apresentados, relativos a ordens de desencriptação de smartphones através da leitura da impressão digital do arguido.

Por fim, no que concerne ao corolário da proporcionalidade em sentido estrito, que visa apurar o equilíbrio na relação entre a importância do fim visado – realização da justiça e busca pela verdade material – e a gravidade do sacrifício imposto – violação do princípio *nemo tenetur* (e, simultaneamente, do direito à reserva sobre a vida privada) -, cumpre comparar os prejuízos impostos aos direitos fundamentais, contrapostos aos benefícios produzidos na obtenção do fim visado com a restrição.

Este subprincípio da proporcionalidade em sentido estrito corresponde, como vimos, à máxima designada como "Lei da Ponderação", criada por Alexy. Esta máxima defende

que "quanto maior for o grau de não realização ou de afectação de um princípio, maior deve ser a importância da realização do princípio colidente"[490].

Sandra Oliveira e Silva vem defender que a aplicação da lei da ponderação à resolução dos conflitos entre o *nemo tenetur* e o interesse da perseguição criminal se redunda numa verdadeira aporia metodológica. Isto porque, segundo a Autora, "os critérios legitimadores da restrição do *nemo tenetur* no interesse da eficácia da perseguição criminal (a saber: a gravidade do crime investigado, a indispensabilidade da prova, a fidedignidade da informação que se espera obter…) são precisamente os que tornam mais intensa a necessidade de tutela do arguido contra a autoincriminação (é mais grave a pena esperada, maior o efeito incriminatório da diligência a realizar, etc)[…]", pelo que nunca se poderá afirmar "[…] que a um grau mais elevado de afectação do direito sacrificado (a prerrogativa contra a autoincriminação) corresponde uma maior medida de realização do interesse contrário (os da investigação criminal)"[491]. Ou seja, se o interesse do Estado em obter provas autoincriminatórias cresce numa relação de proporcionalidade directa à pretensão individual do arguido em negar-lhas, nunca será possível atingir um ponto óptimo de equilíbrio que se espera da ponderação como critério de delimitação do âmbito concreto de operatividade de direitos fundamentais[492]. Pelo que, ainda do ponto de vista da citada Autora, o critério da ponderação torna-se, neste caso concreto, um critério frágil e subjectivo.

Contudo, a nossa posição vai, respeitosamente, em sentido contrário da tese defendida por Sandra Oliveira e Silva. De facto, segundo nossa opinião, para justificar uma afectação elevada do princípio *nemo tenetur* é necessário que a realização do princípio contrário, neste caso, a realização da justiça, se revele de maior importância. Contrariamente ao defendido por Sandra Oliveira e Silva, não cremos que o aumento do interesse do Estado em obter provas autoincriminatórias (dada a gravidade do crime investigado, a indispensabilidade da prova, a fidedignidade da informação que se espera obter, entre outros motivos) faça forçosamente aumentar a necessidade de protecção do arguido contra a autoincriminação (uma vez que a pena esperada é mais grave, o efeito incriminatório da diligência a realizar é maior, etc). Para defendermos este entendimento

[490] Alexy, 2014: 821.
[491] Oliveira Silva, 2015: 622.
[492] Oliveira Silva, 2015: 622.

apoiamo-nos num exemplo prático do nosso ordenamento jurídico: a sujeição do arguido ao teste de alcoolemia através de colheita de ar expirado.

Neste caso em concreto, o interesse do Estado em obter provas autoincriminatórias é bastante elevado, uma vez que a gravidade do crime (condução sob o efeito de álcool) é considerável, a prova (colheita de ar expirado) é indispensável para a acusação e a informação recolhida através da análise do ar expirado é fidedigna. Ainda assim, este aumento do interesse do Estado em obter provas autoincriminatórias não culmina na necessidade de uma maior protecção do arguido contra a autoincriminação, muito pelo contrário, dada a gravidade do crime e do risco criado para a comunidade, a restrição do *nemo tenetur* considera-se justificada através de um critério de ponderação.

Este caso acaba por demonstrar que, depois de valoradas todas as circunstâncias do caso através do método de ponderação de bens, só uma maior medida de realização da justiça e de busca pela verdade material (atendendo à gravidade do crime investigado, à indispensabilidade da prova, à fidedignidade da informação que se espera obter, entre outros motivos) justifica um grau mais elevado de afectação do privilégio contra a autoincriminação.

Por conseguinte, a aplicação da lei da ponderação à resolução dos conflitos entre o princípio *nemo tenetur se ipsum accusare* e o interesse da perseguição criminal, no sentido de estabelecer o valor prevalecente, é fundamental. E, afim de percebemos se as ordens de desencriptação de smartphones através da leitura da impressão digital do arguido, apresentadas anteriormente, respeitam esta lei da ponderação (quanto maior for o grau de não realização ou de afectação de um princípio, maior deve ser a importância da realização do princípio colidente), cumpre esclarecer várias questões[493].

Com a desencriptação do smartphone, seja através do método da revelação da palavra-passe ou da leitura da impressão digital do arguido, as autoridades judiciárias passam a ter acesso e controlo sobre todo o contéudo aí armazenado. Assim, como já tivemos oportunidade de mencionar, para além de estar aqui em causa uma violação ao princípio

[493] "*El principio de proporcionalidad es un concepto abstracto que alude a la relación entre el fin a alcanzar – prevención/represión del delito – y el medio empleado para ello – diligencia restrictiva de un derecho fundamental. Para ello se ponderan diversos elementos como: la gravedad del hecho delictivo; la intensidad de la sospecha o el tipo de indicios; las perspectivas de éxito de la medida; el esfuerzo en su realización en relación con el resultado a obtener; el perjuicio que se causa en relación con la utilidad del resultado. Tales elementos son critérios orientativos para valorar la contraposición entre el interés individual que puede verse afectado por la medida y el interés público que subyace en la investigación procesal penal, valoración que habrá de concretarse en cada caso*". Cf. Winter, 2010: 174.

contra a autoincriminação, poderão levantar-se, ainda, questões relativas à privacidade não só do arguido como também de terceiros que possam estar envolvidos nos ficheiros gravados electronicamente no dispositivo (quer através de comunicações encetadas entre o arguido e o terceiro, quer através de fotografias tiradas ao terceiro, etc.).

Atendendo a esta ingerência do público no universo privado, violentando direitos constitucionalmente atribuídos e protegidos, a desencriptação de smartphones (independentemente do método utilizado) deverá ser realizada a título excepcional e obedecendo a critérios mais exigentes[494]. Nomeadamente, acreditamos que, em virtude desta intervenção sobre direitos fundamentais do arguido e de terceiros, a ordem de desencriptação compelida de smartphones dirigida ao arguido só se justificará, em primeiro plano, mediante prévia autorização judicial e, apenas, se o crime sob investigação for de considerável gravidade. Sendo que esta gravidade deve ser avaliada no caso concreto (gravidade concreta do facto)[495]. Neste sentido, defendemos a ideia de que a legitimidade da desencriptação de smartphones depende (além da verificação de todos os limites aos limites) da consagração legal de um catálogo de crimes mais graves a que a medida deverá obedecer, à semelhança do que acontece em sede de escutas telefónicas[496].

Ademais, deve ter-se ainda em conta, em sede de análise da proporcionalidade em sentido estrito, que qualquer ordem de desencriptação de smartphone dirigida ao arguido culmina na obtenção de ficheiros electrónicos criados mesmo antes da suspeita do crime, pelo que, novamente, surgem questões relativas não só à autoincriminação do arguido (no sentido de que se poderão encontrar provas de outros crimes ainda não conhecidos pelas autoridades judiciárias) como também à reserva da intimidade da vida privada do arguido e de possíveis terceiros, que devem ser levadas em conta quando em confronto com o interesse na persecução da justiça.

É ainda de ressalvar que, tanto no caso Paytsar Bkhchadzhyan como no caso do mandado de 9 de Maio de 2016, as autoridades judiciárias parecem ter emitido ordens de desencriptação dos smartphones através da leitura das impressões digitais dos supostos proprietários com a intenção de realizarem autênticas "*fishing expeditions*" indiscriminadas em busca de qualquer tipo de prova autoincriminatória revelante sobre

[494] Santos, 2009: 108.
[495] Rogall, 2010: 125.
[496] Susano, 2009: 24. Jesus, 2015: 291. Rodrigues, 2009b: 215-216.

qualquer crime. Esta questão é claramente outro ponto a ter em atenção aquando da análise da proporcionalidade da medida, sendo que o recurso a estas *"fishing expeditions*" está completamente interdito às autoridades judiciárias.

Um outro ponto a chamar à colação no âmbito da análise da proporcionalidade (*stricto sensu*) destas ordens de desencriptação, prende-se com o facto de a impressão digital já não poder ser vista como o tradicional meio de identificação de sujeitos.

A impressão digital tem sido considerada, ao longo do tempo, como um meio de identificação, tal como uma fotografia. No entanto, à medida que a tecnologia avança, a impressão digital (assim como outros identificadores biométricos), deixa de ter esse propósito singular, passando a ser usada para guardar informação possivelmente mais privada do que a própria identidade do indivíduo[497]. Como bem salienta Alex Abdo, não estamos aqui perante a recolha de uma impressão digital para identificar um sujeito, mas sim perante uma impressão digital que é usada para proteger uma quantidade considerável de informação privada[498]. Assim, a impressão digital deve ser vista como algo privado e digno de protecção (tal como a palavra-passe), contrariamente a uma fotografia, que facilmente pode ser obtida pelo público.

É da nossa opinião que no caso de encriptação de smartphones por impressão digital, este dado biométrico funciona como uma substituição da tradicional palavra-passe alfanumérica ou, por outras palavras, como uma palavra-passe secundária. Prova disso é o facto de a impressão digital ficar registada no dispositivo apenas pela sua representação matemática, ou seja, por um longo número composto por 50 a 100 dígitos, designado de *biometric hash*.

Por fim, cabe ainda clarificar que a errónea interpretação da impressão digital como um mero meio de identificação conduz-nos ao problema da instrumentalização do corpo do arguido[499], que, compelido a colocar o dedo no sensor do seu dispositivo para permitir o acesso às entidades judiciárias, estará a usá-lo como meio de prova contra si próprio[500], incorrendo, desta forma, numa clara violação do princípio contra a autoincriminação.

---

[497] Goldman, 2015: 230.
[498] "*This is not law enforcement requesting a fingerprint to identifying someone, this is a fingerprint that is being used to open up a treasure trove of information"*. Cf. Spring, 2016: 2. Disponível em: https://threatpost.com/experts-outraged-by-warrant-demanding-fingerprints-to-unlock-smartphones/121348/ [consultado em 21.02.2017].
[499] Girotto, 2009: 455.
[500] Dias, 2005: 209.

Depois de sopesadas todas as questões assinaladas, cumpre deixar claro que todas as ordens de desencriptação apresentadas anteriormente (no caso Baust, Diamond e Paystar - no caso do mandado de 9 de Maio de 2016 não temos informações suficientes quanto à finalidade da medida) são adequadas a atingir o fim, na medida em que, segundo um juízo de prognose, o acesso aos smartphones permitiria (possivelmente) aceder a provas incriminatórias; não são necessárias, pressupondo que a entidade pública dispunha de medidas alternativas menos restritivas com idêntico grau (ou até mesmo superior) de eficácia na obtenção do mesmo fim; finalmente, face aos dados dos casos apresentados no Capítulo I, as ordens de desencriptação mostram-se como manifestamente desproporcionadas, por vários motivos: a) em alguns casos, foram usadas como autênticas "*fishing expeditions*" indiscriminadas; b) a gravidade de alguns crimes, a dispensabilidade da prova e a fidedignidade da mesma (não raras vezes as provas utilizadas são fotografias ou gravações de vídeo que facilmente são adulteradas) não justificavam uma lesão tão extensa do princípio *nemo tenetur*; c) dada a ingerência do público na esfera privada do arguido, não só estariam prejudicadas as suas garantias de defesa como também o respeito pela sua reserva da intimidade da vida privada e de terceiros. Pelo que, em resultado, as ordens de desencriptação apresentadas no Capítulo I – independentemente do método utilizado - seriam consideradas inconstitucionais.

Em jeito de conclusão da análise do princípio da proporcionalidade em sentido amplo, podemos então afirmar que as referidas ordens de desencriptação de smartphones através da leitura da impressão digital do arguido (valendo o que foi dito para a desencriptação de smartphones através da palavra-passe) introduzem na ordem jurídica um benefício marginal considerável para o fim visado, mas produzem, simultaneamente, um acréscimo significativo de sacrifícios nas garantias de defesa do arguido e na garantia da reserva da intimidade da sua vida privada e de terceiros, resultando na desproporcionalidade da relação entre benefícios e sacrifícios e, consequentemente, na inconstitucionalidade da medida adoptada pelas entidades judiciárias.

Quanto ao requisito da garantia do conteúdo essencial do direito restringido, queda-nos referir que, pela nossa parte, a ordem de desencriptação de smartphone através da leitura da impressão digital arguido respeita este quarto e último requisito material das restrições a direitos fundamentais. Sendo que o núcleo essencial do princípio *nemo tenetur se ipsum accusare* é aniquilado apenas nas situações em que alguém é "coagido a emitir declarações autoincriminatórias, a declarar a sua culpabilidade, a admitir a sua

participação numa infracção […]"[501] e, atendendo ao facto de que a desencriptação do smartphone através da leitura da impressão digital do arguido somente implica a colocação do dedo do arguido no sensor do dispositivo, podemos afirmar que neste caso em concreto o núcleo essencial do *nemo tenetur* não é atingido nem tão pouco aniquilado. Ainda assim, importa não esquecer que este requisito funciona apenas como um "*plus*" em relação aos restantes limites atrás enunciados, ou seja, funciona como barreira última e efectiva de garantia dos direitos fundamentais caso os restantes requisitos tenham sido previamente preenchidos (o que não se verifica).

Por fim, resta perceber se a norma constante da alínea d) do n.º 3 do artigo 61.º do Código de Processo Penal, mesmo que interpretada, contrariamente ao nosso entendimento, como uma obrigação de o arguido desencriptar o dispositivo através da leitura da sua impressão digital, respeita os requisitos formais impostos pelo artigo 18.º da Constituição da República Portuguesa. Ora, esta norma, ao estipular que recaem em especial sobre o arguido os deveres de "sujeitar-se a diligências de prova […] especificadas na lei e ordenadas e efectuadas por entidade competente", cumpre os requisitos da generalidade, abstracção e não retroactividade. Isto porque é aplicável a um número indeterminado de pessoas, regula um número indeterminado de casos e não se aplica a situações ou actos passados mas sim a desencriptações futuras.

Por tudo o que foi dito até então relativamente à verificação dos limites aos limites nas ordens de desencriptação de smartphones através da leitura da impressão digital do arguido apresentados no Capítulo I, acreditamos que podemos concluir pela sua ilegitimidade caso fossem aprovadas em território nacional. Desde logo, pela ausência de lei prévia e expressa, uma vez que, como vimos, inexiste qualquer disposição legal que obrigue, especificamente, o arguido a desencriptar o seu dispositivo. Depois, porque à luz dos subprincípios da adequação, necessidade e proporcionalidade em sentido estrito, a legitimidade daquela ordem sempre se revelaria desproporcionada, uma vez que, como afirmámos, estes corolários não seriam devidamente respeitados.

6. Conclusões intermédias

Percorremos um longo caminho para chegar à conclusão de que, tanto as ordens de desencriptação de smartphones através da revelação da palavra-passe, quanto as ordens de desencriptação de smartphones através da leitura da impressão digital do arguido, são,

[501] Anastácio, 2010: 217.

nos casos concretos apresentados, ilegítimas por violação do princípio *nemo tenetur se ipsum accusare*. Na verdade, somos levados a crer que, contrariamente ao defendido na jurisprudência e doutrina norte-americanas, não se justifica a necessidade de um tratamento díspar entre os dois métodos de desencriptação: palavra-passe e impressão digital. Da nossa parte, acreditamos ser incoerente a distinção entre um e outro método, isto porque, permitir, por um lado, a coacção de um arguido a fornecer a sua "palavra-passe" na forma de uma impressão digital mas, por outro, proteger o arguido de ser compelido a revelar a sua palavra-passe alfanumérica, acaba por criar uma distinção arbitrária que ignora completamente o propósito do princípio *nemo tenetur se ipsum accusare*[502].

Prova desta indistinção entre a desencriptação através da revelação da palavra-passe e a desencriptação através da leitura da impressão digital é o já mencionado artigo 14.º da Lei do Cibercrime, que parece tratar a desencriptação como um todo[503]. O referido artigo, ao consagrar que "se no decurso do processo se tornar necessário à produção de prova, tendo em vista a descoberta da verdade, obter dados informáticos específicos e determinados, armazenados num determinado sistema informático, a autoridade judiciária competente ordena a quem tenha disponibilidade ou controlo desses dados que os comunique ao processo ou permita o acesso aos mesmos, sob pena de punição por desobediência", não faz distinção entre os métodos de acesso, nomeadamente, de acesso ao smartphone.

A *ratio* do artigo 14.º da Lei do Cibercrime, designadamente do seu n.º 5, é a de proibir toda e qualquer concessão de acesso ao dispositivo electrónico (*v.g.* smartphone) por parte do suspeito ou arguido, sem nunca fazer menção ao método utilizado no acesso. Assim, retiramos da leitura deste preceito, que o legislador quis simplesmente proteger a concessão de acesso aos dados armazenados no sistema informático, seja através da desencriptação por palavra-passe, seja através da desencriptação por leitura da impressão digital, tratando estes dois métodos como iguais.

Desta forma, se a revelação da palavra-passe está protegida pelo *nemo tenetur* por se entender que o arguido tem o direito ao silêncio sempre que lhe sejam dirigidas perguntas cuja resposta possa culminar na sua incriminação, também a desencriptação do smartphone através da leitura da impressão digital deverá seguir o mesmo entendimento,

[502] Larkin, 2012: 270.
[503] Fakhoury, 2012: 86.

uma vez que o resultado será o mesmo num e noutro método: facultar o acesso ao dispositivo encriptado onde potencialmente estarão armazenadas provas incriminatórias.

Ainda no âmbito da indistinção entre os métodos de desencriptação, cumpre esclarecer que, tal como foi mencionado em sede de desencriptação de smartphones através da revelação da palavra-passe, também a impressão digital pode ser considerada como incriminatória, uma vez que o acto de fornecer acesso a um smartphone encriptado às entidades judiciárias indica conhecimento e posse sobre todos os ficheiros e documentos que aí estejam armazenados[504]. Neste sentido, reiteramos a ideia de que determinadas condutas e gestos podem ser consideradas incriminatórias desde que estas, por sua vez, revelem factos, pensamentos, crenças e/ou conhecimento de factos.

Apenas quem tenha registado a sua impressão digital no smartphone pode ter acesso a ele. Por esse motivo, se a impressão digital do arguido permitir o acesso ao smartphone, fica implicitamente provado que o arguido será responsável pelos conteúdos encriptados que estejam armazenados no dispositivo, porquanto ele terá acesso e controlo sobre os mesmos[505]. Neste sentido, na doutrina norte-americana, Susan Brenner vem também reiterar a ideia de que o arguido, ao pressionar o botão do seu smartphone com o seu dedo, desencriptando-o, está a autenticar todos os dados que aí estarão armazenados[506].

A impressão digital acaba por funcionar, aqui, como uma linguagem corporal com intenção comunicativa[507] ou, se preferirmos, como um acto que importa uma declaração autoincriminatória tácita[508].

Em suma, segundo o nosso entendimento, apesar de, nos casos em análise, termos concluído pela ilegitimidade das ordens de desencriptação, quer através da revelação da palavra-passe, quer através da leitura da impressão digital do arguido, não rejeitamos a

---

[504] Goldman, 2015: 224.

[505] "*A fingerprint does more than provide access. It could be use to authenticate identity, but it is clearly a means to identify its owner*". Cf. SaintGermain, 2014a: 29. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2367479 [consultado em 20.02.2017]. "*[…] biometric authentication may communicate an implicit factual assertion that the accused owns the smartphone or laptop and the data therein*". Cf. Sales, 2014: 228. "*Decryption would also require him to admit to possessing the files, controlling the files, being able to access the files, and being able to decrypt the device"*. Cf. Jarone, 2015: 787. Neste sentido, cf. Keenan, 2016: 4. Colarusso, 2011: 135.

[506] A Autora vai mais longe e afirma que "*by showing you opened the phone, you showed that you have control over it. It's the same as if you went home and pulled out paper documents – you produced it"*. Cf. Hamilton/Winton, 2016: 1. Disponível em: http://www.latimes.com/local/california/la-me-iphones-fingerprints-20160430-story.html [consultado em 21.02.2017].

[507] Oliveira Silva, 2015: 269.

[508] Garrett, 2007: 21.

possibilidade de poder haver casos de colaboração do arguido. Concluímos pela existência de uma tipicidade dos casos de colaboração do arguido, mas admitimos que uma lei formal possa impor novos casos de colaboração (independentemente do método de desencriptação), contando que se respeitem os n.os 2 e 3 do artigo 18.º da Constituição da República Portuguesa[509]. Assim, como reiterámos anteriormente, o ponto é que haja uma lei formal que exija a colaboração, que se salvaguarde um outro direito ou interesse constitucionalmente protegido, que esta seja necessária, adequada e proporcional em sentido estrito, que não afecte o núcleo essencial do direito fundamental restringido[510] e que seja uma restrição de carácter geral, abstracto e não retroactivo.

Chegados a este ponto, e depois de esclarecida a questão da violação do privilégio de não-autoincriminação nos casos de desencriptação de smartphones apresentados no Capítulo I, resta-nos apenas indagar sobre a possibilidade de as entidades judiciárias, ainda assim, compelirem o arguido a desencriptar o seu dispositivo, ganhando acesso a todos os dados aí armazenados. Neste caso, que tratamento se deverá dar a estas provas recolhidas em violação do princípio *nemo tenetur se ipsum accusare*?

[509] Pinto, 2013: 111.

[510] Cumpre esclarecer que, no caso de aprovação de uma ordem de desencriptação através da revelação da palavra-passe dirigida arguido, dificilmente se ultrapassará este último requisito material da garantia do núcleo essencial do *nemo tenetur*, mesmo depois da verificação dos restantes requisitos.

CAPÍTULO V – A RECOLHA DE PROVAS EM VIOLAÇÃO DO PRINCÍPIO DE NÃO-AUTOINCRIMINAÇÃO

Como corolário lógico dos direitos de acção e de defesa, as partes têm o direito de introduzir provas no processo com as quais pretendam demonstrar a veracidade das suas alegações[511]. Nas palavras de Germano Marques da Silva, o direito à prova é "a faculdade que têm os sujeitos processuais de participar activamente na produção da prova, quer requerendo a sua admissão no processo, quer participando na sua produção"[512].

No entanto, tal como todos os outros direitos, este também não será um direito absoluto, ou seja, há limites para a admissão e produção de prova. Neste sentido, Elizabeth Queijo atesta que "se não houvesse limitações ao direito à prova, todo e qualquer material probatório, mesmo que produzido à custa de violações a direitos, poderia ser introduzido no processo e valorado, o que conduziria à adopção de um modelo de processo autoritário e distante da ética"[513].

Assim sendo, o nosso Código de Processo Penal consagra, no seu artigo 125.º, o princípio da legalidade da prova – "são admissíveis as provas que não forem proibidas por lei". Ao proibir a utilização de certos meios probatórios, quis o legislador delimitar (negativamente) o elenco das provas admitidas em processo penal. A fórmula adoptada no artigo 125.º tem aqui o sentido de que não são apenas admitidos os meios probatórios tipificados, mas também todos os meios de prova que não forem proibidos mesmo sendo atípicos[514]. Daqui resulta que, para a aquisição de informação probatória necessária, pode o julgador socorrer-se dos meios tipificados: as chamadas provas típicas (testemunhos, documentos, perícias, etc). Mais: é-lhe reconhecida, em princípio, a liberdade de escolher indiferentemente qualquer dessas fontes tipificadas de conhecimento, seja qual for a natureza da factualidade a provar[515].

[511] Ristori, 2007: 163.
[512] Marques da Silva, 2011: 116.
[513] Queijo, 2012: 374.
[514] Oliveira Silva, 2011: 560. Neste sentido escreve também Germano Marques da Silva, "proibindo a utilização de certos meios de prova, a norma consagra também […] a liberdade da prova, no sentido de serem admissíveis para a prova de quaisquer factos todos os meios de prova admitidos em direito, ou seja, que não sejam proibidos, mesmo sendo atípicos". Cf. Marques da Silva, 2011: 136-137.
[515] Oliveira Silva, 2011: 561.

Não obstante esta liberdade, a realização da justiça e a busca pela verdade material, à semelhança do direito à prova, e apesar de serem valores constitucionais[516], não são valores absolutos, que possam ser perseguidos por qualquer forma[517]. Esta verdade não é uma verdade absoluta ou ontológica, mas uma verdade judicial, que deve ser procurada e obtida através dos meios legalmente admissíveis[518].

1. As proibições de prova

Um dos meios de que a lei se serve para, protegendo os cidadãos, impedir as práticas abusivas na produção de prova é através do estabelecimento de proibições de prova. A este propósito, escreve Costa Andrade: "Como Gössel acentua, as proibições de prova são «barreiras colocadas à determinação dos factos que constituem objecto do processo». Mais do que a modalidade do seu enunciado, o que define a proibição de prova é a prescrição de um limite à descoberta da verdade. Normalmente formulada como proibição, a proibição de prova pode igualmente ser ditada através de uma imposição e, mesmo, de uma permissão. É que, como Gössel pertinentemente assinala, «toda a regra relativa à investigação dos factos proíbe ao mesmo tempo as vias não permitidas de averiguação»"[519].

1.1. A distinção entre proibições de produção de prova e proibições de valoração de prova

Por doutrina das proibições de prova compreende-se aqui a doutrina das proibições de investigação de determinados factos relevantes para o objecto do processo, bem como das proibições de levar determinados factos ao objecto da sentença e, finalmente, das consequências processuais da violação daquelas proibições[520].

Neste sentido, a doutrina portuguesa[521], na esteira do defendido pela doutrina maioritária alemã, vem distinguir, no âmbito das proibições de prova, entre proibições de produção de prova (*Beweiserhebungsverbote*) e proibições de valoração de prova (*Beweisverwertungsverbote*). As primeiras regulam e limitam o modo de obtenção das

[516] Miranda/Medeiros, 2010: 737.
[517] Marques da Silva, 2006: 39. Neste sentido vai também Claus Roxin: "[…] A averiguação da verdade não é um valor absoluto no processo penal; pelo contrário, o próprio processo penal está impregnado de hierarquias éticas e jurídicas […]". Cf. Roxin, 2000: 191.
[518] Andrade, 2010: 47.
[519] Costa Andrade, 1992: 83.
[520] Gössel, 1992: 397-398.
[521] "A doutrina processual penal das proibições de prova abrange (1) as proibições de produção de prova e (2) as proibições de valoração de prova […]". Cf. Sousa Mendes, 2004: 134.

provas[522], ao passo que as segundas impedem que determinados factos sejam objecto de sentença[523]. Cumpre deixar claro, nesta sede, que é na determinação da proibição da valoração de prova que se colocam os grandes dilemas que surgem no confronto com a realidade. Saber se à proibição de produção de prova deve corresponder sempre, por vezes ou nunca uma proibição de valoração da prova é, no fundo, a questão que desde sempre é tratada com maior acuidade e dissonâncias, tanto na doutrina, como na jurisprudência[524].

Além desta diferenciação, dentro das proibições de produção de prova, distinguem-se tradicionalmente três categorias: a) os temas de prova proibidos[525] (há temas de prova proibidos e que, por conseguinte, não devem ser investigados – é o caso dos factos abrangidos pelo segredo de Estado[526]); b) os meios de prova proibidos[527] (há também proibições de produção de prova através de determinados meios de prova: é o caso da proibição de produção de prova através dos suportes técnicos e respectivas transcrições quando tiverem sido gravadas conversações em que intervenham o Presidente da República, o Presidente da Assembleia da República ou o Primeiro-Ministro – al. b) do n.º 2 do artigo 11.º do CPP[528]); c) os métodos de prova proibidos[529] (os métodos de prova são os procedimentos usados pelas autoridades judiciárias, pelas polícias criminais, pelos advogados e até pelos particulares para a aquisição de meios de prova e sua utilização no processo[530])[531].

1.2. O regime legal das proibições de prova

O regime das proibições de prova no âmbito do processo penal encontra-se essencialmente regulado pelo preceituado nos artigos 125.º e 126.º do Código de Processo Penal, os quais devem ser conjugados com as garantias constitucionais de defesa, consagradas no artigo 32.º da Constituição da República Portuguesa, mormente a

[522] Ambos, 2008: 329.
[523] Gössel, 1992: 399.
[524] Neves, 2011: 317.
[525] "As proibições de temas de prova impedem a obtenção de provas sobre determinados factos (temas), por exemplo, antecedentes criminais já eliminados do Registo Central Federal […]". Cf. Ambos, 2008: 329.
[526] Sousa Mendes, 2017: 178.
[527] "As proibições de meios de prova impedem a utilização de determinados meios de prova, como por exemplo, uma declaração prestada por uma testemunha que tenha abdicado do seu direito a testemunhar […]". Cf. Ambos, 2008: 329.
[528] Sousa Mendes, 2017: 179.
[529] "As proibições de metódos de prova impedem um determinado modo de obtenção de prova, por exemplo, um método de interrogatório proibido de acordo com o §136ª". Cf. Ambos, 2008: 329.
[530] Sousa Mendes, 2017: 179.
[531] Rosa, 2010: 221-222.

injunção imposta pelo seu n.º 8, bem como, com as disposições específicas que disciplinam a obtenção do meio de prova de que se pretende fazer uso.

O n.º 8 do artigo 32.º da Constituição, que consagra o princípio das proibições de prova e encontra também consagração nos textos do direito internacional[532], estabelece a nulidade[533] de "todas as provas obtidas mediante tortura, coacção, ofensa da integridade física ou moral da pessoa, abusiva intromissão da vida privada, no domicílio, na correspondência ou nas telecomunicações". A tortura, a coacção ou a ofensa da integridade física ou moral da pessoa em geral são métodos absolutamente proibidos de obtenção de provas. Já a intromissão na vida privada, no domicílio, na correspondência ou nas telecomunicações são métodos relativamente proibidos, como podemos comprovar pelo afastamento da proibição, quer pelo acordo do titular dos direitos em causa, quer pelas restrições à inviolabilidade desses direitos constantes nos n.os 2, 3 e 4 do artigo 34.º da Constituição da República Portuguesa[534].

Desta forma, na disciplina da matéria das proibições de prova, o legislador constituinte não se limitou, com efeito, a propor os valores e a definir as balizas a que deveria obedecer a configuração do processo penal, em definitivo acometida ao legislador ordinário. Em vez de delinear apenas o horizonte político-criminal e axiológico das normas ordinárias, o legislador constitucional optou por defenir, desde logo, os princípios materiais reitores do processo, chamando a si a conformação normativa directa dos aspectos mais decisivos

[532] Cf. artigos 5.º e 12.º da Declaração Universal dos Direitos do Homem, artigos 3.º e 8.º da Convenção Europeia dos Direitos do Homem e artigo 7.º do Pacto Internacional sobre Direitos Civis e Políticos.

[533] "O que há de novo no n.º 8 não é a proibição do uso de meios proibidos na obtenção dos elementos de prova, mas essencialmente a utilização das provas obtidas por tais meios. Essas provas é que são nulas […]". Cf. Miranda/Medeiros, 2010: 737.

[534] Sousa Mendes, 2017: 180. Neste sentido, cf. Ristori, 2007: 168-169; Simas Santos/Leal-Henriques, 2008: 663. "A interdição é absoluta no caso do direito à integridade pessoal; e relativa, nos restantes casos, devendo ter-se por abusiva a intromissão quando efectuada fora dos casos previstos na lei e sem intervenção judicial (n.os 2 e 4 do artigo 34.º), quando desnecessária ou desproporcionada ou quando aniquiladora dos próprios direitos". Cf. Gomes Canotilho/Moreira, 2014: 524. "[…] é possível autonomizar no espectro de análise duas espécies diferenciadas de provas proibidas, consoante a natureza dos direitos fundamentais em causa. Na primeira parte da norma, estabelece-se sem mais a nulidade de todas as provas obtidas à custa de «tortura, coacção, ofensa da integridade física ou moral da pessoa» (1.ª parte do n.º 8 do artigo 32.º da CRP). Na segunda parte, alude-se às provas obtidas com «intromissão da vida privada, no domicílio, na correspondência ou nas telecomunicações», que se contra-distinguem das primeiras pela circunstância de, em relação a elas, a interdição só existir se a intromissão se revelar «abusiva» (2.ª parte do n.º 8 do artigo 32.º da CRP) – uma asserção que é, aliás, corroborada pelo teor dos artigos 26.º e 34.º da CRP". Cf. Oliveira Silva, 2011: 584. A legislação alemã faz, igualmente, a distinção entre proibições absolutas e relativas, sendo que "Enquanto as absolutas têm uma validade geral, as relativas limitam a obtenção de prova, no sentido em que, apenas determinadas pessoas estão habilitadas a ordenar ou realizar uma produção probatória, estabelecendo assim uma proibição para qualquer outro sujeito". Cf. Ambos, 2008: 329.

da tramitação, em que avulta com particular destaque a disciplina dos métodos proibidos de prova[535].

Sob a epígrafe de "métodos proibidos de prova", o artigo 126.º do Código de Processo Penal, ao concretizar a nulidade dos métodos de produção de prova a que se refere o n.º 8 do artigo 32.º da CRP, repete a citada distinção entre as proibições absolutas e as proibições relativas de obtenção de provas. No caso dos n.os 1 e 2 do artigo 126.º, vigora uma proibição absoluta de obtenção de provas através dos meios ali indicados, ainda que sejam obtidas a coberto do consentimento do titular dos direitos em causa. No caso do n.º 3 do artigo 126.º, a proibição é afastada pelo acordo do titular dos direitos em causa ou, em alternativa, é removida mediante as ordens ou autorizações emanadas de certas autoridades, nos termos da lei[536]. Ainda em sede de caracterização geral dos métodos proibidos de prova convirá ressalvar que nada parece impor a conclusão de que no artigo 126.º se contenha uma enumeração taxativa[537]. Para além das técnicas proibidas elencadas no artigo 126.º e das demais proibições de prova dispersas pelo ordenamento processual, outras poderão ser reconhecidas pela doutrina e pela jurisprudência nos domínios em que o método de aquisição probatória concretamente utilizado importe uma intromissão injustificada nos direitos fundamentais do arguido ou outras pessoas[538].

Posto isto, a especificidade do sistema processual penal português reside na estipulação de uma norma constitucional, bem como de uma correspectiva regra legal que a densifica, ambas com vocação genérica, que especificam exactamente quais os direitos fundamentais cuja violação inquina a prova em processo penal e gera a sua nulidade[539].

Na tutela conferida a estes direitos fundamentais enquanto limitações à prova radicam antes de mais a posição e o estatuto do arguido como sujeito processual. O étimo comum de muitos dos métodos de prova proscritos pelo legislador reconduz-se à ideia de que "a utilização do arguido como meio de prova deverá ser sempre limitada pelo integral respeito pela sua decisão de vontade: só no exercício de uma plena liberdade de vontade pode o arguido decidir-se se e como deseja tomar posição perante a matéria que constitui objecto do processo"[540]. Desde logo, se considerarmos a vertente negativa desta liberdade

[535] Oliveira Silva, 2011: 576-577.
[536] Sousa Mendes, 2017: 180.
[537] Costa Andrade, 1992: 216.
[538] Oliveira Silva, 2011: 589.
[539] Morão, 2006: 588.
[540] Oliveira Silva, 2011: 578.

de vontade, enquanto autêntico direito de defesa (*Abwehrrecht*) contra o Estado[541], vedando todas as tentativas de obtenção, por meios enganosos ou, no nosso caso, por coacção, de declarações autoincriminatórias, podemos afirmar que é precisamente nesta dimensão, associada ao princípio *nemo tenetur se ipsum accusare*, que a liberdade de vontade do arguido assume a mais directa relevância em matéria de proibições de prova[542].

1.3. A invalidade do acto processual

Cumpre ainda deixar claro, como ensina Costa Andrade, que o legislador português associou as proibições de prova à figura e ao regime das nulidades, isso diante da locução "São nulas todas as provas […]", no n.º 8 do artigo 32.º da CRP[543]. No entanto, o regime da nulidade das provas proibidas é substancialmente mais rigoroso do que o das nulidades dependentes de arguição (artigo 120.º do CPP) ou mesmo do que o das nulidades insanáveis (artigo 119.º do CPP). O legislador português, ciente desta disparidade, prescreveu, no n.º 3 do artigo 118.º do Código de Processo Penal, a autonomia técnica das proibições de prova[544], estabelecendo, de forma expressa, que "as disposições do presente título não prejudicam as normas deste Código relativas a proibições de prova"[545]. Ou seja, que as regras gerais sobre as nulidades processuais penais não se aplicam às proibições de prova.

Bem vistas as coisas, o legislador criou pelo menos um regime *sui generis* a saber: as nulidades do artigo 126.º do Código de Processo Penal. Na verdade, a nulidade mencionada no n.º 8 do artigo 32.º da CRP e no artigo 126.º do CPP não é uma nulidade em sentido técnico-processual, mas uma nulidade dotada de uma autonomia técnica completa em face do regime das nulidades processuais[546].

O carácter *sui generis* do regime da nulidade de prova cominada nos n.ºs 1 e 3 do artigo 126.º Código de Processo Penal, há-de consistir no seu conhecimento oficioso, podendo ser declarada mesmo depois do trânsito em julgado da decisão final, admitindo-se assim a revisão de sentença[547]. Por fim, cumpre ressalvar que o n.º 4 do artigo 126.º do CPP

[541] Oliveira Silva, 2011: 579.
[542] Costa Andrade, 1992: 121.
[543] Costa Andrade, 1992: 313.
[544] Costa Andrade, 2009: 133.
[545] Correia, 1999b: 156.
[546] Sousa Mendes, 2017: 187.
[547] Questões Avulsas, 2000: 100-101.

apenas admite a utilização de provas proibidas para proceder criminalmente contra quem as obteve. Contudo, não se pode ignorar a possibilidade de utilizar a prova com a finalidade de demonstrar que é proibida[548].

1.4. O efeito-à-distância das proibições de prova

Por fim, perante uma prova proibida, coloca-se a questão de saber se a proibição vale só para o meio de prova obtido directamente de modo proibido ou se também afecta outros meios de prova obtidos indirectamente através da prova proibida[549] – é a problemática do efeito-à-distância das proibições de prova. De facto, é na consideração da extensão da proibição da valoração da prova obtida com proibição de produção que se colocam muitas das problemáticas que ainda hoje ocupam a doutrina e a jurisprudência[550].

O problema do efeito-à-distância suscita-se nos casos em que a obtenção de uma determinada prova torna possível a descoberta de novos meios de prova contra o arguido ou contra terceiro. Nestes casos, cabe questionar se a proibição de valoração que eventualmente inquine a prova primária ou directa se comunica, e em que medida, às provas secundárias ou indirectas, impondo a sua exclusão em cadeia. Como facilmente se representará, o problema ganha particular relevo prático-jurídico nas hipóteses frequentes em que o recurso a métodos proibidos de prova (*v.g.*, a coacção) levam o arguido a comprometedoras declarações autoincriminatórias[551].

Como defende Paulo de Sousa Mendes, a doutrina jurisprudencial dos "frutos da árvore envenenada" (*fruit of the poisonous tree doctrine*) ou da "mácula" (*taint doctrine*) e a sua equivalente germânica, também designada de teoria da mácula (*Makel-Theorie*), enquanto metáfora da nodóa de ilegalidade, reconhece que as provas que atentam contra os direitos de liberdade arrostam com um efeito-à-distância que consiste em tornarem inaproveitáveis as provas secundárias a elas causalmente vinculadas[552].

---

[548] Rosa, 2010: 235.
[549] Miranda/Medeiros, 2010: 737.
[550] Neves, 2011: 317.
[551] Costa Andrade, 1992: 169.
[552] Sousa Mendes, 2014: 219. A génese da jurisprudência da 'mácula' foi o caso Silverthorne Lumber Co. v. United States, decidido pelo Supremo Tribunal dos Estados Unidos da América, em 1920. Estava em causa o facto de agentes federais terem apreendido ilegalmente documentos nas instalações da sociedade comercial Silverthorne, que um tribunal de comarca (*district court*) mandou devolver, tendo o procurador (*prosecutor*) promovido perante um grande júri (*grand jury*) a notificação dos arguidos (*defendants*) para produzirem os mesmos documentos, sob pena de multas (*subpoenas*). Em via de recurso, o Supremo Tribunal dos Estados Unidos da América decidiu que as referidas intimações eram inválidas, declarando, pela pena do famoso Juiz Conselheiro Oliver Wendell Holmes, Jr., enquanto relator que: "[a] essência de uma norma de proibição de aquisição de provas de certa maneira não se limita a determinar que as provas

O efeito-à-distância é a única forma de impedir que os investigadores policiais, os procuradores e os juízes menos escrupulosos se aventurem à violação das proibições de produção de prova na mira de prosseguirem sequências investigatórias às quais não chegariam através dos meios postos à sua disposição pelo Estado de Direito[553].

Na jurisprudência portuguesa, o efeito-à-distância foi reconhecido, pela primeira vez, pelo Tribunal Judicial de Oeiras (Sentença do 3.º Juízo, de 5 de Março de 1993, Proc. n.º 777/91, 2.ª Secção): "a nulidade do primeiro dos meios de prova é extensiva ao segundo, impossibilitando, da mesma forma, o julgador de extrair deste último qualquer juízo valorativo".

Contudo, a vigência da doutrina do efeito-à-distância está longe de ser absoluta e irrestrita. A história da emergência e afirmação do princípio também é a história do enunciado e das tentativas de fundamentação e sistematização de uma gama alargada de excepções[554].

Entre elas avulta, em primeiro lugar, a excepção da "fonte independente" (*independent source exception*)[555], derivada dos precedentes Silverthorne Lumber Co. v. United States[556] de 1920, Wong Sun v. United States[557] de 1963 e Segura v. United States[558] de 1984, que admite a possibilidade de valoração das provas mediatas, nos casos em que, ao lado do chamado caminho proibido, existe um outro caminho autónomo, independente, de onde as mesmas provas podem também ser retiradas[559]. Ou seja, aceita as provas que foram ou poderiam ter sido obtidas por via autónoma e lícita[560].

---

assim adquiridas não poderão ser utilizadas em tribunal, mas também que não poderão ser usadas de maneira nenhuma. É claro que isto não significa que os factos assim obtidos se tornem sagrados e inacessíveis. Se a informação acerca dos mesmos for obtida através de uma fonte independente, então esses factos podem ser provados tal como quaisquer outros, mas o conhecimento obtido pelo Estado por meios ilícitos não pode ser por si usado da maneira pretendida". A expressão "frutos da árvore envenenada" surgiu pela pena do igualmente famoso Juiz Conselheiro Felix Frankfurter, no caso Nardone v. United States, de 1939. Cf. Sousa Mendes, 2017: 192.

[553] Sousa Mendes, 2014: 220.

[554] Costa Andrade, 1992: 171.

[555] Kamisar/LaFave/Israel/King/Kerr/Primus, 2015: 765-768.

[556] Silverthorne Lumber Co. v. United States, 1920. Disponível em: https://supreme.justia.com/cases/federal/us/251/385/case.html [consultado em 09.03.2017].

[557] Wong Sun v. United States, 1963. Disponível em: https://supreme.justia.com/cases/federal/us/371/471/case.html [consultado em 09.03.2017].

[558] Segura v. United States, 1984. Disponível em: https://supreme.justia.com/cases/federal/us/468/796/ [consultado em 09.03.2017].

[559] Morão, 2006: 613.

[560] Miranda/Medeiros, 2010: 737.

A segunda excepção do efeito-à-distância é designada por excepção da "descoberta inevitável" (*inevitable discovery exception*)[561], foi fundada nas importantes decisões Brewer v. Williams[562] de 1977 e Nix v. Williams[563] de 1984 e determina a aceitação das provas que inevitavelmente seriam descobertas, mesmo que mais tarde, através de outro tipo de investigação[564]. Trata-se, segundo Paulo de Sousa Mendes, de uma "variante da 'fonte independente', mas difere desta excepção na medida em que não se exige aqui que a polícia tenha, de facto, obtido provas também através de uma fonta autónoma e legal, mas apenas que tivesse podido, hipoteticamente, fazê-lo […]"[565].

Por fim, a terceira e última excepção, a excepção da "nódoa (ou mácula) dissipada" (*purged taint exception*)[566], baseada nas decisões Wong Sun v. United States[567] de 1963 e United States v. Ceccolini[568] de 1978, vem estabelecer a possibilidade de utilização no processo de toda a prova secundária a que os órgãos de investigação criminal não teriam chegado, de uma perspectiva de relação causal, sem a violação da proibição de prova, mas relativamente à qual se pode dizer que já nenhum nexo causal efectivo subsiste entre tal prova mediata e a violação inicial[569]. Ou seja, poderiam ser valoradas todas as provas secundárias se a conexão se tiver tornado tão atenuada a ponto de dissipar a mácula[570]. Seria o caso do arguido que é levado a confessar determinados factos de modo autoincriminatório[571], por força de uma anterior violação de proibição de prova, mas que, mais tarde, após ter sido convenientemente informado de que tais provas não podem ser utilizadas, opta por confessar os mesmos factos espontaneamente[572].

---

[561] Kamisar/LaFave/Israel/King/Kerr/Primus, 2015: 775-780.
[562] Brewer v. Williams, 1977. Disponível em: https://supreme.justia.com/cases/federal/us/430/387/ [consultado em 09.03.2017].
[563] Nix v. Williams, 1984. Disponível em: https://supreme.justia.com/cases/federal/us/467/431/case.html [consultado em 09.03.2017].
[564] Miranda/Medeiros, 2010: 738.
[565] Sousa Mendes, 2017: 193.
[566] Kamisar/LaFave/Israel/King/Kerr/Primus, 2015: 774.
[567] Wong Sun v. United States, 1963. Disponível em: https://supreme.justia.com/cases/federal/us/371/471/case.html [consultado em 09.03.2017].
[568] United States v. Ceccolini, 1978. Disponível em: https://supreme.justia.com/cases/federal/us/435/268/ [consultado em 09.03.2017].
[569] Morão, 2006: 615.
[570] Sousa Mendes, 2014: 221.
[571] Elementos de estudo, 2012: 639-640. Morão, 2012: 717.
[572] Morão, 2006: 615. Cf. Acórdão do Tribunal Constitucional n.º 198/2004, de 24 de Março de 2004, disponível em: http://www.tribunalconstitucional.pt/tc/acordaos/20040198.html [consultado em 09.03.2017]. Decisão Sumária do Tribunal Constitucional n.º 13/2008, de 11 de Janeiro de 2008, disponível em: http://www.tribunalconstitucional.pt/tc/decsumarias/20080013.html [consultada em 09.03.2017].

Chegados a este ponto, e analisada que está a consagração e o regime das proibições de prova em processo penal, resta-nos apenas indagar da aplicabilidade deste regime ao nosso caso concreto: violação do princípio *nemo tenetur se ipsum accusare* através da ordem de desencriptação compelida dirigida ao arguido no sentido de permitir o acesso ao seu smartphone, quer através do fornecimento da sua palavra-passe quer através da leitura da sua impressão digital.

2. Consequências da recolha de prova em violação do princípio de não-autoincriminação

O princípio *nemo tenetur se ipsum accusare* constitui, como já tivemos oportunidade de analisar, um direito do arguido perante o *ius puniendi* do Estado. Desta forma, toda e qualquer restrição deste direito que não obedeça aos limites aos limites dos direitos fundamentais (n.os 2 e 3 do artigo 18.º da Constituição da República Portuguesa), instrumentalizando o arguido contra a sua vontade ou através do seu corpo, a ser objecto da sua própria incriminação, viola este princípio.

No caso concreto da ordem de desencriptação do smartphone dirigida ao arguido por parte das autoridades judiciárias, podemos afirmar que estaremos aqui perante um método proibido de prova, dado que o arguido é utilizado como meio de prova com perturbação da sua vontade e liberdade através da coacção.

Mais especificamente, no que concerne ao primeiro método de desencriptação – o fornecimento da palavra-passe – importa reter as palavras de Figueiredo Dias quando atesta que "têm de considerar-se proibidos e inadmissíveis em processo penal todos os meios de interrogatório e de obter declarações que importem […] qualquer perturbação da liberdade de vontade e de decisão [do arguido]"[573], nomeadamente através de coacção. Desta forma, dada a coacção empregue, por parte das autoridades judiciárias, na ordem de desencriptação do smartphone dirigida ao arguido no sentido de este revelar a palavra-passe do seu dispositivo, outra não poderá ser a conclusão senão a de que este será um método de obtenção de prova proibido.

[573] Figueiredo Dias, 2004: 454. Também na doutrina alemã, Claus Roxin informa que o Tribunal Federal alemão tem considerado o direito de guardar silêncio entre os princípios fundamentais do processo penal, de tal modo que também a sua violação pela polícia deve conduzir a uma proibição de valoração. Cf. Roxin, 2000: 195-196. Neste sentido vai também Gössel ao afirmar que a legislação alemã proíbe, no §136a do StPO, a valoração dos interrogatórios produzidos à custa do sacrifício da liberdade de formação de vontade do arguido. Cf. Gössel, 1992: 415, 423.

Por outro lado, e apesar de a desencriptação do smartphone através da leitura da impressão digital do arguido não se enquadrar, como vimos anteriormente, na categoria de "meios de interrogatório ou de obter declarações", acreditamos que quaisquer restrições a direitos, liberdades e garantias fundamentais (*v.g.* direito de não-autoincriminação) que não atendam estritamente ao texto constitucional serão intoleráveis e inadmissíveis, sendo as provas obtidas por esses meios proibidas. Ou seja, toda e qualquer restrição que não obedeça aos limites aos limites dos direitos fundamentais, reprimindo a liberdade ou a vontade de decisão do arguido, por qualquer meio, constitui uma violação do princípio *nemo tenetur* e, como efeito, prova proibida. Defendemos a ideia de que a vinculatividade do artigo 126.º transcende claramente o domínio do interrogatório e das declarações do arguido, projetando-se como limite à admissibilidade de quaisquer outras diligências probatórias. Também em sede de proibições de prova parece não haver distinção entre os dois métodos de desencriptação: palavra-passe e biometria.

Assim, todas as provas autoincriminatórias obtidas à custa de coacção e em violação dos limites aos limites das restrições aos direitos fundamentais são provas proibidas[574]. Não é outra leitura que se infere da Constituição da República Portuguesa e do Código de Processo Penal. A sua interdição é absoluta, configurando-se em provas de valoração proibida, nos termos do n.º 8 do artigo 32.º da CRP e do n.º 1 do artigo 126.º do CPP[575], cominação que traduz a existência de uma nulidade particularmente grave e insanável[576].

Manuel da Costa Andrade entende que neste campo de danosidade social será muito difícil valorar a prova proibida[577]. Estando perante um caso de proibição de prova desencadeada pela violação insuportável de direitos de defesa do arguido, como é o caso do direito à não-autoincriminação, não só não se poderá valorar a prova inicialmente proibida, como também as provas que se desencadearam com base naquela primeira.

De facto, dado que a desencriptação do smartphone permitirá às autoridades acederem a provas incriminatórias, a doutrina do efeito-à-distância pode aqui prevenir uma tão frontal como indesejável violação do princípio *nemo tenetur se ipsum accusare*. Costa Andrade reitera ainda que "como assinala Beulke, «a valoração de meios de prova tornados

[574] Costa Andrade, 1992: 126-127.
[575] O n.º 8 do artigo 32.º da CRP consagra que "São nulas todas as provas obtidas mediante […] coacção […]". O n.º 1 do artigo 126.º do CPP estipula que "São nulas, não podendo ser utilizadas, as provas obtidas mediante […] coacção […]".
[576] Silva Dias/Ramos, 2009: 36-37.
[577] Costa Andrade, 1992: 282.

possíveis a partir de declarações obtidas à custa de coação […], equivaleria a compelir o arguido a colaborar na sua própria condenação»"[578].

Assim, segundo a teoria dos "frutos da árvore envenenada", também as provas secundárias recolhidas a partir da desencriptação do smartphone em que houve violação do *nemo tenetur* são proibidas. No entanto, como reiterámos anteriormente, esta doutrina tem excepções. Para o nosso caso concreto – desencriptação de smartphones – interessa-nos apenas a excepção da "fonte independente" (*independent source exception*) e a excepção da "nódoa (ou mácula) dissipada" (*purged taint exception*).

A excepção da "fonte independente" (*independent source exception*) poderia ser aplicada no nosso caso concreto nas situações em que a polícia conseguisse aceder às provas armazenadas no smartphone de forma lícita, nomeadamente através da utilização de nova tecnologia que permitisse a desecriptação ou até mesmo através da descoberta da palavra-passe. Assim, mesmo depois de acederem às provas contidas no smartphone que fora ilicitamente acedido através da coacção do arguido – quer pela revelação da palavra-passe, quer pela leitura da sua impressão digital -, as autoridades judiciárias poderiam utilizar os ficheiros – agora licitamente - recolhidos.

À semelhança da excepção da "fonte independente", também a excepção da "nódoa (ou mácula) dissipada" (*purged taint exception*) pode ser aplicada no nosso caso de desencriptação de smartphones. Se o arguido permitisse o acesso ao seu smartphone, através da revelação da palavra-passe ou da leitura da sua impressão digital, por força de uma anterior violação de proibição de prova e, posteriormente, optasse por confessar a palavra-passe, as autoridades judiciárias poderiam utilizar esta palavra-passe para aceder licitamente aos ficheiros autoincriminatórios armazenados no dispositivo e utilizá-los como prova no processo penal.

Deste modo, podemos concluir que a ordem de desencriptação de smartphone, seja através da revelação da palavra-passe ou da leitura da impressão digital do arguido, culmina numa situação de obtenção de prova à custa da coacção do arguido (n.º 8 do artigo 32.º da CRP e n.º 1 do artigo 126.º do CPP). E, segundo a doutrina do efeito-à-distância, não só não se poderá valorar a prova inicialmente proibida (provas primárias), como também as provas que se desencadearam com base naquela primeira (provas secundárias). No entanto, as provas incriminatórias armazenadas no smartphone podem,

[578] Costa Andrade, 1992: 315.

ainda assim, ser utilizadas e valoradas no processo caso a excepção da "fonte independente" ou da "nódoa/mácula dissipada" se verifiquem.

CONCLUSÕES GERAIS

Conforme se depreende do exposto ao longo desta nossa investigação, a ordem de desencriptação dirigida ao arguido, pelas autoridades judiciárias, no sentido de este permitir o acesso ao seu smartphone através da revelação da palavra-passe ou da leitura da sua impressão digital, suscita uma série de questões.

As discussões na doutrina norte-americana em volta desta problemática influenciarão o mundo e desencadearão novas discussões, nomeadamente em território nacional, considerando que o princípio *nemo tenetur se ipsum accusare* foi, nos casos apresentados, claramente restringido até ao ponto de restar apenas o direito ao silêncio.

Depois de nos munirmos dos conhecimentos necessários quanto ao acesso e apreensão dos dados armazenados no smartphone segundo a Lei do Cibercrime, à encriptação destes dispositivos e à articulação entre a colaboração do arguido nos casos de desencriptação compelida e o princípio contra a autoincriminação, estamos já em posição de criticar a fundamentação e a decisão dos casos norte-americanos apresentados no primeiro capítulo e de discutir o seu enquadramento no direito processual penal português.

Ficou expresso anteriormente que o princípio *nemo tenetur se ipsum accusare*, tendo por fundamento as garantias processuais reconhecidas ao arguido no texto constitucional, poderá ser alvo de limitações. De facto, pela circunstância de não se revestir de natureza absoluta, este princípio poderá ser derrogado, nomeadamente nos casos em que o arguido é obrigado a identificar-se ou a sujeitar-se a determinados exames ou perícias.

Por esse motivo, não consideramos defensável que se infira uma total inflexibilidade do princípio contra a autoincriminação que inviabilize por completo a adopção de normas que permitam a emissão de ordens de desencriptação e que, em complemento, incriminem a conduta omissiva do arguido.

Contudo, revisitando uma vez mais o que por nós já foi afirmado quanto à natureza da revelação, por parte do arguido, de uma palavra-passe, entendemos que a mesma pode ser reconduzida ao instituto das declarações do arguido. Assim, se a natureza da revelação de uma palavra-passe pode ser entendida do mesmo modo que uma declaração proferida pelo arguido, a ponderação do direito ao silêncio não pode deixar de ser efectuada. Sendo o direito ao silêncio, como vimos, um expoente máximo do princípio *nemo tenetur*, não podemos deixar de considerar que o mesmo seria objecto de uma evidente derrogação

acaso os investigadores criminais compelissem o arguido a revelar a palavra-passe que permite o acesso ao seu dispositivo electrónico. Segundo um critério de ponderação e atendendo, igualmente, aos limites aos limites das restrições de direitos fundamentais (*v.g.* direito à não-autoincriminação), esta ordem seria ilegítima por falta de previsão legal expressa, por ser desproporcional e por violar o núcleo essencial do princípio *nemo tenetur*. Efectivamente, no panorama legal português não há uma previsão legal no sentido de estabelecer uma excepção ao princípio *nemo tenetur*, ao contrário do que se passa na lei inglesa e belga.

No que à leitura da impressão digital diz respeito, podemos agora concluir que, tendo como base os casos apresentados no primeiro capítulo da presente investigação, também a ordem dada ao arguido no sentido de este desencriptar o seu smartphone através da leitura da sua impressão digital é uma ordem ilegítima e violadora do princípio contra a autoincriminação. Cremos nesta conclusão por dois motivos principais: a) o dever de sujeição a diligências de prova consagrado na alínea d) do n.º 3 do artigo 61.º do Código de Processo Penal, dada a sua generalidade, não pode ser entendido como previsão legal expressa no sentido de estabelecer uma excepção ao princípio contra a autoincriminação, resultando na falta de preenchimento do primeiro requisito das restrições de direitos fundamentais (exigência de lei formal); b) e, atendendo às circunstâncias dos casos concretos, todas estas ordens de desencriptação através da leitura da impressão digital do arguido revelaram-se desproporcionais.

Isto posto, outra não poderá ser a conclusão senão a de que, nestes casos apresentados, as ordens de desencriptação dos smartphones através da revelação da palavra-passe ou da leitura da impressão digital dirigidas aos arguidos/suspeitos são, segundo o ordenamento jurídico português, ilegítimas por violação do princípio *nemo tenetur se ipsum accusare*. Se, ainda assim, forem recolhidas provas autoincriminatórias do smartphone em violação deste princípio a consequência é óbvia: proibição de valoração dessas provas.

O que se deve discutir aqui não é a possibilidade de o Estado restringir o direito do arguido à sua não-autoincriminação, mas sim a que extensão essa restrição pode ocorrer sem que se torne a ordem inconstitucional. Daí se infere que, apesar da conclusão a que chegamos quanto aos casos norte-americanos, no ordenamento jurídico nacional, uma vez que o princípio *nemo tenetur se ipsum accusare* não tem carácter absoluto, por intermédio de legislação específica, com o objectivo de salvaguardar um outro direito ou interesse constitucionalmente protegido, sendo proporcional em sentido amplo e não violadora do

núcleo essencial do direito, poderá um arguido ser compelido a desencriptar o seu smartphone, independentemente do método (palavra-passe ou impressão digital), no âmbito de uma investigação criminal. Não podemos defender aqui peremptoriamente uma zona de *offshore* digital num Estado de Direito[579].

[579] Expressão usada por Pedro Verdelho na Conferência sobre Prova Digital em Processo Penal, realizada a 24 de Maio de 2017 na Faculdade de Direito da Universidade de Lisboa.

BIBLIOGRAFIA

AA.VV., Elementos de Estudo: Direito Processual Penal, 2.ª Reimpressão, Lisboa, AAFDL, 2012.

AA.VV., Questões Avulsas de Processo Penal, Lisboa, AAFDL, 2000.

AGOSTINHO, Patrícia Naré, Intrusões Corporais em Processo Penal, Coimbra, Coimbra Editora, 2014.

AJELLO, Nicholas J., Fitting a Square Peg in a Round Hole: Bitcoin, Money Laundering, and the Fifth Amendment Privilege Against Self-Incrimination, *in Brooklyn Law Review*, Vol. 80, N.º 2, Brooklyn, Brooklyn Law School, 2015, pp. 435-461.

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

ALEXANDRINO, José Melo, A Estruturação do Sistema de Direitos, Liberdades e Garantias na Constituição Portuguesa: A Construção Dogmática, Volume II, Coimbra, Almedina, 2006.

ALEXANDRINO, José Melo, Direitos Fundamentais: Introdução Geral, 2.ª Edição, Lisboa, Principia, 2015.

ALEXY, Robert, Direitos Fundamentais e Princípio da Proporcionalidade, *in O Direito*, Ano 146.º, N.º 4, Coimbra, Almedina, 2014, pp. 817-834.

ALEXY, Robert, Teoría de Los Derechos Fundamentales, 2.ª Edição, Madrid, Centro de Estudios Politicos y Constitucionales, 2008.

ALLEN, Ronald J., MACE, M. Kristin, The Self-Incrimination Clause Explained and Its Future Predicted, *in Journal of Criminal Law and Criminology,* Vol. 94, N.º 2, Chicago, Northwestern University School of Law, 2004, pp. 243-294.

AMBOS, Kai, Las Prohibiciones de Utilización de Pruebas en el Proceso Penal Alemán, *in Prueba y Proceso Penal: Análisis especial de la prueba prohibida en el sistema español y en el derecho comparado*, Valencia, Tirant lo Blanch, 2008, pp. 325-360.

ANASTÁCIO, Catarina, O Dever de Colaboração no Âmbito dos Processos de Contra-Ordenação por Infracção às Regras de Defesa da Concorrênia e o Princípio *Nemo Tenetur Se Ipsum Accusare*, *in Revista de Concorrência e Regulação,* Ano 1, Número 1, Janeiro-Março, Coimbra, Almedina, 2010, pp. 199-235.

ANDRADE, Catarina Almeida, O Princípio da Não Auto-Inculpação e sua concatenação com o dever de colaboração do arguido: especificidades em torno das ordens de desencriptação ou de revelação de palavra-passe, Lisboa, Faculdade de Direito da Universidade Católica Portuguesa, 2014.

ANDRADE, Manuel Domingues de, Noções Elementares de Processo Civil, Revista e Actualizada, Coimbra, Coimbra Editora, 1979.

ANDRADE, Maria Paula Gouveia, Prática de Direito Processual Penal: Questões Teóricas e Hipóteses Resolvidas, Lisboa, Quid Juris, 2010.

ANDREWS, Sarah, Who Holds the Key? A Comparative Study of US and European Encryption Policies, *in The Journal of Information, Law and Technology*, Ano 2000, N.º 2, Coventry, University of Warwick, 2000, pp. 207-242.

App Store Support – Apple Developer. Disponível em: https://developer.apple.com/support/app-store/

Apple Support – About Touch ID security on iPhone and iPad. Disponível em: https://support.apple.com/en-us/HT204587

ASCENSÃO, José de Oliveira, Interpretação das Leis: Integração de Lacunas – Aplicação do Princípio da Analogia, *in Revista da Ordem dos Advogados*, Ano 57, N.º 3, Dezembro, Lisboa, 1997, pp. 913-941.

ASHWORTH, Andrew, Self-Incrimination in European Human Rights Law: A Pregnant Pragmatism? *in Cardozo Law Review*, Volume 30, N.º 3, Dezembro, Washington, Washington & Lee Law School, 2008, pp.751-773

ATWOOD, J. Riley, The Encryption Problem: Why the Courts and Technology are Creating a Mess for Law Enforcement, *in Saint Louis University Public Law Review*, Vol. 34, N.º 407, Saint Louis, Saint Louis University, 2015, pp. 407-433.

BALES, Chase, Unbreakable: The Fifth Amendment and Computer Passwords, *in Arizona State Law Journal*, Vol. 44, Arizona, Arizona State University, 2012, pp. 1293-1314.

BENEVIDES, Electra Almeida, Reflexões sobre a privacidade na era cibernética, Lisboa, Faculdade de Direito de Lisboa, 2002.

BERGER, Mark, American Perspectives on Self-Incrimination and the Compelled Production of Evidence, *in The International Journal of Evidence and Proof*, Vol. 6, N.º 4, Oxford, Vathek Publishing, 2002, pp. 218-242.

BLUE, Violet, How Armenian gangsters blew up the fingerprint-password debate, 2016. Disponível em: https://www.engadget.com/2016/05/06/how-armenian-gangsters-blew-up-the-fingerprint-password-debate/

BODI, Anna, Phones, Fingerprints and Fifth Amendment, 2015. Disponível em: http://www.americancriminallawreview.com/aclr-online/phones-fingerprints-and-fifth-amendment/

BONIN, Adam C., Protecting Protection: First and Fifth Amendment Challenges to Cryptography Regulation, *in University of Chicago Legal Forum*, Vol. 1996, N.º 1, Chicago, University of Chicago, 1996, pp. 495-517.

CASEY, Eoghan, Practical Approaches to Recovering Encrypted Digital Evidence, *in International Journal of Digital Evidence*, Vol. 1, N.º 3, Delhi, Research India Publications, 2002, pp. 103-128.

CASTANHEIRA NEVES, António, Sumários de Processo Criminal: 1967-1968, Coimbra, 1968.

CAUTHEN, Robert, The Fifth Amendment and Compelling Unencrypted Data, Encryption Codes and/or Passwords, *in The Federal Law Enforcement Informer*, Março, Georgia, Federal Law Enforcement Training Centers, 2016, pp. 4-9.

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.

CHU, Vivian, RAJENDRAN, Gayathri, Use of Biometrics, *in TechCast Article Series*, The George Washington University, 2009. Disponível em: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.363.739

CLEMENS, Aaron M., No Computer Exception to the Constitution: The Fifth Amendment Protects Against Compelled Prodution of an Encrypted Document or Private Key, *in Journal of Law and Technology*, Vol. 8, N.º1, California, University of California School of Law, 2004, pp. 1-27.

COLARUSSO, David, Heads in the Cloud, a Coming Storm the Interplay of Cloud Computing, Encryption, and the Fifth Amendment's Protection Against Self-Incrimination, *in Journal of Science & Technology Law*, Vol. 17, N.º 1, Boston, Boston University School of Law, 2011, pp. 132-168.

CORCORAN, Peter, COSTACHE, Claudia, Biometric Technology and Smartphones, *in IEEE Consumer Electronics Magazine*, Vol. 5, N.º 2, New York, IEEE Consumer Electronics Society, 2016, pp. 70-78.

CORREIA, João Conde, Contributo para a Análise da Inexistência e das Nulidades Processuais Penais, Coimbra, Coimbra Editora, 1999b.

CORREIA, João Conde, Prova Digital: As Leis que Temos e a Lei que Devíamos Ter, *in Revista do Ministério Público*, Ano 35, N.º 139, Julho-Setembro, Coimbra, Coimbra Editora, 2014, pp. 29-59.

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

COSTA ANDRADE, Manuel da, Nemo Tenetur Se Ipsum Accusare e Direito Tributário: ou a insustentável indolência de um Acórdão (n.º 340/2013) do Tribunal Constitucional, *in Revista de Legislação e de Jurisprudência*, Ano 144, N.º 3989, Novembro-Dezembro, Coimbra, Coimbra Editora, 2014, pp.121-157.

COSTA ANDRADE, Manuel da, Sobre as Proibições de Prova em Processo Penal, Coimbra, Coimbra Editora, 1992.

COSTA ANDRADE, Manuel, "Bruscamente no Verão Passado": A Reforma do Código de Processo Penal – Observações críticas sobre uma Lei que podia e devia ter sido diferente, Coimbra, Coimbra Editora, 2009.

COSTA, Joana, O Princípio *Nemo Tenetur* na Jurisprudência do Tribunal Europeu dos Direitos do Homem, *in Revista do Ministério Público*, Ano 32, N.º 128, Outubro-Dezembro, Lisboa, 2011, pp. 117-183.

CRAIGER, J. Philip, SWAUGER, Jeff, MARBERRY, Chris, Digital Evidence Obfuscation: Recovery Techniques, 2005. Disponível em: http://cet4862.pbworks.com/w/file/fetch/69342454/Craiger,%20Swauger,%20and%20Marberry.pdf

CRUZ BUCHO, José Manuel, Sobre a Recolha de Autógrafos do Arguido: natureza, recusa, crime de desobediência v. direito à não auto-incriminação (notas de estudo), 2013. Disponível em: https://www.trg.pt/ficheiros/estudos/sobre_a_recolha_de_autografos_do_arguido.pdf

CRUZ, Joana Maria da, *Nemo Tenetur Se Ipsum Accusare* e a Obrigação de Sujeição a Exames, Lisboa, Faculdade de Direito da Universidade de Lisboa, 2011.

CURADO, Ana Pascoal, As Averiguações Preliminares da CMVM no Âmbito da Luta Contra a Criminaliade Financeira: Natureza Jurídica e Aplicação do Princípio *Nemo Tenetur*, *in Revista de Concorrência e Regulação*, Ano 3, Número 9, Janeiro-Março, Coimbra, Almedina, 2012, pp. 239-274.

DIAS, Maria do Carmo da Silva, Particularidades da Prova em Processo Penal: Algumas Questões Ligadas à Prova Pericial, *in Revista do CEJ*, 2.º Semestre, N.º 3, Coimbra, Almedina, 2005, pp. 169-225.

DRIPPS, Donald A., Self-incrimination, *in Heritage Guide to the Constitution*, Washington D.C., D. Forte & M. Spalding, eds., 2005, pp. 335-337.

DUONG, John, The Intersection of the Fourth and Fifth Amendments in the Context of Encrypted Personal Data at the Border, *in Drexel Law Review*, Vol. 2, N.º1, Virginia, Washington and Lee University Law School, 2009, pp. 313-359.

DWORKIN, Ronald, Taking Rights Seriously, London, Duckworth, 1977.

ENGEL, Joshua A., Rethinking the Application of the Fifth Amendment to Passwords and Encryption in the Age of Cloud Computing, *in Whittier Law Review*, Vol. 3, N.º 3, 2012, pp. 101-127.

FAKHOURY, Hanni, A Combination or a Key? The Fifth Amendment and Privilege Against Compelled Decryption, *in Digital Evidence and Electronic Signature Law Review*, N.º 9, Bedfordshire, Pario Communications Limited, 2012, pp. 81-87.

FARAHANY, Nita A., Incriminating Thoughts, *in Public Law and Legal Theory Working Papers*, Vol. 64, Chicago, Vanderbilt University Law School, 2012, pp. 351-408.

FARIVAR, Cyrus, Woman ordered to provide her fingerprint to unlock seized iPhone, 2016. Disponível em: http://arstechnica.com/tech-policy/2016/05/should-the-govt-be-able-to-force-you-to-open-your-phone-with-just-your-fingerprint/

FELDMAN, Robin, Considerations on the Emerging Implementation of Biometric Technology, *in Hastings Communications and Entertainment Law Journal*, Vol. 25, N.º 3-4, California, Hastings College of the Law, 2003, pp. 101-128.

FERMINO, David W., FEUCHTBAUM, Louis P., The law's breakable protections for unbreakable encryption, 2016. Disponível em: http://www.law.com/sites/articles/2016/06/23/the-laws-breakable-protections-for-unbreakable-encryption/

FIDALGO, Sónia, Determinação do Perfil Genético como Meio de Prova em Processo Penal, *in Revista Portuguesa de Ciência Criminal*, Ano 16, N.º 1, Janeiro-Março, Coimbra, Coimbra Editora, 2006, pp. 115-148.

FIGUEIREDO DIAS, Jorge de, COSTA ANDRADE, Manuel da, Poderes de Supervisão, Direito ao Silêncio e Provas Proibidas (Parecer), *in Supervisão, Direito ao Silêncio e Legalidade da Prova*, Coimbra, Almedina, 2009, pp. 11-56.

FIGUEIREDO DIAS, Jorge de, Direito Processual Penal, 1.ª Edição, Reimpressão, Coimbra, Coimbra Editora, 2004.

FIGUEIREDO DIAS, Jorge de, O Processo Penal Português: Problemas e Prospectivas, *in* AA.VV., *Que futuro para o direito processual penal? – Simpósio em homenagem a*

Jorge de Figueiredo Dias por ocasião dos 20 anos do Código de Processo Penal português, Coimbra, Coimbra Editora, 2009, pp. 805-819.

FIGUEIREDO DIAS, Jorge de, Sobre os Sujeitos Processuais no Novo Código de Processo Penal, *in Jornadas de Direito Processual Penal: O Novo Código de Processo Penal*, Centro de Estudos Judiciários, Coimbra, Coimbra Almedina, 1997, pp. 3-34.

FOX-BREWSTER, Thomas, Feds Walk Into A Building, Demand Everyone's Fingerprints To Open Phones, 2016. Disponível em: http://www.forbes.com/sites/thomasbrewster/2016/10/16/doj-demands-mass-fingerprint-seizure-to-open-iphones/#46075ff48d9d

FRUITERMAN, Erica, Upgrading the Fifth Amendment: New Standards for Protecting Encryption Passwords, *in Temple Law Review*, Vol. 85, N.º 3, Philadelphia, Temple University Beasley School of Law, 2013, pp. 655-689.

GARFINKEL, Simson, The iPhone has Passed a Key Security Threshold, 2012. Disponível em: https://www.technologyreview.com/s/428477/the-iphone-has-passed-a-key-security-threshold/

GARRETT, Francisco de Almeida, Sujeição do Arguido a Diligências de Prova e Outros Temas, Porto, Fronteira do Caos Editores, 2007.

GELB, Alan, CLARK, Julia, Identification for Development: The Biometrics Revolution, Washington D.C., Center for Global Development, 2013.

GEORGE, Esther, MASON, Stephen, Obtaing Evidence from Mobile Devices and the Cloud, *in Computer and Telecommunications Law Review*, Volume 21, Issue 8, London, Sweet & Maxwell, 2015, pp. 245-252.

GERSHOWITZ, Adam M., Password Protected? Can a Password Save Your Cell Phone from the Search Incident to Arrest Doctrine? *in Iowa Law Review*, University of Houston Law Center, 2010. Disponível em: https://papers.ssrn.com/sol3/papers2.cfm?abstract_id=1669403

GIROTTO, Sabina, Biometria e Nanomedicina: Le Nuove Frontiere Della Riconcettualizzazione Tecnologica del Corpo Umano, *in La Nuova Giurisprudenza Civile Commentata*, Ano 25, N.º 9, Milano, CEDAM, 2009, pp. 452-459.

GOLDMAN, Kara, Biometric Passwords and the Privilege Against Self-Incrimination, *in Cardozo Arts & Entertainment Law Journal*, Vol. 33, N.º 2, New York, Benjamin N. Cardozo School of Law, 2015, pp. 211-236.

GOMES CANOTILHO, J. J., Direito Constitucional e Teoria da Constituição, Reimpressão da 7.ª Edição, Coimbra, Almedina, 2016.

GOMES CANOTILHO, J. J., MOREIRA, Vital, Constituição da República Portuguesa Anotada, Volume I, Reimpressão, Coimbra, Coimbra Editora, 2014.

GOMES CANOTILHO, J. J., MOREIRA, Vital, Fundamentos da Constituição, Coimbra, Coimbra Editora, 1991.

GÖSSEL, Karl-Heinz, As Proibições de Prova no Direito Processual Penal da República Federal da Alemanha, *in Revista Portuguesa de Ciência Criminal*, Ano 2, N.º 3, Julho-Setembro, Lisboa, Aequitas Editora, 1992, pp. 397-441.

GREENBERG, Andy, German Hacker Group Says It's Broken The iPhone's TouchID Fingerprint Reader, 2013. Disponível em: http://www.forbes.com/sites/andygreenberg/2013/09/22/german-hackers-say-theyve-broken-the-iphones-touchid-fingerprint-reader/#2a8d881167c4

HADDAD, Carlos Henrique Borlido, Conteúdo e Contornos do Princípio Contra a Auto-Incriminação, Belo Horizonte, Faculdade de Direito da Universidade Federal de Minas Gerais, 2003.

HAMILTON, Matt, WINTON, Richard, The government wants your fingerprint to unlock your phone. Should that be allowed? 2016. Disponível em: http://www.latimes.com/local/california/la-me-iphones-fingerprints-20160430-story.html

HOYOS LABS, Guaranteeing Identity With Biometric Authentication: Exploring the Role of Mobile Authentication in Fraud Litigation, One You Benelux, Houten, 2016. Disponível em: http://pimn-public.sharepoint.com/Documentatie/2016-06-10-idm-Hoyos-Labs-Guaranteeing-identity-with-biometric-authentication.pdf

HUDMAN, Katheryn, Virginia v. Baust, *in Intellectual Property Law Bulletin*, Vol. 19, n.º 215, 2015, pp. 213-214.

HUSTLE, Rob, Biometrics and the Constitution: Why Fingerprints are Less Secure than Passwords, 2014. Disponível em: http://rebelpundit.com/biometrics-and-the-constitution-why-fingerprints-are-less-secure-than-passwords/

JAFFER, Jamil N., ROSENTHAL, Daniel J., Decrypting Our Security: A Bipartisan Argument for a Rational Solution to the Encryption Challenge, *in Catholic University Journal of Law and Technology*, Vol. 24, N.º 2, Washington D.C., The Catholic University of America, 2016, pp. 273-317.

JARONE, Joseph, An Act of Decryption Doctrine: Clarifying the Act of Production Doctrine's Application to Compelled Decryption, *in FIU Law Review*, Vol. 10, N.º 2, Florida, Florida International University College of Law, 2015, pp. 767-802.

JESUS, Francisco Marcolino de, Os Meios de Obtenção da Prova em Processo Penal, Coimbra, Almedina, 2015.

KAMISAR, Yale, LAFAVE, Wayne, ISRAEL, Jerold, KING, Nancy, KERR, Orin, PRIMUS, Eve, Modern Criminal Procedure: Cases, Comments & Questions, 14.ª Edição, Minnesota, West Academic, 2015.

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

KERR, Orin, Virginia state trial court ruling on the Fifth Amendment and smart phones, 2014. Disponível em: https://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/11/03/virginia-state-trial-court-ruling-on-the-fifth-amendment-and-smart-phones/?utm_term=.399c18bf1a04

KIOK, Jeffrey, Missing the Metaphor: Compulsory Decryption and the Fifth Amendment, *in Boston University Public Interest Law Journal*, Vol. 24, N.º 1, Boston University School of Law, Boston, 2015, pp. 53-79.

KOOPS, Bert-Jaap, Cybercrime Legislation in the Netherlands, *in Electronic Journal of Comparative Law*, Vol. 14, N.º 3, Dezembro, Tilburg, Tilburg Institute for Law, Technology and Society, 2010, pp. 595-633.

LARKIN, John E. D., Compelled Production of Encrypted Data, *in Vanderbilt Journal of Entertainment and Technology Law*, Volume 14, N.º 2, Tennessee, Vanderbilt Law School, 2012, pp. 253-278.

LEHTINEN, Rick, GANGEMI, G. T., Computer Security Basics, 2.ª Edição, California, O'Reilly Media, 2006.

LOWMAN, Sarah, The Effect of File and Disk Encryption on Computer Forensics, 2010. Disponível em: https://www.lowmanio.co.uk/share/The%20Effect%20of%20File%20and%20Disk%20Encryption%20on%20Computer%20Forensics.pdf

MARQUES DA SILVA, Germano, Curso de Processo Penal, Volume I, 6.ª Edição, Revista e Actualizada, Lisboa, Verbo, 2010.

MARQUES DA SILVA, Germano, Curso e Processo Penal, Volume II, 5.ª Edição, Lisboa, Verbo, 2011.

MARQUES DA SILVA, Germano, Direito Processual Penal Português: Noções Gerais – Sujeitos Processuais e Objecto, Volume I, Lisboa, Universidade Católica Portuguesa, 2013.

MARQUES DA SILVA, Germano, Produção e Valoração da Prova em Processo Penal, *in Revista do CEJ*, 1.º Semestre, N.º 4, Coimbra, Almedina, 2006, pp. 37-53.

MARQUES, J. A. Garcia, MARTINS, A. G. Lourenço, Direito da Informática, 2ª Edição Refundida e Actualizada, Coimbra, Almedina, 2006.

MARTINEZ, Soares, Comentários à Constituição Portuguesa de 1976, Lisboa, Verbo, 1992.

MARTINS, A. G. Lourenço, MARQUES, J. A. Garcia, DIAS, Pedro Simões, Cyberlaw em Portugal: O Direito das Tecnologias da Informação e da Comunicação, Lisboa, Centro Atlântico, 2004.

MARTINS, Paulo Amaral, *Nemo Tenetur Se Ipsum Accusare* e a Obrigação de Sujeição a Exames, Lisboa, Instituto Superior de Ciências Policiais e Segurança Interna, 2015.

MATHUR, Akanksha, An ASCII Value Based Data Encryption Algorithm and its Comparison With Other Symmetric Data Encryption Algorithms, *in International Journal on Computer Science and Engineering*, Vol. 4, N.º 9, Tamil Nadu, India, IJCSE Managing Editor, 2012, pp. 1650-1657.

MATLIN, Margaret W., FARMER, Thomas A., Cognition, 9.ª Edição, New Jersey, Wiley, 2015.

McCARTHY, Hugh J., Decoding the Encryption Debate: Why Legislating to Restrict Strong Encryption Will Not Resolve the "Going Dark" Problem, *in Journal of Internet Law,* Vol. 20, N.º 3, New York, Wolters Kluwer, 2016, pp. 17-39.

MENEZES, Sofia Saraiva de, O Direito ao Silêncio: A verdade por trás do mito, *in Prova Criminal e Direito de Defesa: Estudos sobre teoria da prova e garantias de defesa em processo penal*, Coimbra, Almedina, 2010, pp. 117-136.

MESQUITA, Paulo Dá, A Prova do Crime e o Que Se Disse Antes do Julgamento: Estudo sobre a prova no processo penal português à luz do sistema norte-americano, Coimbra, Coimbra Editora, 2011.

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

MILITÃO, Renato Lopes, A Propósito da Prova Digital no Processo Penal, *in Revista da Ordem dos Advogados,* Ano 72, N.º 1, 2012, pp. 247-283.

MIRANDA, Jorge, Manual de Direito Constitucional: Direitos Fundamentais, Volume II, Tomo IV, 5.ª Edição, Coimbra, Coimbra Editora, 2014.

MIRANDA, Jorge, MEDEIROS, Rui, Constituição Portuguesa Anotada, Tomo I, 2.ª Edição, Revista, Actualizada e Ampliada, Coimbra, Coimbra Editora, 2010.

MIRANDA, Jorge, Os Direitos Fundamentais e o Terrorismo: Os Fins Nunca Justificam os Meios, Nem Para Um Lado, Nem Para Outro, *in Revista do Tribunal Regional Federal*, 3.ª Região, N.º 75, Janeiro-Fevereiro, São Paulo, Thomson IOB, 2006, pp. 89-104.

MOHAN, Vivek, VILLASENOR, John, Decrypting the Fifth Amendment: The Limits of Self-Incrimination in the Digital Era, *in Journal of Constitutional Law Heightened Scrutiny*, Vol. 15, Pennsylvania, University of Pennsylvania Law School, 2012, pp. 11-28.

MONIZ, Helena, A Base de Dados de Perfis de ADN para Fins de Identificação Civil e Criminal e a Cooperação Transfronteiras em Matéria de Transferência de Perfis de ADN, *in Revista do Ministério Público,* Ano 30, N.º 120, Outubro-Dezembro, Lisboa, Editorial Minerva, 2009, pp. 145-156.

MONTE, Mário Ferreira, O Resultado da Análise de Saliva Colhida através de Zaragatoa Bucal é Prova Proibida? *in Revista do Ministério Público*, Ano 27. N-º 108, Outubro-Dezembro, Lisboa, Editorial Minerva, 2006, pp. 239-262.

MORAIS, Inês Santos, A Apreensão de Correio Electrónico em Processo Penal: dos direitos fundamentais às ingerências, constitucional e legalmente legitimadas, nas comunicações, Dissertação de Mestrado Profissionalizante em Ciências Jurídico-Forenses, Lisboa, Faculdade de Direito de Lisboa, 2012.

MORÃO, Helena, Efeito-à-Distância das Proibições de Prova e Declarações Confessórias: O Acórdão n.º 198/2004 do Tribunal Constitucional e o Argumento "The Cat is Out of the Bag", *in Revista Portuguesa de Ciência Criminal*, Ano 22, N.º 4, Outubro-Dezembro, Coimbra, Coimbra Editora, 2012, pp. 689-726.

MORÃO, Helena, O Efeito-à-Distância das Proibições de Prova no Direito Processual Penal Português, *in Revista Portuguesa de Ciência Criminal*, Ano 16, N.º 4, Outubro-Dezembro, Coimbra, Coimbra Editora, 2006, pp. 575-620.

MORRISON, Caren Myers, Passwords, Profiles, and the Privilege Against Self-Incrimination: Facebook and the Fifth Amendment, *in Arkansas Law Review*, Vol. 65, Georgia, Georgia State University College of Law, 2012, pp. 133-162.

MOURAZ LOPES, José, e ANTÃO CABREIRO, Carlos, A Emergência da Prova Digital na Investigação da Criminalidade Informática, *in Sub Judice – Justiça e Sociedade*, n.º 35, Abril-Junho, Coimbra, Coimbra Editora, 2006, pp. 71-79.

MUKASEY, Michael B., SEDGWICK, Jeffrey L., HAGY, David W., Electronic CSI, A Guide for First Responders, 2ª Edição, Washington, National Institute of Justice, 2008.

NATIONAL SCIENCE AND TECHNOLOGY COUNCIL, Fingerprint Recognition, Committee on Technology, Committee on Homeland and National Security, Subcommittee on Biometrics, Executive Office of the President of the United States, 2006. Disponível em: https://www.fbi.gov/file-repository/about-us-cjis-fingerprints_biometrics-biometric-center-of-excellences-fingerprint-recognition.pdf/view

NETO, Luísa, O Direito Fundamental à Disposição Sobre o Próprio Corpo: A relevância da vontade na configuração do seu regime, Coimbra, Coimbra Editora, 2004.

NETO, Theodomiro Dias, O Direito ao Silêncio: Tratamento nos Direitos Alemão e Norte-Americano, *in Revista Brasileira de Ciências Criminais,* Ano 5, N.º 19, Julho-Setembro, São Paulo, Editora Revista dos Tribunais LTDA., 1997, pp. 179-204.

NEVES, Rita Castanheira, As Ingerências nas Comunicações Electrónicas em Processo Penal: Natureza e Respectivo Regime Jurídico do Correio Electrónico Enquanto Meio de Obtenção de Prova, Coimbra, Coimbra Editora, 2011.

NEVES, Rita Castanheira, CORREIA, Hélder Santos, A Lei do Cibercrime e a Colaboração do Arguido no Acesso aos Dados Informáticos, *in Actualidad Jurídica Uría Menéndez*, N.º 38, Madrid, Dykinson, S.L., 2014, pp. 146-149.

OCDE, Biometric-based Technologies, 2004. Disponível em: http://www.oecd-ilibrary.org/docserver/download/232075642747.pdf?expires=1481644102&id=id&accname=guest&checksum=B1A21B7898A864D5763D4AB7F7310AFA

OLIVEIRA SILVA, Sandra, Legalidade da Prova e Provas Proibidas, *in Revista Portuguesa de Ciência Criminal*, Ano 21, N.º 4, Outubro-Dezembro, Coimbra, Coimbra Editora, 2011, pp. 545-591.

OLIVEIRA SILVA, Sandra, O Arguido como Meio de Prova Contra Si Mesmo, *in Revista da Faculdade de Direito da Universidade do Porto,* Ano 10, Porto, Faculdade de Direito da Universidade do Porto, 2013, pp. 361-379.

OLIVEIRA SILVA, Sandra, O Arguido como Meio de Prova Contra Si Mesmo: Considerações em torno do princípio *nemo tenetur se ipsum accusare*, Porto, Faculdade de Direito da Universidade do Porto, 2015.

OLIVEIRA, Francisco da Costa, A Defesa e a Investigação do Crime: Guia prático para a análise da investigação judiciária e para a investigação pelos recursos próprios da defesa criminal, 2.ª Edição, Coimbra, Almedina, 2008.

PAGLIERY, Jose, FBI wasn't able to unlock iPhone, even with a 'fingerprint unlock warrant', 2016. Disponível em: http://money.cnn.com/2016/05/12/technology/fbi-fingerprint-iphone/

PALFREYMAN, Brendan M., Lessons from the British and American Approaches to Compelled Decryption, *in Brooklyn Law Review,* Vol. 75, N.º 1, Brooklyn, Brooklyn Law School, 2009, pp. 345-378.

PALMA, Maria Fernanda, O Direito à Não Auto-Incriminação, *in Boletim Informativo*, Ano 1, Edição n.º 1, Dez. 2008/Jan. 2009, Lisboa, Instituto de Direito Penal e Ciências Criminais, 2009. Disponível em: http://www.idpcc.pt/xms/files/Newsletters/Boletim_Ano1_Ed1_Dez08Jan09.pdf

PATO, Joseph N., MILLETT, Lynette I., Biometric Recognition: Challenges and Opportunities, Washington D.C., The National Academies Press, 2010.

PAUL, Greig, IRVINE, James, IEDs on the Road to Fingerprint Authentication: Biometrics have vulnerabilities that PINs and passwords don't, *in IEEE Consumer Electronics Magazine*, Vol. 5, N.º 2, New York, IEEE Consumer Electronics Society, 2016, pp. 79-86.

PFEFFERKORN, Riana, In re Boucher: Hard Drives Make Pretty Good Law? Encryption Passphrases as Testimonial Evidence Under the Fifth Amendment, 2009. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1883697&download=yes

PINTO, Lara Sofia, Privilégio Contra a Auto-Incriminação Versus Colaboração do Arguido – Case study: revelação coactiva da *password* para desencriptação de dados – *resistance is futile*? *in Prova Criminal e Direito de Defesa*, 2.ª Reimpressão, Coimbra, Almedina, 2013, pp. 91-116.

POTAPCHUK, John L., A Second Bite at the Apple: Federal Courts' Authority to Compel Technical Assistance to Government Agents in Accessing Encrypted Smartphone Data Under the All Writs Act, *in Boston College Law Review*, Vol. 57, N.º 4, Boston, Boston College Law School, 2016, pp. 1403-1446.

QUEIJO, Maria Elisabeth, O Direito de Não Produzir Prova Contra Si Mesmo: O princípio *nemo tenetur se detegere* e suas decorrências no processo penal, 2.ª Edição., São Paulo, Saraiva Editora, 2012.

QUELHAS, Filipa de Figueiroa, O Meio de (Obtenção de) Prova Digital Electrónica: Sua admissibilidade e relevância, em especial, face à globalização e ao uso das novas tecnologias pelas organizações criminosas, Lisboa, Faculdade de Direito da Universidade de Lisboa, 2008.

RAMALHO, David Silva, A Recolha de Prova Penal em Sistemas de Computação em Nuvem, *in Revista de Direito Intelectual*, N.º 02, Coimbra, Almedina, 2014, pp. 123-162.

RAMOS, Armando Dias, A Prova Digital em Processo Penal: O Correio Electrónico, Lisboa, Chiado Editora, 2014.

RAMOS, Vânia Costa, Corpus Juris 2000: Imposição ao Arguido de Entrega de Documentos para Prova e *Nemo Tenetur Se Ipsum Accusare*, *in Revista do Ministério Público*, Ano 28, N.º 109, Janeiro-Março, Lisboa, 2007, pp. 57-96.

RAMOS, Vânia Costa, *Nemo Tenetur Se Ipsum Accusare* e Concorrência: Jurisprudência do Tribunal de Comércio de Lisboa, *in Revista de Concorrência e Regulação,* Ano 1, Número 1, Janeiro-Março, Coimbra, Almedina, 2010, pp. 175-198.

REIS NOVAIS, Jorge, As Restrições aos Direitos Fundamentais Não Expressamente Autorizadas pela Constituição, 2.ª Edição, Coimbra, Coimbra Editora, 2010.

REIS NOVAIS, Jorge, Direitos Fundamentais e Justiça Constitucional em Estado de Direito Democrático, Coimbra, Coimbra Editora, 2012.

REIS NOVAIS, Jorge, Direitos Fundamentais: Trunfos Contra a Maioria, Coimbra, Coimbra Editora, 2006.

RISTORI, Adriana Dias Paes, Sobre o Silêncio do Arguido no Interrogatório no Processo Penal Português, Coimbra, Almedina, 2007.

RODRIGUES, Anabela Miranda, A Defesa do Arguido: Uma garantia constitucional em perigo no "admirável mundo novo", *in Revista Portuguesa de Ciência Criminal*, Ano 12, N.º 4, Outubro-Dezembro, Coimbra, Coimbra Editora, 2002, pp. 549-571.

RODRIGUES, Benjamim Silva, Da Prova Penal – Bruscamente… A(s) Face(s) Oculta(s) dos Métodos Ocultos de Investigação Criminal, Tomo II, Lisboa, Rei dos Livros, 2010.

RODRIGUES, Benjamin Silva, Da Prova Penal – A Prova Científica: Exames, Análises ou Perícias de ADN? Controlo de Velocidade, Álcool e Substâncias Psicotrópicas, Volume I, Coimbra, Coimbra Editora, 2008.

RODRIGUES, Benjamin Silva, Das Escutas Telefónicas à Obtenção da Prova [Em Ambiente Digital] – A monitorização dos fluxos informacionais e comunicacionais, Volume II, 2.ª Edição, Coimbra, Coimbra Editora, 2009b.

RODRIGUES, Benjamin Silva, Direito Penal – Parte Especial, Tomo I – Direito Penal Informático-Digital, Coimbra, Coimbra Editora, 2009a.

ROGALL, Klaus, A Nova Regulamentação da Vigilância das Telecomunicações na Alemanha, *in 2.º Congresso de Investigação Criminal*, Coimbra, Almedina, 2010, pp. 117-141.

ROSA, Luís Bértolo, Consequências Processuais das Proibições de Prova, *in Revista Portuguesa de Ciência Criminal*, Ano 20, N.º 2, Abril-Junho, Coimbra, Coimbra Editora, 2010, pp. 219-277.

ROXIN, Claus, Derecho Procesal Penal, Buenos Aires, Editores del Puerto, 2000.

ROXIN, Claus, Pasado, Presente y Futuro del Derecho Procesal Penal, Versão castelhana traduzida por Óscar Guerrero Peralta, Santa Fe, Rubinzal-Culzoni Editores, 2009.

RUBENS, Paul, Biometric Authentication: How It Works, 2012. Disponível em: http://www.esecurityplanet.com/trends/biometric-authentication-how-it-works.html

SÁ, Liliana da Silva de, O Dever de Cooperação do Contribuinte e o Direito ao Silêncio do Arguido: Impacto na Actividade Inspectiva, *in Ciência e Técnica Fiscal*, N.º 414, Julho-Dezembro, Coimbra, Almedina, 2004, pp. 171-217.

SAINTGERMAIN, Sonthonax Bolivar, Is the Battle Over for Smart-Phones? Search Warrants Cannot Overcome Biometric Protections, 2014b. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2498707

SAINTGERMAIN, Sonthonax Bolivar, Testifying by Thumbprint: Biometric Identification, Police Searches and the Privilege Against Self-Incrimination, 2014a. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2367479

SALES, Erin M., The "Biometric Revolution": An Erosion of the Fifth Amendment Privilege to Be Free from Self-Incrimination, *in University of Miami Law Review*, Vol. 69, N.º 1, Miami, University of Miami School of Law, 2014, pp. 193-240.

SANTOS, Inês Moreira, Direito Fundamental à Privacidade vs. Persecução Criminal: A problemática das escutas telefónicas, *in Tratado Luso-Brasileiro da Dignidade Humana*, 2.ª Edição, Actualizada e Ampliada, Saõ Paulo, Editora Quartier Latin do Brasil, 2009, pp. 103-126.

SHAW, Mitchell, DOJ Gets Warrant to Force People to Use Fingerprints to Unlock their Phones, 2016. Disponível em:

http://www.thenewamerican.com/usnews/constitution/item/24354-doj-gets-warrant-to-force-people-to-use-fingerprints-to-unlock-their-phones

SHERWINTER, Daniel J., Surveillance's Splippery Slope: Using Encryption to Recapture Privacy Rights, *in Journal on Telecommunications and High Technology Law*, Vol. 5, N.º 2, Colorado, Univeristy of Colorado Boulder, 2007, pp. 501-532.

SILVA DIAS, Augusto, O Direito à Não Auto-Incriminação no Âmbito das Contra-Ordenações do Código dos Valores Imobiliários, *in Revista de Concorrência e Regulação*, Ano 1, Número 1, Janeiro-Março, Coimbra, Almedina, 2010, pp. 237-265.

SILVA DIAS, Augusto, RAMOS, Vânia Costa, O Direito à Não Auto-Inculpação (*Nemo Tenetur Se Ipsum Accusare*) no Processo Penal e Contra-Ordenacional Português, Coimbra, Coimbra Editora, 2009.

SILVA, Maria de Fátima Reis, O Direito à Não Auto-Incriminação, *in Sub Judice: Justiça e Sociedade*, N.º 40, Julho-Setembro, Coimbra, Almedina, 2007, pp. 59-74.

SILVER, James, Decoding Encryption for Litigators, *in Federal Evidence Review*, Vol. 9, N.º 8, Virginia, 2012, pp. 809-814.

SIMAS SANTOS, Manuel, LEAL-HENRIQUES, Manuel, Código de Processo Penal Anotado, Volume I, 3.ª Edição, Lisboa, Rei dos Livros, 2008.

SIMAS SANTOS, Manuel, LEAL-HENRIQUES, Manuel, SIMAS SANTOS, João, Noções de Processo Penal, Lisboa, Rei dos Livros, 2010.

FERREIRA, José da Silva, Nemo Tenetur Se Ipsum Accusare: o sujeito como objecto de prova, Lisboa, Faculdade de Direito da Universidade de Lisboa, 2014.

SOARES, Nicholas, The Right to Remain Encrypted: The Self-Incrimination Doctrine in the Digital Age, *in American Criminal Law Review*, Vol. 49, N.º 4, Washington D.C., 2012, pp. 2001-2019.

SOUSA MENDES, Paulo de, As Garantias de Defesa no Processo Sancionatório Especial por Práticas Restritivas da Concorrência Confrontadas com a Jurisprudência do Tribunal Europeu dos Direitos do Homem, *in Revista de Concorrência e Regulação*, Ano 1, Número 1, Janeiro-Março, Coimbra, Almedina, 2010, pp. 121-144.

SOUSA MENDES, Paulo de, As Proibições de Prova no Processo Penal, *in Jornadas de Direito Processual Penal e Direitos Fundamentais*, Coimbra, Almedina, 2004, pp. 133-154.

SOUSA MENDES, Paulo de, Estatuto de Arguido e Posição Processual da Vítima, *in Revista Portuguesa de Ciência Criminal*, Ano 17, N.º 4, Outubro-Dezembro, Coimbra, Coimbra Editora, 2007, pp. 601-612.

SOUSA MENDES, Paulo de, Lições de Direito Processual Penal, Reimpressão, Coimbra, Almedina, 2017.

SOUSA MENDES, Paulo de, O Efeito-à-Distância das Proibições de Prova, *in Revista do Ministério Público do Rio Grande do Sul*, N.º 74, Janeiro-Abril, Porto Alegre, AMP/RS, 2014, pp. 219-228.

SOUTAR, Colin, ROBERGE, Danny, STOIANOV, Alex, GILROY, Rene, KUMAR, B. V. K. Vijaya, Biometric Encryption, 2007. Disponível em: http://www.cse.lehigh.edu/prr/Biometrics/Archive/Papers/BiometricEncryption.pdf

SPRING, Tom, Experts 'Outraged' by Warrant Demanding Fingerprints to Unlock Smartphones, 2016. Disponível em: https://threatpost.com/experts-outraged-by-warrant-demanding-fingerprints-to-unlock-smartphones/121348/

SUSANO, Helena, Escutas Telefónicas: Exigências e Controvérsias do Actual Regime, Coimbra, Coimbra Editora, 2009.

SWIRE, Peter, AHMAD, Kenesa, Encryption and Globalization, *in The Columbia Science & Technology Law Review*, Vol. 13, New York, Columbia Law School, 2012, pp. 416-481.

TABINI, Marco, Open Sesame: How iOS 8 will unlock Touch ID's power, 2014. Disponível em: http://www.macworld.com/article/2455474/open-sesame-how-ios-8-will-unlock-touch-ids-power.html

TARANTOLA, Andrew, Stop Worrying About the New iPhone's Fingerprint Scanner, 2013. Disponível em: http://gizmodo.com/stop-worrying-about-the-new-iphones-fingerprint-scanne-1326146704

TERZIAN, Dan, Forced Decryption Equilibrium, *in Northwestern University Law Review*, Vol. 109, N.º 4, Chicago, Northwestern University School of Law, 2015, pp. 1131-1140.

TERZIAN, Dan, The Fifth Amendment, Encryption, and the Forgotten State Interest, *in UCLA Law Review Discourse*, Vol. 61, California, University of California School of Law, 2014, pp. 298-312.

TERZIAN, Dan, The Micro-Hornbook on the Fifth Amendment and Encryption, *in The Georgetown Law Journal Online*, Vol. 104, N.º 168, 2016, pp. 168-174.

THOMPSON, Richard M., JAIKARAN, Chris, Encryption: Selected Legal Issues, Congressional Research Service, 2016. Disponível em: https://www.fas.org/sgp/crs/misc/R44407.pdf

UNGBERG, Andrew J., Protecting Privacy Through a Responsible Decryption Policy, *in Harvard Journal of Law & Technology*, Vol. 22, N.º 2, Massachusetts, Harvard Law School, 2009, pp. 537-558.

VAAS, Lisa, Feds got search warrant demanding anyone's fingerprints to open phones, 2016. Disponível em: https://nakedsecurity.sophos.com/2016/10/18/feds-got-search-warrant-demanding-anyones-fingerprints-to-open-phones/

VAGLE, Jeffrey L., Furtive Encryption: Power, Trust, and the Constitutional Cost of Collective Surveillance, *in Indiana Law Journal*, Pennsylvania, University of Pennsylvania Law School, 2015, pp. 101-150.

VENÂNCIO, Pedro Dias, Lei do Cibercrime: Anotada e Comentada, Coimbra, Coimbra Editora, 2011.

VERDELHO, Pedro, A Nova Lei do Cibercrime, *in Scientia Iuridica, Revista de Direito Comparado Português e Brasileiro*, Tomo LVIII, N.º 320, Outubro-Dezembro, Braga, Universidade do Minho, 2009, pp. 717-749.

VIERA DE ANDRADE, José Carlos, Os Direitos Fundamentais na Constituição Portuguesa de 1976, 5.ª Edição, Coimbra, Almedina, 2016.

VOGL, Kristen, iSearch Into the iPhone, *in Journal of Technology Law & Policy*, Vol. 20, N.º 2, Florida, Univeristy of Florida Frederic G. Levin College of Law, 2015, pp. 179-208.

VORDOGLOU, Evangelos, The Compatibility of Decryption Orders with the Right Against Self-Incrimination: Compelled Revelation of Passwords, School of Economics, Business Administration & Legal Studies, Thessaloniki, 2016. Disponível em: https://repository.ihu.edu.gr/xmlui/bitstream/handle/11544/14539/Dissertation-Final-1104130034-Vordoglou.pdf?sequence=1

WEINBERG, Kenneth P., Cryptography: "Key Recovery" Shaping Cyberspace (Pragmatism and Theory), *in Journal of Intellectual Property Law*, Vol. 5, N.º 2, Georgia, University of Georgia School of Law, 1998, pp. 667-700.

WHITTAKER, Zack, iPhone 5S Fingerprint Reader: Doubling down on identity, a death knell to passwords? 2013. Disponível em: http://www.smartsuite.in/iphone-5s-fingerprint-reader-doubling-down-on-identity-a-death-knell-to-zdnet.html

WILSON, Sarah, Compelling Passwords from Third Parties: Why the Fourth and Fifth Amendments do Not Adequately Protect Individuals When Third Parties are Forced to Hand Over Passwords, *in Berkeley Technology Law Journal*, Vol. 30, N.º 1, California, University of California, 2015, pp. 1-38.

WINKLER, Andrew T., Password Protection and Self-Incrimination: Applying the Fifth Amendment privilege in the technological era, *in Rutgers Computer & Technology Law Journal*, Volume 39, N.º 2, Setembro, Washington, Rutgers Law School, 2013, pp. 37-56.

WINTER, Lorena Bachmaier, Investigación Criminal y Protección de la Privacidad en la Doctrina del Tribunal Europeo de Derechos Humanos, *in 2.º Congresso de Investigação Criminal*, Coimbra, Almedina, 2010, pp. 161-185.

WINTERBOTTOM, Ken, Court Rules Police May Compel Suspects to Unlock Fingerprint-Protected Smartphones, 2014. Disponível em: http://jolt.law.harvard.edu/digest/telecommunications/court-rules-police-may-compel-suspects-to-unlock-fingerprint-protected-smartphones

WISEMAN, Timothy A., Encryption, Forced Decryption, and the Constitution, *in I/S: A Journal of Law and Policy for the Information Society*, Vol. 11, N.º 2, Ohio, Moritz College of Law, 2015, pp. 525-575.

WISEMAN, Timothy A., Finding the Foregone Conclusions of Encryption, 2014. Disponível em: https://works.bepress.com/timothy_wiseman/2/

WOLFSLAST, Gabriele, Beweisführung durch heimliche Tonbandaufzeichnung, NStZ, 1987.

JURISPRUDÊNCIA E PARECERES

Commonwealth of Virginia v. David Charles Baust, 2014. Disponível em: https://consumermediallc.files.wordpress.com/2014/11/245515028-fingerprint-unlock-ruling.pdf

State of Minnesota v. Matthew Vaughn Diamond, 2017. Disponível em: http://mn.gov/law-library-stat/archive/ctappub/2017/OPa152075-011717.pdf

Holt v. United States, 1910. Disponível em: https://supreme.justia.com/cases/federal/us/218/245/case.html

Riley v. California, 2014. Disponível em: https://www.supremecourt.gov/opinions/13pdf/13-132_8l9c.pdf

Minnesota v. Murphy, 1984. Disponível em: https://supreme.justia.com/cases/federal/us/465/420/case.html

Fisher v. United States, 1976. Disponível em: https://supreme.justia.com/cases/federal/us/425/391/case.html

Schmerber v. California, 1966. Disponível em: https://supreme.justia.com/cases/federal/us/384/757/case.html

United States v. Doe, 1984. Disponível em: https://supreme.justia.com/cases/federal/us/465/605/

United States v. Washington, 1977. Disponível em: https://supreme.justia.com/cases/federal/us/431/181/case.html

Kastigar v. United States, 1972. Disponível em: https://supreme.justia.com/cases/federal/us/406/441/case.html

United States v. Hubbel, 2000. Disponível em: https://supreme.justia.com/cases/federal/us/530/27/case.html

Hoffman v. United States, 1951. Disponível em: https://supreme.justia.com/cases/federal/us/341/479/case.html

Doe v. United States, 1988. (Doe II) Disponível em: https://supreme.justia.com/cases/federal/us/487/201/

United States v. Kirschner, 2010. Disponível em: https://www.ravellaw.com/opinions/789d10be33066b73e4377a26bf5c574a

United States v. Doe, 2011. (Doe III) Disponível em: http://law.justia.com/cases/federal/appellate-courts/F3/112/910/585109/

In re Grand Jury Subpoena to Sebastien Boucher, 2009. Disponível em: http://volokh.com/files/BoucherDCT.1.pdf

United States v. Wade, 1967. Disponível em https://supreme.justia.com/cases/federal/us/388/218/case.html

United States v. Dionisio, 1973. Disponível em: https://supreme.justia.com/cases/federal/us/410/1/case.html

Gilbert v. California, 1967. Disponível em: http://supreme-court-cases.insidegov.com/l/2630/Gilbert-v-California

United States v. Fricosu, 2012. Disponível em: https://www.wired.com/images_blogs/threatlevel/2012/01/decrypt.pdf

Commonwealth v. Gelfgatt, 2014. Disponível em: http://law.justia.com/cases/massachusetts/supreme-court/2014/sjc-11358.html

United States v. Gavegnano, 2012. Disponível em: http://federalevidence.com/pdf/Comput/U.S.%20v.%20Gavegnano.pdf

United States v. Hatfield, 2010. Disponível em: http://caselaw.findlaw.com/us-7th-circuit/1519786.html

Acórdão do Tribunal da Relação de Guimarães, de 29 de Março de 2011, disponível em: http://www.dgsi.pt/jtrg.nsf/86c25a698e4e7cb7802579ec004d3832/6aa96edf91e899b2802578a00054631f?OpenDocument

Acórdão do Tribunal da Relação de Lisboa, de 11 de Janeiro de 2011, disponível em: http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/e5ed1936deb44eb180257824004ab09d?OpenDocument

Acórdão do Tribunal Constitucional n.º 304/2004, de 5 de Maio de 2004, disponível em: http://www.tribunalconstitucional.pt/tc/acordaos/20040304.html

Acórdão do Tribunal da Relação de Coimbra, de 23 de Outubro de 2013, disponível em: http://www.dgsi.pt/jtrc.nsf/c3fb530030ea1c61802568d9005cd5bb/d3a8f7db2f94ad6180257c0f0052958b?OpenDocument

Acórdão do Tribunal Constitucional n.º 340/2013, de 17 de Junho de 2013, disponível em: http://www.tribunalconstitucional.pt/tc/acordaos/20130340.html

Acórdão do Tribunal da Relação de Évora, de 30 de Setembro de 2008, disponível em: http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/986b0759b8e0108880257de100574d46?OpenDocument

Acórdão do Tribunal Constitucional n.º 696/95, de 5 de Dezembro de 1995, disponível em: http://www.tribunalconstitucional.pt/tc/acordaos/19950695.html

Acórdão do Tribunal Constitucional n.º 372/98, de 13 de Maio de 1998, disponível em: http://www.tribunalconstitucional.pt/tc/acordaos/19980372.html

Parecer do Conselho Consultivo da Procuradoria Geral da República, P000642006, de 2 de Novembro de 2006, disponível em: http://www.ministeriopublico.pt/iframe/pareceres-do-conselho-consultivo-da-pgr

Acórdão do Tribunal da Relação de Lisboa, de 3 de Março de 2016, disponível em: http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/36f34b50b321b89980257f6f004d5fc6?OpenDocument

Acórdão Saunders v. Reino Unido, de 17 de Dezembro de 1996, disponível em: http://hudoc.echr.coe.int/webservices/content/pdf/001-58009?TID=thkbhnilzk

Acórdão Quinn v. Irlanda, de 21 de Dezembro de 2000, disponível em: http://hudoc.echr.coe.int/eng#{"itemid":["001-59098"]}

Acórdão P.G. e J.H. v. Reino Unido, de 25 de Setembro de 2001, disponível em: http://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=002-5500&filename=002-5500.pdf&TID=ihgdqbxnfi

Acórdão Shannon v. Reino Unido, de 4 de Outubro de 2005, disponível em: http://hudoc.echr.coe.int/webservices/content/pdf/001-70364?TID=ihgdqbxnfi

Acórdão Jalloh v. Alemanha, de 11 de Julho de 2006, disponível em: https://wcd.coe.int/ViewDoc.jsp?p=&id=1018815&Site=COE&direct=true

Acórdão do Tribunal Constitucional n.º 155/2007, de 2 de Março de 2007, disponível em: http://www.tribunalconstitucional.pt/tc/acordaos/20070155.html

Acórdão do Tribunal da Relação de Évora, de 15 de Novembro de 2011, disponível em: http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/3475e69cdc8de87380257de10056f84a?OpenDocument

Acórdão do Tribunal da Relação de Évora, de 21 de Abril de 2015, disponível em: http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/21398dcfc4605f1980257e43003306a9?OpenDocument

Acórdão do Tribunal da Relação de Évora, de 11 de Outubro de 2011, disponível em: http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/3693bad042ba17bb80257de10056f62e?OpenDocument

Acórdão do Tribunal da Relação do Porto, de 28 de Janeiro de 2009, disponível em: http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/f861aadc84da529a8025754e0054040e?OpenDocument

Acórdão do Tribunal da Relação do Porto, de 10 de Dezembro de 2008, disponível em: http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/673fcb5dc0168da6802575220056a553?OpenDocument

Acórdão do Tribunal da Relação de Lisboa, de 17 de Abril de 2012, disponível em: http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/849980283d233cfd802579e6004e401f?OpenDocument

Acórdão do Supremo Tribunal de Justiça n.º 14/2014, de 21 de Outubro de 2014, disponível em: https://dre.pt/application/file/58512485

Silverthorne Lumber Co. v. United States, 1920. Disponível em: https://supreme.justia.com/cases/federal/us/251/385/case.html

Wong Sun v. United States, 1963. Disponível em: https://supreme.justia.com/cases/federal/us/371/471/case.html

Segura v. United States, 1984. Disponível em: https://supreme.justia.com/cases/federal/us/468/796/

Brewer v. Williams, 1977. Disponível em: https://supreme.justia.com/cases/federal/us/430/387/

Nix v. Williams, 1984. Disponível em: https://supreme.justia.com/cases/federal/us/467/431/case.html

United States v. Ceccolini, 1978. Disponível em: https://supreme.justia.com/cases/federal/us/435/268/

Acórdão do Tribunal Constitucional n.º 198/2004, de 24 de Março de 2004, disponível em: http://www.tribunalconstitucional.pt/tc/acordaos/20040198.html

Decisão Sumária do Tribunal Constitucional n.º 13/2008, de 11 de Janeiro de 2008, disponível em: http://www.tribunalconstitucional.pt/tc/decsumarias/20080013.html

ANEXOS

Anexo I – Caso Commonwealth of Virginia v. David Charles Baust

COMMONWEALTH OF VIRGINIA

EDWARD W. HANSON, JR.
A. BONWILL SHOCKLEY
H. THOMAS PADRICK, JR.
STEPHEN C. MAHAN
WILLIAM R. O'BRIEN
LESLIE L. LILLEY
GLENN R. CROSHAW
STEVEN C. FRUCCI

CIRCUIT COURT JUDGES OFFICE
CITY OF VIRGINIA BEACH
JUDICIAL CENTER, BLDG. 10
2425 NIMMO PARKWAY
VIRGINIA BEACH, VA 23456-9017
(757) 385-4501
www.vbgov.com/courts
Direct Dial # 385-8680

SECOND JUDICIAL CIRCUIT

October 28, 2014

Eleanor Gaines, Esquire
Office of the Commonwealth's Attorney
2425 Nimmo Parkway
Building 10B, Second Floor
Virginia Beach, VA 23456

James O. Broccoletti, Esquire
Zoby, Broccoletti & Normile, P. C.
6633 Stoney Point South
Norfolk, VA 23502

Re: Commonwealth of Virginia v. David Charles Baust
Docket No.: CR14-1439

Dear Counsel:

This matter is before the court on the Commonwealth's Motion to Compel the Production of the Passcode or Fingerprint to Encrypted Smartphone. The hearing took place Tuesday, October 28, 2014, at which the Defendant, the Commonwealth, and the witness for the Commonwealth were present. For the reasons set forth below, the Motion is denied in part and granted in part.

David Charles Baust, Defendant, is charged by indictment with violating Code of Virginia § 18.2-51.6, Strangling Another Causing Wounding or Injury. On February 19, 2014, Defendant allegedly assaulted the victim in his bedroom at his house. The victim stated that Defendant maintained a recording device that continuously recorded in the room where the assault purportedly took place. On the morning of February 19, 2014, after being assaulted the victim states she went to grab the video equipment from its usual place and Defendant assaulted her again to prevent her from taking the equipment. The victim stated that Defendant had previously transmitted video footage to her through text messaging of the victim and himself engaging in sexual intercourse in his room. The victim additionally admitted that the video recorder transmits to Defendant's smart phone. Pursuant to a search warrant executed several days later, the police were able to recover the phone, several recording devices, assorted discs,

flash drives, and computer equipment belonging to Defendant. The victim and Defendant both affirmed to the officers at the scene that the recording device, connected to Defendant's cell phone "could have possibly" recorded the assault and the recording "may exist" on the phone. Additionally, the testimony before the court from the victim was that the device "could have recorded" the assault and therefore there "may be a recording." Entry to the phone has been prevented by encryption either by passcode or fingerprint.

The question before the court is whether the production of one's passcode or fingerprint is testimonial communication and therefore subject to the defendant's Fifth Amendment privilege against self-incrimination. The Commonwealth argues that the passcode and the fingerprint are not testimonial because the existence of the recording is a "foregone conclusion." Defense Counsel argues that both are testimonial in that either would provide access to all recordings or items on Defendant's phone.

Analysis

The Fifth Amendment to the Constitution of the United States provides that no person "shall be compelled in any criminal case to be a witness against himself." U.S. Const. amend V. "[T]he Fourteenth Amendment secures against state invasion the same privilege that the Fifth Amendment guarantees against federal infringement – the right of a person to remain silent unless he chooses to speak in the unfettered exercise of his own will." *Schmerber v. Cal.*, 384 U.S. 757, 760 (1966) (citation omitted). "[T]he privilege protects an accused only from being compelled to testify against himself, or otherwise provide the State with evidence of a testimonial or communicative nature." *U.S. v. Wade*, 388 U.S. 218, 221 (1967) (citation omitted). Thus the proper inquiry requires the court to resolve whether granting the motion to compel "would require (1) compulsion of a (2) testimonial communication that is (3) incriminating." *U. S. v. Authement*, 607 F.2d 1129, 1131 n. 1 (5th Cir. 1979).

It is a "settled proposition that a person may be required to produce specific documents even though they contain incriminating assertions of fact or belief because the creation of those documents was not 'compelled' within the meaning of the privilege [against self-incrimination]." *United States v. Hubbell*, 530 U.S. 27, 35–36 (2000); *accord Fisher v. United States*, 425 U.S. 391, 401 (1976) ("[T]he *Fifth Amendment* protects against 'compelled self-incrimination, not the disclosure of private information'"). Thus the contents of the phone, obtained pursuant to a validly executed warrant are only subject to objections raised under the *Fourth Amendment*, not the *Fifth Amendment*. Additionally, there is no question that a motion to compel is compulsive and the production of the passcode or fingerprint would be incriminating.[1] The analysis turns on whether a passcode or a fingerprint is "testimonial communication."

[1] Incriminating has been defined as "any disclosures that the witness reasonably believes could be used in a criminal prosecution or could lead to other evidence that might be so used." *Kastigar v. United States*, 406 U.S. 441, 445 (1972).

Passcode or Fingerprint

"An act is testimonial when the accused is forced to reveal his knowledge of facts relating him to the offense or from having to share his thoughts and beliefs with the government." *U.S. v. Kirschner*, 823 F. Supp. 2d 665, 668 (2010) (citing *United States v. Doe*, 487 U.S. 201, 212 (1987)). "[T]here is a significant difference between the use of compulsion to extort communications from a defendant and compelling a person to engage in conduct that may be incriminating." *Hubbell*, 530 U.S.at 35. "[T]he privilege offers no protection against compulsion to submit to fingerprinting, photography, or measurements, to write or speak for identification, to appear in court, to stand, to assume a stance, to walk, or to make a particular gesture." *Wade*, 388 U.S. at 223. "[E]ven though the act may provide incriminating evidence, a criminal suspect may be compelled to put on a shirt, to provide a blood sample or handwriting exemplar, or to make a recording of his voice. The act of exhibiting such physical characteristics is not the same as a sworn communication by a witness that relates either express or implied assertions of fact or belief." *Hubbell*, 530 U.S. at 35.

A witness's "act of production itself could qualify as testimonial if conceding the existence, possession and control, and authenticity of the documents tend[s] to incriminate [him or her]." *United States v. Doe (In re Grand Jury Subpoena Duces Tecum)*, 670 F.3d 1335, 1343 (11th Cir. 2012) (citing holding of *Fisher v. United States*, 425 U.S. 391, 410 (1976)). Nevertheless, "[w]hen the 'existence and location' of the documents under subpoena are a 'foregone conclusion' and the witness 'adds little or nothing to the sum total of the Government's information by conceding that he in fact has the [documents],' then no Fifth Amendment right is touched because the 'question is not of testimony but of surrender.'" *Doe v. United States (In re Grand Jury Subpoena)*, 383 F.3d 905, 910 (9th Cir. 2004) (citing *Fisher*, 425 U.S. at 411). "[T]he Government is in no way relying on the 'truthtelling' of the [witness] to prove the existence of or his access to the documents." *Fisher*, 425 U.S. at 411. "Whether the existence of documents is a foregone conclusion is a question of fact, subject to review for clear error." *United States v. Norwood*, 420 F.3d 888, 895 (8th Cir. 2005) (citing *United States v. Doe*, 425 U.S. 605, 613–14 (1984)).

Therefore, in *Hubbell*, the Court found the action of producing documents in response to a subpoena was testimonial in nature and therefore subject to the constitutional privilege against self-incrimination. *Hubbell*, 530 U.S. at 40. The Court was persuaded by the fact that in the act of production, the respondent had to take "the mental and physical steps necessary to provide the prosecutor with an accurate inventory of the many sources of potentially incriminating evidence sought by the subpoena." Id. at 42. The Court reasoned that given this information, "[b]y 'producing documents in compliance with a subpoena, the witness would admit that the papers existed, were in his possession or control, and were authentic.' Moreover, . . . when the [witness] responds to the subpoena, he may be compelled to take the witness stand

and answer . . . whether he has produced everything demanded by the subpoena." Id. at 36–37. The Court found notable that the text of the subpoena, often using the phrase "any and all documents related," made it obvious that the prosecutor needed respondent's assistance to identify potential sources of information and to produce those sources of information. Id. at 41. Therefore, when the respondent produced these documents in response to the subpoena, it was the "functional equivalent of the preparation of an answer to either a detailed written interrogatory or a series of oral questions at a discovery deposition." Id. at 41–42. "The assembly of those documents was like telling an inquisitor the combination to a wall safe, not like being forced to surrender the key to a strongbox." Further, the Hubbell Court found that the "foregone conclusion" doctrine did not apply in this case, where the Government had not shown that it had any prior knowledge of either the existence or the whereabouts of the 13,120 pages of documents ultimately produced by respondent." Id. at 45.

Similarly, in the context of compelling the production of a passcode, the U.S. District Court for the Eastern District of Michigan held that compelling the defendant to provide a password is a testimonial communication. *United States v. Kirschner*, 823 F. Supp. 2d 665, 669 (E.D. Mich. 2010). The court reasoned "forcing the Defendant to reveal the password . . . requires Defendant to communicate 'knowledge,' unlike the production of a handwriting sample or a voice exemplar." *Id.* "It is the 'extortion of information from the accused,' the attempt to force him to 'disclose the contents of his own mind' that implicates the *Self-Incrimination Clause*." *Id.* (quoting *United States v. Doe*, 487 U.S. at 211) (emphasis in original). The court found *Hubbell's* distinction between telling an inquisitor the combination to a wall safe and surrendering a key to a strongbox instructive. *Id.* Similar to having to divulge the combination to a safe, the court reasoned "the government is not seeking documents or objects – it is seeking testimony from the Defendant, requiring him to divulge through his mental processes his password." *Id.*; *accord In re Grand Jury Subpoena (Boucher)*, No. 2:06-mj-91, 2007 U.S. Dist. LEXIS 87951 at *16, 2007 WL 4246473 (D. Vt. Nov. 29, 2007) ("Since the government is trying to compel the production of the password itself, the foregone conclusion doctrine cannot apply. The password is not a physical thing. If Boucher knows the password, it only exists in his mind.").[2]

In this case, the Defendant cannot be compelled to produce his passcode to access his smartphone but he can be compelled to produce his fingerprint to do the same. The footage itself would not be protected under the Fifth Amendment because its creation was voluntary, i.e. not compelled. As stated above, the *Fifth Amendment* only protects against "compelled" self-incrimination, therefore the contents of Defendant's

[2] However, on appeal, the District Court for the District of Vermont found that requiring Defendant to produce an unencrypted version of the documents in his encrypted hard drive that he had already provided access to previously was not testimonial because the existence of and location of the documents were a "foregone conclusion." *In re Grand Jury Subpoena to Boucher*, 2009 U.S. Dist. LEXIS 13006 at *8, 2009 WL 424718 (D. Vt. Feb. 19, 2009).

phone, created voluntarily, are not protected against disclosure. However, compelling Defendant to provide access through his passcode is both compelled and testimonial and therefore protected. Contrary to the Commonwealth's assertion, the password is not a foregone conclusion because it is not known outside of Defendant's mind. Unlike a document or tangible thing, such as an unencrypted copy of the footage itself, if the password was a foregone conclusion, the Commonwealth would not need to compel Defendant to produce it because they would already know it. As reasoned in *Kirschner*, Defendant cannot be compelled to "divulge through his mental processes" the passcode for entry. The fingerprint, like a key, however, does not require the witness to divulge anything through his mental processes. On the contrary, like physical characteristics that are non-testimonial, the fingerprint of Defendant if used to access his phone is likewise non-testimonial and does not require Defendant to "communicate any knowledge" at all. Unlike the production of physical characteristic evidence, such as a fingerprint, the production of a password forces the Defendant to "disclose the contents of his own mind." For this reason the motion to compel the passcode should be **DENIED** but the motion to compel the fingerprint should be **GRANTED**.

Unencrypted Footage

Neither has the Commonwealth asked to compel the unencrypted video recording. However, from the testimony of the witness at the hearing, the existence and location of the recording is not a foregone conclusion and compelling Defendant to produce an unencrypted version would be self-incriminating. The most the Commonwealth knows is that the recording "could exist" because the device "may have recorded" the assault and transmitted it to the phone. The alternative is also true, that the device "may not have" recorded the assault and the recording "may not exist." This being the only reason the Commonwealth suspects there may be a recording, the existence and location of the recording is not a foregone conclusion. Defendant's production of the unencrypted recording would be testimonial because Defendant would be admitting the recording exists, it was in his possession and control, and that the recording is authentic. Therefore, the Commonwealth could not compel Defendant to produce an unencrypted version of the recording.

Sincerely,

Steven C. Frucci
Presiding Judge

SCF/alg/nc

Anexo II – Caso State of Minnesota v. Matthew Vaughn Diamond

STATE OF MINNESOTA
IN COURT OF APPEALS
A15-2075

State of Minnesota,
Respondent,

vs.

Matthew Vaughn Diamond, Appellant.

Filed January 17, 2017
Affirmed
Smith, Tracy M., Judge

Carver County District Court
File No. 10-CR-14-1286

Lori Swanson, Attorney General, St. Paul, Minnesota; and

Mark Metz, Carver County Attorney, Eric E. Doolittle, Assistant County Attorney, Chaska, Minnesota (for respondent)

Cathryn Middlebrook, Chief Appellate Public Defender, Steven P. Russett, Assistant Public Defender, St. Paul, Minnesota (for appellant)

Considered and decided by Johnson, Presiding Judge; Reyes, Judge; and Smith,

Tracy M., Judge.

S Y L L A B U S

A district court order compelling a criminal defendant to provide a fingerprint to unlock the defendant's cellphone does not violate the Fifth Amendment privilege against compelled self-incrimination.

O P I N I O N

SMITH, TRACY M., Judge

Appellant Matthew Vaughn Diamond appeals his convictions of second-degree burglary, misdemeanor theft, and fourth-degree criminal damage to property following a jury trial. On appeal, Diamond argues his convictions must be reversed because: (1) police seized his property in violation of the Fourth Amendment; (2) the district court violated his Fifth Amendment privilege against compelled self-incrimination by ordering him to provide his fingerprint so police could search his cellphone; and (3) the state's circumstantial evidence was insufficient. We affirm.

FACTS

On October 30, 2014, M.H. left her Chaska home between 10:30 and 10:45 a.m. to run errands. M.H. returned home around noon and noticed that the attached garage's sideentry door appeared to have been kicked in from the outside. M.H. called the police after discovering that a safe, a laptop, and several items of jewelry were missing from her home. While waiting for police to arrive, M.H. found an envelope in her driveway that had the name of S.W. written on it. Police took photographs and measurements of the shoeprints left on the garage's side-entry door.

Detective Nelson of the Chaska Police Department used state databases to determine S.W.'s car model and license plate number and that S.W. had pawned several pieces of jewelry at a Shakopee pawn shop on October 30. M.H. later verified that the pawned jewelry was stolen from her home. On November 4, police located S.W.'s car, which

Diamond was driving at the time. Diamond was arrested on an outstanding warrant unrelated to this case. He was booked at the Scott County jail, where staff collected and stored his property, including his shoes and cellphone.

The following day, Detective Nelson went to the jail and viewed the property that was taken from Diamond. Detective Nelson observed similarities between the tread of Diamond's shoes and the shoeprints left on the garage's side-entry door. Detective Nelson informed the jail staff that she was going to seek a warrant to seize Diamond's property and gave instructions not to release the property to anyone. Later that day, S.W. attempted to collect Diamond's property but was told that it could not be released.

On November 6, Detective Nelson obtained and executed a warrant to search for, and seize, Diamond's shoes and cellphone. On November 12, Detective Nelson obtained an additional warrant to search the contents of Diamond's cellphone. Detective Nelson was unable to unlock the cellphone. She returned the warrant on November 21.

In December, the state filed a motion to compel Diamond to provide his fingerprint on the cellphone to unlock the phone. The motion was deferred to the contested omnibus hearing. Following that hearing, the district court issued an order, filed February 11, 2015, concluding that the warrant to search Diamond's cellphone was supported by probable cause and that compelling Diamond to provide his fingerprint to unlock the cellphone does not violate his Fifth Amendment privilege against compelled self-incrimination. The district court granted the state's motion to compel and ordered Diamond to provide a fingerprint or thumbprint to unlock his cellphone. Diamond refused to comply. On

April 3, the district court found Diamond in civil contempt and informed him that compliance with the order would remedy the civil contempt. Diamond provided his fingerprint, and police immediately searched his cellphone.

At a second omnibus hearing Diamond challenged the refusal to release his cellphone and shoes to S.W., arguing that it constituted a warrantless seizure not justified by any exception to the warrant requirement. The district court's April 3 order concluded that the seizure was justified by exigent circumstances and was tailored to protect against the destruction of evidence while a warrant was sought and obtained. Diamond thereafter brought a pro se motion to suppress all evidence derived from his cellphone and shoes, which the district court denied, relying on the previous orders from February 11 and April 3.

At Diamond's jury trial, S.W. testified that: (1) she believed she was working the day of the burglary; (2) the envelope found in M.H.'s driveway belonged to S.W., and it was in her car the last time she saw it; (3) S.W. sometimes let Diamond use her car when she was working; and (4) on the day of the burglary, Diamond gave her M.H.'s stolen jewelry, and the two of them traveled to the Shakopee pawn shop, where she sold the jewelry. In addition, the state also introduced evidence that: (1) Diamond's wallet and identification card were found in S.W.'s car; (2) Diamond and S.W. exchanged phone calls and text messages throughout the day of the burglary; (3) Diamond's cellphone pinged off cell towers near M.H.'s residence on the day of the burglary; (4) the tread pattern on Diamond's shoes was similar to the shoeprints on the garage's side-entry door; and (5) while in jail, Diamond told S.W. "the only thing that [the state is] going to be able to charge me with is receiving stolen property" and that his attorney said the case would be dismissed if S.W. did not testify or recanted her statement.

The jury found Diamond guilty of second-degree burglary, misdemeanor theft, and fourth-degree criminal damage to property. The district court sentenced Diamond to 51 months in prison for the second-degree burglary and to 90 days in jail for the fourth-degree criminal damage to property.

Diamond appeals.

ISSUES

I. Did the district court err by not suppressing evidence obtained following the temporary seizure of Diamond's property?

II. Did the district court err by ordering Diamond to provide his fingerprint so police could search his cellphone?

III. Does the record contain sufficient evidence to support the jury's conclusion that Diamond committed second-degree burglary, misdemeanor theft, and fourth-degree criminal damage to property?

ANALYSIS

I. The temporary seizure of Diamond's property did not violate the Fourth Amendment.

Diamond argues that the district court erred in denying his suppression motion because Detective Nelson's directions to jail staff not to release Diamond's property while she sought a warrant constituted an unreasonable seizure in violation of the Fourth Amendment. The district court concluded that the exigency exception to the warrant requirement applied. Diamond argues that the exigency exception is inapplicable because Detective Nelson "searched" Diamond's property at the jail before providing instructions

to jail staff.

In evaluating a pretrial order on a motion to suppress, we review factual findings for clear error and legal conclusions de novo. *State v. Milton*, 821 N.W.2d 789, 798 (Minn. 2012). When reviewing the applicability of the exigency exception, we look at the totality of the circumstances. *State v. Horst*, 880 N.W.2d 24, 33 (Minn. 2016). The state has the burden of showing that exigent circumstances justified the seizure. *Id.*

The Fourth Amendment protects the right of the people to be free from "unreasonable searches and seizures" of their "persons, houses, papers, and effects" by the government. U.S. Const. amend. IV; *see Mapp v. Ohio*, 367 U.S. 643, 655-56, 81 S. Ct. 1684, 1691-92 (1961) (incorporating the Fourth Amendment and the consequences for violating it into the Due Process Clause of the Fourteenth Amendment). A "seizure" of property within the meaning of the Fourth Amendment occurs when a government official meaningfully interferes with a person's possessory interest in the property. *United States v. Jacobsen*, 466 U.S. 109, 113, 104 S. Ct. 1652, 1656 (1984). "In general, warrantless searches and seizures are unreasonable in the absence of a legally recognized exception to the warrant requirement." *Horst*, 880 N.W.2d at 33.

A temporary seizure may be permissible under the Fourth Amendment "when needed to preserve evidence until police are able to obtain a warrant." *State v. Holland*, 865 N.W.2d 666, 670 n.3 (Minn. 2015). The United States Supreme Court has approved the temporary seizure of an individual to prevent him from destroying drugs before police could obtain and execute a warrant. *Illinois v. McArthur*, 531 U.S. 326, 331-32, 121 S. Ct. 946, 950 (2001). The Minnesota Supreme Court has observed that, "when lawenforcement officers 'have probable cause to believe that a container holds contraband or evidence of a crime, but have not secured a warrant,' the officers may seize the property, 'pending issuance of a warrant to examine its contents, if the exigencies of the circumstances demand it.'" *Horst*, 880 N.W.2d at 33-34 (quoting *United States v. Place*, 462 U.S. 696, 701, 103 S. Ct. 2637, 2641 (1983)).

Here, Detective Nelson instructed jail staff not to release Diamond's property while she sought a warrant. Detective Nelson's instructions to jail staff were meant to ensure that Diamond's shoes and cellphone,

which Detective Nelson considered potential evidence, were not lost or destroyed. The following day, Detective Nelson obtained and executed a warrant to seize Diamond's shoes and cellphone.

In *Horst*, the Minnesota Supreme Court deemed a similar warrantless seizure lasting only one day to be justified. *Id.* at 34-35. There, police had seized the defendant's cellphone when she was interviewed at the police station prior to her arrest, and police obtained a warrant the following day. *Id.* The supreme court concluded that the seizure was justified by exigent circumstances because, as the United States Supreme Court had recently observed, "the owner of a cellphone . . . can quickly and easily destroy the data contained on such a device." *Id.* at 35 (citing *Riley v. California*, 134 S. Ct. 2473, 2486 (2014)). Thus, the temporary seizure of Diamond's cellphone at the jail was justified by exigent circumstances. The need to protect physical evidence from loss or destruction similarly justified the temporary seizure of Diamond's shoes. *See McArthur*, 531 U.S. at

331-32, 121 S. Ct. at 950.

Diamond argues that the exigent-circumstances exception does not apply because Detective Nelson "searched" Diamond's property at the jail prior to the seizure. As an initial matter, we observe that Diamond did not argue to the district court that the evidence should be suppressed because Detective Nelson's act of viewing his property at the jail constituted a "search" rendering the exigency exception for the seizure inapplicable. An appellate court generally will not consider matters not argued to and considered by the district court. *Roby v. State*, 547 N.W.2d 354, 357 (Minn. 1996). This rule applies to constitutional questions. *See In re Welfare of C.L.L.*, 310 N.W.2d 555, 557 (Minn. 1981) (declining to address a constitutional issue raised for the first time on appeal from a termination of parental rights).

But even if Diamond's district court argument could be read expansively so as to encompass this argument, we still find it unpersuasive. Diamond does not provide any support for his conclusory assertion that Detective Nelson's act of viewing his property at the jail prior to obtaining a search warrant constituted a "search" under the Fourth Amendment. *See State v. Johnson*, 831 N.W.2d 917, 922 (Minn. App. 2013) ("A 'search' within the meaning of the Fourth Amendment occurs upon an official's invasion of a person's reasonable expectation of privacy." (citing *Jacobsen*, 466 U.S. at 114, 104 S. Ct. at 1656)), *review denied* (Minn. Sept. 17, 2013). Nor does he argue that such action was unreasonable.

As articulated in *McArthur*, we must determine whether "police made reasonable efforts to reconcile their law enforcement needs with the demands of personal privacy." 531 U.S. at 332, 121 S. Ct. at 950. In *McArthur*, the United States Supreme Court determined that the proper balance between law-enforcement needs and personal privacy permitted police to seize the defendant while they sought a warrant to search his trailer. *Id.* at 332, 121 S. Ct. at 950-51. Here, Detective Nelson properly balanced law-enforcement needs with Diamond's personal privacy. Diamond concedes that his property was lawfully seized and inventoried when he was booked into jail on November 4. The following day, Detective Nelson viewed Diamond's property and observed similarities between the tread of Diamond's shoes and the shoeprints left on M.H.'s garage's side-entry door. Recognizing the possibility that these items could be lost or destroyed, Detective Nelson instructed jail staff to maintain custody of the property and immediately sought a warrant. On November 6, Detective Nelson executed the warrant, seizing the cellphone and shoes. Before attempting to access the cellphone's contents, which plainly constitutes a search within the meaning of the Fourth Amendment, Detective Nelson obtained the November 12 search warrant. *See Riley*, 134 S. Ct. at 2495.

We conclude that the temporary seizure of Diamond's property was justified by exigent circumstances and that the district court did not err in denying Diamond's suppression motion.

II. Diamond's Fifth Amendment privilege was not violated when the district court ordered him to provide his fingerprint so police could search his cellphone.

Diamond argues that the district court's order to provide his fingerprint to unlock his cellphone violated his Fifth Amendment privilege against compelled selfincrimination.[580] This is an issue of first impression for

[580] Diamond also argues that the search of his cellphone violated the Fourth Amendment because, he asserts, the police did not have a valid warrant at the time his cellphone was searched in April 2015.

Minnesota appellate courts. Whether the district court violated Diamond's Fifth Amendment privilege against self-incrimination is a question of law, which this court reviews de novo. *State v. Kaquatosh*, 600 N.W.2d 153, 156 (Minn. App. 1999), *review denied* (Minn. Dec. 14, 1999).

The Fifth Amendment provides that no person "shall be compelled in any criminal case to be a witness against himself." U.S. Const. amend. V; *see Malloy v. Hogan*, 378 U.S. 1, 8, 84 S. Ct. 1489, 1493-94 (1964) (incorporating Fifth Amendment protections into the Due Process Clause of the Fourteenth Amendment). "The essence of this basic constitutional principle is the requirement that the [s]tate which proposes to convict and punish an individual produce the evidence against him by the independent labor of its officers, not by the simple, cruel expedient of forcing it from his own lips." *Estelle v. Smith*, 451 U.S. 454, 462, 101 S. Ct. 1866, 1872 (1981) (quotation and emphasis omitted). The Supreme Court has explained that "the privilege protects a person only against being incriminated by his own compelled testimonial communications." *Fisher v. United States*, 425 U.S. 391, 409, 96 S. Ct. 1569, 1580 (1976). Here, the record establishes that Diamond was compelled to produce his fingerprint to unlock the cellphone. The record also reflects that police obtained incriminating evidence once the cellphone was unlocked. Therefore, the question before this court is whether the act of providing a fingerprint to unlock a cellphone is a "testimonial communication."

In examining its application of Fifth Amendment principles, the Supreme Court has established that, "in order to be testimonial, [a criminal defendant's] communication must itself, explicitly or implicitly, relate a factual assertion or disclose information. Only then is a person compelled to be a 'witness' against himself." *Doe v. United States*, 487 U.S. 201, 210, 108 S. Ct. 2341, 2347-48 (1988). The Supreme Court has further noted that

> [t]his understanding is perhaps most clearly revealed in those cases in which the Court has held that certain acts, though incriminating, are not within the privilege. Thus, a suspect may be compelled to furnish a blood sample; to provide a handwriting exemplar, or a voice exemplar; to stand in a lineup; and to wear particular clothing.

Id. at 210, 108 S. Ct. at 2347 (citing *United States v. Dionisio*, 410 U.S. 1, 7, 93 S. Ct. 764, 768 (1973) (voice exemplar); *Gilbert v. California*, 388 U.S. 263, 266-67, 87 S. Ct. 1951, 1953 (1967) (handwriting exemplar); *United States v. Wade*, 388 U.S. 218, 221-22, 87 S. Ct. 1926, 1929 (1967) (lineup); *Schmerber v. California*, 384 U.S. 757, 765, 86 S. Ct. 1826,

---

Diamond maintains that "no search warrant existed" in April because Detective Nelson had previously returned the November 12 search warrant on November 21 after unsuccessfully attempting to access the contents of the cellphone. However, Diamond did not make this argument at the contested omnibus hearing, where he challenged the probable cause supporting the November 12 warrant and opposed the state's motion for an order compelling him to provide his fingerprint. Instead, Diamond waited until two days before trial to present this argument to the district court, asserting it for the first time during oral argument on his pro se motion to suppress evidence. Because Diamond did not raise this argument at the omnibus hearing, the argument was not timely raised and is not reviewable on appeal. *See State v. Brunes*, 373 N.W.2d 381, 386 (Minn. App. 1985), *review denied* (Minn. Oct. 11, 1985).

1832-33 (1966) (blood sample); *Holt v. United States*, 218 U.S. 245, 252-53, 31 S. Ct. 2, 6 (1910) (clothing)). In addition, the Supreme Court has recognized that "both federal and state courts have usually held that [the Fifth Amendment] offers no protection against compulsion to submit to fingerprinting." *Schmerber*, 384 U.S. at 764, 86 S. Ct. at 1832; *see Doe*, 487 U.S. at 219, 108 S. Ct. at 2352 (Stevens, J., dissenting) ("Fingerprints, blood samples, voice exemplars, handwriting specimens, or other items of physical evidence may be extracted from a defendant against his will."); *State v. Breeden*, 374 N.W.2d 560, 562 (Minn. App. 1985) ("The gathering of real evidence such as blood samples, fingerprints, or photographs does not violate a defendant's [F]ifth [A]mendment rights.").

Diamond relies on *In re Grand Jury Subpoena Duces Tecum*, 670 F.3d 1335 (11th Cir. 2012), to support his argument that supplying his fingerprint was testimonial. In *In re Grand Jury*, the court reasoned that requiring the defendant to decrypt and produce the contents of a computer's hard drive, when it was unknown whether any documents were even on the encrypted drive, "would be tantamount to testimony by [the defendant] of his knowledge of the existence and location of potentially incriminating files; of his possession, control, and access to the encrypted portions of the drives; and of his capability to decrypt the files." *Id.* at 1346. The court concluded that such a requirement is analogous to requiring production of a combination and that such a production involves implied factual statements that could potentially incriminate. *Id.*

By being ordered to produce his fingerprint, however, Diamond was not required to disclose any knowledge he might have or to speak his guilt. *See Doe*, 487 U.S. at 211, 108 S. Ct. at 2348. The district court's order is therefore distinguishable from requiring a defendant to decrypt a hard drive or produce a combination. *See, e.g.*, *In re Grand Jury*,

670 F.3d at 1346; *United States v. Kirschner*, 823 F. Supp. 2d 665, 669 (E.D. Mich. 2010) (holding that requiring a defendant to provide computer password violates the Fifth

Amendment). Those requirements involve a level of knowledge and mental capacity that is not present in ordering Diamond to place his fingerprint on his cellphone. Instead, the task that Diamond was compelled to perform—to provide his fingerprint—is no more testimonial than furnishing a blood sample, providing handwriting or voice exemplars, standing in a lineup, or wearing particular clothing. *See Doe*, 487 U.S. at 210, 108 S. Ct. at 2347-48.

Diamond argues, however, that the district court's order effectively required him to communicate "that he had exclusive use of the phone containing incriminating information." This does not overcome the fact that such a requirement is not testimonial. In addition, Diamond provides no support for the assertion

that only his fingerprint would unlock the cellphone or that his provision of a fingerprint would communicate his exclusive use of the cellphone.

Diamond also argues that he "was required to identify for the police which of his fingerprints would open the phone" and that this requirement compelled a testimonial communication. This argument, however, mischaracterizes the district court's order. The district court's February 11 order compelled Diamond to "provide a fingerprint or thumbprint as deemed necessary by the Chaska Police Department to unlock his seized cell phone." At the April 3 contempt hearing, the district court referred to Diamond providing his "thumbprint." The prosecutor noted that they were "not sure if it's an index finger or a thumb." The district court answered, "Take whatever samples you need." Diamond then asked the detectives which finger they wanted, and they answered, "The one that unlocks it."

It is clear that the district court permitted the state to take samples of all of Diamond's fingerprints and thumbprints. The district court did not ask Diamond whether his prints would unlock the cellphone or which print would unlock it, nor did the district court compel Diamond to disclose that information. There is no indication that Diamond would have been asked to do more had none of his fingerprints unlocked the cellphone. Diamond himself asked which finger the detectives wanted when he was ready to comply with the order, and the detectives answered his question. Diamond did not object then, nor did he bring an additional motion to suppress the evidence based on the exchange that he initiated.

In sum, because the order compelling Diamond to produce his fingerprint to unlock the cellphone did not require a testimonial communication, we hold that the order did not violate Diamond's Fifth Amendment privilege against compelled self-incrimination.[581]

III. The record contains sufficient evidence to support Diamond's convictions.

Diamond argues that his convictions must be reversed because the state's circumstantial evidence does not exclude the rational hypothesis that Diamond merely committed the crime of transferring stolen property. When evaluating the sufficiency of circumstantial evidence, the reviewing court uses a two-step analysis. *State v. Silvernail*, 831 N.W.2d 594, 598 (Minn. 2013). "The first step is to identify the circumstances proved." *Id.* "In identifying the circumstances proved, we defer to the jury's acceptance of the proof of these circumstances and rejection of evidence in the record that conflicted with the circumstances proved by the [s]tate." *Id.* at 598-99 (quotation omitted). The reviewing court "construe[s] conflicting evidence in the light most favorable to the verdict and assume[s] that the jury believed the [s]tate's witnesses and disbelieved the defense witnesses." *Id.* at 599 (quotation omitted). "The second step is to determine

[581] We express no opinion regarding whether, in a given case, a defendant may be compelled to produce a cellphone password, consistent with the Fifth Amendment.

whether the circumstances proved are consistent with guilt and inconsistent with any rational hypothesis except that of guilt." *Id.* (quotation omitted).

Here, Diamond was convicted of second-degree burglary, misdemeanor theft, and fourth-degree criminal damage to property. A person is guilty of second-degree burglary if the person enters a dwelling without consent and with the intent to commit a crime. Minn. Stat. § 609.582, subd. 2(a) (2014). A person is guilty of theft if the person "intentionally and without claim of right takes . . . movable property of another without the other's consent and with intent to deprive the owner permanently of possession of the property." Minn. Stat. § 609.52, subd. 2(a)(1) (2014). A person is guilty of fourth-degree criminal damage to property if the person intentionally causes damage to another's physical property without the other person's consent. Minn. Stat. § 609.595, subd. 3 (2014).

The circumstances proved support the jury's conclusion that Diamond committed these crimes. On October 30, 2014, M.H. returned home after running errands and discovered that someone had kicked in her garage's side-entry door and had stolen jewelry and a number of other items. Police recovered an envelope in M.H.'s driveway that had S.W.'s name written on it. S.W. testified that this envelope was in her car the last time she saw it. S.W. also testified that she believed she was working on the day of the burglary, and that she sometimes let Diamond use her car when she was working. Diamond's cellphone pinged off cell towers near M.H.'s residence on the day of the burglary. S.W. also testified that, on the day of the burglary, Diamond gave her M.H.'s stolen jewelry, and the two of them traveled to the Shakopee pawn shop, where she sold the jewelry. Finally, Detective Nelson testified regarding consistencies between the tread of Diamond's shoes and the shoeprints on M.H.'s garage's side-entry door.

Diamond argues that certain circumstances do not exclude the possibility that he did not commit the crimes at issue. This argument is unconvincing. Diamond considers the individual circumstances proved in isolation. But the evidence as a whole firmly supports the jury's conclusion that Diamond kicked down M.H.'s garage's side-entry door, entered her dwelling without consent and with the intent to commit a crime, and stole M.H.'s property. Together, the circumstances proved are inconsistent with any other rational hypothesis. Therefore, we conclude that the record contained sufficient evidence to support the jury's conclusion that Diamond committed the offenses of second-degree burglary, misdemeanor theft, and fourth-degree criminal damage to property.

D E C I S I O N

The district court did not err in denying Diamond's suppression motion because the temporary seizure of his property was justified by exigent circumstances and, therefore, did not violate the Fourth Amendment. The district court did not violate Diamond's Fifth Amendment privilege against self-incrimination by ordering him to provide his fingerprint so police could search his cellphone because such an order does not require a testimonial communication. Finally, the record contains sufficient evidence to support the jury's conclusion that Diamond committed second-degree burglary, misdemeanor theft, and fourth-degree criminal damage to property.

Affirmed.

Anexo III – Caso Paytsar Bkhchadzhyan

NO. LA081589

SUPERIOR COURT OF CALIFORNIA COUNTY OF LOS ANGELES

PAGE NO. 1

THE PEOPLE OF THE STATE OF CALIFORNIA vs. CURRENT DATE 05/03/16 DEFENDANT 01: PAYTSAR BKHCHADZHYAN

LAW ENFORCEMENT AGENCY EFFECTING ARREST: CHP - WEST VALLEY STATION

BAIL: APPEARANCE AMOUNT DATE RECEIPT OR SURETY COMPANY REGISTER

DATE OF BAIL POSTED BOND NO. NUMBER 09/09/15 $50,000.00 08/25/15 AS50K60527 ALLEGHENY CASUALTY

CASE FILED ON 08/18/15.

COMPLAINT FILED, DECLARED OR SWORN TO CHARGING DEFENDANT WITH HAVING COMMITTED, ON OR ABOUT 11/27/14 IN THE COUNTY OF LOS ANGELES, THE FOLLOWING OFFENSE(S) OF:

COUNT 01: 530.5(A) pc FEL
COUNT 02: 487 (A) pc FEL
COUNT 03: 529(A) (3) pc FEL
COUNT 04: 484E(D) pc FEL
COUNT 05 : 484E(D) pc FEL
COUNT 06: 484E(D) pc FEL
COUNT 07: 4841(C) pc FEL NEXT SCHEDULED EVENT:

ARREST WARRANT TO ISSUE

08/18/15 ARREST WARRANT IN THE AMOUNT OF $250,000.00 BY ORDER OF JUDGE JOSEPH A. BRANDOLINO ISSUED. (08/18/15) .

ON 08/21/15 AT 800 AM:

NEXT SCHEDULED EVENT:

08/21/15 830 AM ARRAIGNMENT DIST VAN NUYS COURTHOUSE DEPT 100

ON 08/21/15 AT 830 AM IN VAN NUYS COURTHOUSE DEPT 100
CASE CALLED FOR ARRAIGNMENT

PARTIES: JOHN REID (JUDGE) U-CHIN JANG (CLERK)
HILDA GUTIERREZ (REP) LOU ANN CLEMENS (DA)

DEFENDANT IS PRESENT IN COURT, AND REPRESENTED BY A. BOYADZHYAN PRIVATE COUNSEL COURT ORDERS AND FINDINGS:

-THE COURT ORDERS THE DEFENDANT TO APPEAR ON THE NEXT COURT DATE. THE MATTER IS CONTINUED TO SEPTEMBER 9, 2015, IN DEPARTMENT 100, FOR EARLY DISPOSITION HEARING.

A PENAL CODE SECTION 1275 HOLD IS PLACED ON THE DEFENDANT. BAIL SET AT $50,000.

WAIVES STATUTORY TIME.

NEXT SCHEDULED EVENT:

09/09/15 830 AM DISPOSITIONDIST VAN NUYS COURTHOUSE DEPT 100

08/21/15 ARREST WARRANT IN THE AMOUNT OF $250,000.00 RECALLED. (08/24/15).

CUSTODY STATUS: REMANDED TO CUSTODY

ON 08/24/15 AT 830 AM IN VAN NUYS COURTHOUSE DEPT 100
CASE CALLED FOR FURTHER PROCEEDINGS

PARTIES: JOHN REID (JUDGE) U-CHIN JANG (CLERK)
HILDA GUTIERREZ (REP) LOU ANN CLEMENS (DA)

DEFENDANT IS NOT PRESENT IN COURT, BUT REPRESENTED BY GEORGE MGDESYAN PRIVATE COUNSEL

THE MATTER TS PLACED ON CALENDAR ON BEHALF OF THE DEFENDANT. THE DISTRICT ATTORNEY STIPULATES TO LIFT THE 1275PC HOLD ON THE

DEFENDANT .

NEXT SCHEDULED EVENT:
DISPOSITION

ON 09/09/15 AT 830 AM IN VAN NUYS COURTHOUSE DEPT 100

CASE CALLED FOR DISPOSITION

PARTIES: LELAND B. HARRIS (JUDGE) U-CHIN JANG (CLERK)

HILDA GUTIERREZ (REP) LOU ANN CLEMENS (DA)

DEFENDANT IS PRESENT IN COURT, AND REPRESENTED BY GEORGE MGDESYAN PRIVATE COUNSEL

DEFENDANT WAIVES ARRAIGNMENT, READING OF COMPLAINT, AND STATEMENT OF CONSTITUTIONAL AND STATUTORY RIGHTS .

DEFENDANT PLEADS NOT GUILTY TO COUNT 01, 530. 5(A) PC.

DEFENDANT PLEADS NOT GUILTY TO COUNT 02, 487(A) PC.

DEFENDANT PLEADS NOT GUILTY TO COUNT 05, 484E(D) pc.

DEFENDANT PLEADS NOT GUILTY TO COUNT 06, 484E(D) pc.
DEFENDANT PLEADS NOT GUILTY TO COUNT 07, 4841(C) pc.
DEFENDANT PLEADS NOT GUILTY TO COUNT 03, 529(A)(3) PC. DEFENDANT PLEADS NOT GUILTY TO COUNT 04, 484E(D) pc.

COURT ORDERS AND FINDINGS:

-THE COURT ORDERS THE DEFENDANT TO APPEAR ON THE NEXT COURT DATE.

DEFENDANT DENIES ANY AND ALL ALLEGATIONS AND PRIOR CONVICTIONS. PRELIMINARY HEARING SETTING IS SET FOR 9-29-15, AT 8:30 AM, IN DEPARTMENT 112, AS ZERO OF 10.

THE HELD TO ANSWER DEPARTMENT IS NW F.

WAIVES STATUTORY TIME.

NEXT SCHEDULED EVENT:

09/29/15 830 AM PRELIM SETTING/RESETTING DIST VAN NUYS COURTHOUSE DEPT 112 DAY 00 OF 10

09/09/15 BAIL TO STAND, # AS50K60527

CUSTODY STATUS: BAIL TO STAND

ON 09/29/15 AT 830 AM IN VAN NUYS COURTHOUSE DEPT 112

CASE CALLED FOR PRELIM SETTING/RESETTING

PARTIES: KAREN J . NUDELL (JUDGE) LYNNE GARCIA (CLERK)

TROYETTE SCOTT (REP) MICHAEL J . MORSE (DA)

DEFENDANT IS PRESENT IN COURT, AND REPRESENTED BY GEORGE MGDESYAN PRIVATE COUNSEL

THIS MATTER IS CONTINUED FOR PRELIMINARY HEARING SETTING TO DATE AND TIME INDICATED BELOW COURT ORDERS AND FINDINGS:

-THE COURT ORDERS THE DEFENDANT TO APPEAR ON THE NEXT COURT DATE.

WAIVES STATUTORY TIME.

NEXT SCHEDULED EVENT:

10/28/15 830 AM PRELIM SETTING/RESETTING DIST VAN NUYS COURTHOUSE DEPT 112

DAY 00 OF 10

09/29/15 BAIL TO STAND, # AS50K60527

CUSTODY STATUS: BAIL TO STAND

ON 10/28/15 AT 830 AM IN VAN NUYS COURTHOUSE DEPT 112
CASE CALLED FOR PRELIM SETTING/RESETTING

PARTIES: MARTIN L. HERSCOVITZ (JUDGE) LYNNE GARCIA (CLERK)

TROYETTE SCOTT (REP) MELANY AVANESSIANS (DA)

DEFENDANT IS PRESENT IN COURT, AND REPRESENTED BY GEORGE MGDESYAN PRIVATE COUNSEL

ATTY LANCE ROSENBERG APPEARING.

THIS MATTER IS CONTINUED FOR PRELIMINARY HEARING SETTING TO DATE AND TIME INDICATED BELOW COURT ORDERS AND FINDINGS:

-THE COURT ORDERS THE DEFENDANT TO APPEAR ON THE NEXT COURT DATE.
WAIVES STATUTORY TIME.

NEXT SCHEDULED EVENT:

12/09/15 830 AM PRELIM SETTING/RESETTING DIST VAN NUYS COURTHOUSE DEPT
112
DAY OO OF 30

10/28/15 BAIL TO STAND, # AS50K60527

CUSTODY STATUS: BAIL TO STAND

ON 12/09/15 AT 830 AM IN VAN NUYS COURTHOUSE DEPT 112
CASE CALLED FOR PRELIM SETTING/RESETTING

PARTIES: KAREN J . NUDELL (JUDGE) LYNNE GARCIA (CLERK)

TROYETTE SCOTT (REP) MELANY AVANESSIANS (DA)

DEFENDANT IS PRESENT IN COURT, AND REPRESENTED BY GEORGE MGDESYAN PRIVATE COUNSEL

DEFENDANT ADVISED OF AND PERSONALLY AND EXPLICITLY WAIVES THE FOLLOWING RIGHTS • WRITTEN ADVISEMENT OF RIGHTS AND WAIVERS FILED, INCORPORATED BY REFERENCE HEREIN

JURY TRIAL OR COURT TRIAL AND PRELIMINARY HEARING

CONFRONTATION AND CROSS-EXAMINATION OF WITNESSES;

SUBPOENA OF WITNESSES INTO COURT TO TESTIFY IN YOUR DEFENSE; AGAINST SELF-INCRIMINATION;

DEFENDANT ADVISED OF THE FOLLOWING:

THE NATURE OF THE CHARGES AGAINST HIM, THE ELEMENTS OF THE OFFENSE IN THE COMPLAINT, AND POSSIBLE DEFENSES TO SUCH CHARGES;

THE POSSIBLE CONSEQUENCES OF A PLEA OF GUILTY OR NOLO CONTENDERE, INCLUDING THE MAXIMUM PENALTY AND ADMINISTRATIVE SANCTIONS AND THE POSSIBLE LEGAL EFFECTS

AND MAXIMUM PENALTIES INCIDENT TO SUBSEQUENT CONVICTIONS FOR THE

SAME OR SIMILAR OFFENSES;

THE EFFECTS OF PROBATION;

IF YOU ARE NOT A CITIZEN, YOU ARE HEREBY ADVISED THAT A CONVICTION OF THE OFFENSE FOR WHICH YOU HAVE BEEN CHARGED WILL HAVE THE CONSEQUENCES OF DEPORTATION, EXCLUSION FROM ADMISSION TO THE UNITED STATES, OR DENIAL OF NATURALIZATION PURSUANT TO THE LAWS OF THE UNITED STATES.

THE COURT FINDS THAT EACH SUCH WAIVER IS KNOWINGLY, UNDERSTANDINGLY, AND EXPLICITLY MADE; COUNSEL JOINS IN THE WAIVERS

THE DEFENDANT PERSONALLY WITHDRAWS PLEA OF NOT GUILTY TO COUNT 01 AND PLEADS NOLO CONTENDERE WITH THE APPROVAL OF THE COURT TO A VIOLATION OF SECTION

530. 5(A) pc IN COUNT 01. THE COURT FINDS THE DEFENDANT GUILTY.
COUNT (01) DISPOSITION: CONVICTED COURT ORDERS AND FINDINGS:

-THE COURT ORDERS THE DEFENDANT TO APPEAR ON THE NEXT COURT DATE.

COURT FINDS THAT THERE IS A FACTUAL BASIS FOR DEFENDANT'S PLEA, AND COURT ACCEPTS PLEA.

SENTENCING CONTINUED IN DEPT. 112 TO 1-25-16
NEXT SCHEDULED EVENT:

01/25/16 830 AM PROBATION AND SENTENCE HEARING DIST VAN NUYS COURTHOUSE DEPT 112

12/09/15 BAIL TO STAND, # AS501<60527

CUSTODY STATUS: BAIL TO STAND

ON 01/25/16 AT 830 AM IN VAN NUYS COURTHOUSE DEPT 112
CASE CALLED FOR PROBATION AND SENTENCE HEARING

PARTIES: KAREN J . NUDELL (JUDGE) LYNNE GARCIA (CLERK)

TROYETTE SCOTT (REP)JESSICA M. BALADY (DA)

DEFENDANT PRESENT IN COURT, AND REPRESENTED BY GEORGE MGDESYAN PRIVATE COUNSEL

ATTY CHRISTINA SARKISS APPEARING.

SENTENCING CONTINUED IN DEPT. 112 TO 2-25-16
COURT ORDERS AND FINDINGS:

-THE COURT ORDERS THE DEFENDANT TO APPEAR ON THE NEXT COURT DATE. NEXT SCHEDULED EVENT:

02/25/16 830 AM PROBATION AND SENTENCE HEARING DIST VAN NUYS COURTHOUSE DEPT 112

01/25/16 BAIL TO STAND, # AS501<60527

CUSTODY STATUS: BAIL TO STAND

ON 02/25/16 AT 830 AM IN VAN NUYS COURTHOUSE DEPT 112

CASE CALLED FOR PROBATION AND SENTENCE HEARING

PARTIES: KAREN J . NUDELL (JUDGE) LYNNE GARCIA (CLERK)

, TROYETTE SCOTT (REP) STACEY SOLOMONS (DA)

DEFENDANT IS PRESENT IN COURT, AND REPRESENTED BY ANNA OSIPOV PRIVATE COUNSEL DEFENDANT WAIVES ARRAIGNMENT FOR JUDGMENT AND STATES THERE IS NO LEGAL CAUSE WHY SENTENCE SHOULD NOT BE PRONOUNCED. THE COURT ORDERED THE FOLLOWING JUDGMENT:

AS TO COUNT (01) :
COURT ORDERS PROBATION DENIED.

SERVE 2 YEARS IN COUNTY JAIL , PURSUANT TO pc 1170(H) (1) AND (H) (2)
COURT SELECTS THE MID TERM OF 2 YEARS AS TO COUNT 01.
DEFENDANT GIVEN TOTAL CREDIT FOR 10 DAYS IN CUSTODY 5 DAYS ACTUAL CUSTODY AND 5 DAYS GOOD TIME/WORK TIME

FORTHWITH

PLUS $40.00 COURT OPERATIONS ASSESSMENT (PURSUANT TO 1465 .8(A) (1) P . c .)

$30.00 CRIMINAL CONVICTION ASSESSMENT (PURSUANT TO 70373 G.C.)

$10.00 CRIME PREVENTION FINE (PURSUANT TO 1202.5 P.C.)

COMMIT
MENT
ISSUED
TOTAL
DUE:
$80.00 IN
ADDITIO
N:

-THE DEFENDANT IS TO PAY A RESTITUTION FINE PURSUANT TO SECTION 1202.46) PENAL CODE IN THE AMOUNT OF $300.

COURT ORDERS AND FINDINGS:

-PURSUANT TO PC SECTION 296, THE DEFENDANT IS ORDERED TO PROVIDE BUCCAL SWAB SAMPLES, A RIGHT THUMB PRINT, A FULL PALM PRINT

IMPRESSION OF EACH HAND, ANY BLOOD SPECIMENS OR OTHER BIOLOGICAL SAMPLES AS REQUIRED BY THIS SECTION FOR LAW ENFORCEMENT IDENTIFICATION .

HARVEY WAIVER TAKEN.

COUNT (01) : DISPOSITION:
CONVICTED REMAINING COUNTS
DISMISSED.

COUNT (02) : DISMISSED DUE TO PLEA NEGOTIATION

COUNT (03) : DISMISSED DUE TO PLEA NEGOTIATION
COUNT (04) : DISMISSED DUE TO PLEA NEGOTIATION
COUNT (05) : DISMISSED DUE TO PLEA NEGOTIATION
COUNT (06) : DISMISSED DUE TO PLEA NEGOTIATION
COUNT (07) : DISMISSED DUE TO PLEA NEGOTIATION
DMV ABSTRACT NOT REQUIRED NEXT SCHEDULED EVENT:

PROCEEDINGS TERMINATED

02/25/16 EXONERATED, # AS50K60527

CUSTODY STATUS: BAIL EXONERATED

ON 02/29/16 AT 900 AM:

COUNTY JAIL ABSTRACT PACKET COMPLETED AND FORWARDED TO COUNTY

JAIL VIA SHERIFF'S TRANSPORT. ABSTRACT COMPLETED BY A. BERGIN

03/04/16 ARREST DISPOSITION REPORT SENT VIA FILE TRANSFER TO DEPARTMENT OF
J USTICE

Anexo IV – Mandado Caso Paytsar Bkhchadzhyan

ORIGINAL

AO 93 (Rev. 12/09) Search and Seizure Warrant (USAO CDCA Rev. 01/2013)

UNITED STATES DISTRICT COURT

for the

Central District of California

FILED
2016 MAR 15 PM 3:34
CLERK U.S. DIST. COURT
CENTRAL DIST. CALIF.
LOS ANGELES

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
iPhone seized from [redacted] in Glendale, California

Case No. 16-03 98M

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Central District of California
(identify the person or describe the property to be searched and give its location):

See Attachment A

The person or property to be searched, described above, is believed to conceal *(identify the person or describe the property to be seized)*:

See Attachment B

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property. Such affidavit(s) or testimony are incorporated herein by reference and attached hereto.

YOU ARE COMMANDED to execute this warrant on or before 14 days from the date of its issuance
(not to exceed 14 days)

☑ in the daytime 6:00 a.m. to 10 p.m. ☐ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge on duty at the time of the return through a filing with the Clerk's Office.
(name)

☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)* ☐ for _____ days *(not to exceed 30)*.

☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 2/25/2016 12:28 pm

Alicia G. Rosenberg
Judge's signature

City and state: Los Angeles, California

Honorable Alicia G. Rosenberg, U.S. Magistrate Judge
Printed name and title

AUSA: Vicki Chou (x8692)

AO 93 (Rev. 12/09) Search and Seizure Warrant (Page 2)

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
LA-6908698	2/25/2016 1:00PM	LASD LOCKUP SUPERVISOR

Inventory made in the presence of :
N/A

Inventory of the property taken and name of any person(s) seized:
[Please provide a description that would be sufficient to demonstrate that the items seized fall within the items authorized to be seized pursuant to the warrant (e.g., type of documents, as opposed to "miscellaneous documents") as well as the approximate volume of any documents seized (e.g., number of boxes). If reference is made to an attached description of property, specify the number of pages to the attachment and any case number appearing thereon.]

ARTSAR BKCHARZHYAN - FINGERPRINT ON iPHONE DEVICE.

Certification (by officer present during the execution of the warrant)

I declare under penalty of perjury that I am an officer who executed this warrant and that this inventory is correct and was returned along with the original warrant to the designated judge through a filing with the Clerk's Office.

Date: 2/25/2016

Executing officer's signature

SPECIAL AGENT RAYMOND Y. MARTINEZ III

Printed name and title

AUSA: Vicki Chou (x8692)

ATTACHMENT A

For the following Target Subject, law enforcement may undertake the activity described in Attachment B.

Paytsar Bkhchadzhyan

ATTACHMENT B

Law enforcement personnel are authorized to depress the fingerprints and/or thumbprints of the person covered by this warrant onto the Touch ID sensor of the Apple iPhone seized from [redacted] Glendale, California 91214 on February 25, 2016.

Anexo V – *Memorandum* do Caso de 9 de Maio de 2016

Case [redacted]

EILEEN M. DECKER
United States Attorney
LAWRENCE S. MIDDLETON
Assistant United States Attorney
Chief, Criminal Division
J. MARK CHILDS (Cal. Bar No. 162684)
Assistant United States Attorney
OCDETF Section
1400 United States Courthouse
312 North Spring Street
Los Angeles, California 90012
Telephone: (213) 894-2433
Facsimile: (213) 894-0142
E-mail: mark.childs@usdoj.gov

Attorneys for Plaintiff
UNITED STATES OF AMERICA

FILED
CLERK, U.S. DISTRICT COURT
MAY - 9 2016
CENTRAL DISTRICT OF CALIFORNIA
BY DEPUTY

UNITED STATES DISTRICT COURT

FOR THE CENTRAL DISTRICT OF CALIFORNIA

IN RE THE SEARCH OF [redacted]

No. [redacted]

NOTICE OF FILING MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT OF SEARCH WARRANT APPLICATION

Plaintiff United States of America, by and through its counsel of record, the United States Attorney for the Central District of California and Assistant United States Attorney J. MARK CHILDS, hereby files its Notice of Filing Memorandum of Points and Authorities in Support of Search Warrant Application.

This Notice is based upon the attached memorandum of points and authorities, the files and records in this case including the

///

[redacted]

application and search warrant filed in this matter, and such further evidence and argument as the Court may permit.

Dated: May 9, 2016

Respectfully submitted,

EILEEN M. DECKER
United States Attorney

LAWRENCE S. MIDDLETON Assistant
United States Attorney
Chief, Criminal Division

/s/
J. MARK CHILDS
Assistant United States Attorney

Attorneys for Plaintiff
UNITED STATES OF AMERICA

[redacted]

MEMORANDUM OF POINTS AND AUTHORITIES

I. INTRODUCTION

The government submits this supplemental authority in support of its application for a search warrant which seeks authorization to depress the fingerprints and thumbprints of every person who is located at the SUBJECT PREMISES during the execution of the search and who is reasonably believed by law enforcement to be a user of a fingerprint sensor-enabled device that is located at the SUBJECT PREMISES and falls within the scope of the warrant. The government seeks this authority because those fingerprints, when authorized by the user of the device, can unlock the device.

This procedure will not vi Attached hereto is an article from the Daily Journal dated Friday, May 6, 2016, entitled "Thumbprints to unlock phones can be compelled, courts say."

II. FACTUAL BACKGROUND

In the affidavit in support of the search warrant, the affiant states that Apple Inc., Motorola, HTC, and Samsung, among other companies, produce devices that can be unlocked by the user with a numerical or an alpha-numerical password, or, for some newer versions of the devices, with a fingerprint placed on a fingerprint sensor. Each company has a different name for its fingerprint sensor feature; for example, Apple's is called "Touch ID." Once a user has set up the fingerprint sensor feature in the security settings of the device, the user can unlock the device by placing a finger or thumb on the device's fingerprint sensor. If that sensor recognizes the fingerprint or thumbprint, the device unlocks. Most devices can be set up to recognize multiple prints, so that different prints, not

[redacted]

necessarily from the same person, will unlock the device. If there is no sensor on the device, the device will not open with prints.

There are limits on the ability to use a fingerprint or thumbprint to unlock a device, which varies by manufacturer. For example, with Apple, the Touch ID feature only permits up to five attempts with a print before the device will require the user to enter a passcode. Furthermore, the Touch ID feature will not substitute for the use of a passcode or password if more than 48 hours have passed since the device has been unlocked; in other words, if more than 48 hours have passed since the device was accessed, the device will require the passcode or password programmed by the user and will not allow access to the device based on a print alone. Similarly, Touch ID will not allow access if the device has been restarted or was off and has been turned on, if the device has received a remote lock command, or if five attempts to match a print have been unsuccessful. Other brands have similar restrictions.

In order to attempt to gain access to the devices found at the SUBJECT PREMISES, the search warrant seeks the authority to use the fingerprints and thumbprints of any person who is located at the SUBJECT PREMISES during the execution of the search and who is reasonably believed by law enforcement to be a user of a fingerprint sensor-enabled device that is located at the SUBJECT PREMISES and falls within the scope of the warrant. Without the numerical or alpha-numerical passcode, the government may not be able to obtain the contents of the devices if those prints are not used. Furthermore, delaying action may prevent even the use of this method of gaining access if that delay prevents the government from attempting to access the device beyond 48 hours since the last time

[redacted]

the device was accessed. It is not known which finger(s) or thumb of which person(s) will unlock the device, but in any event all that would result from successive failed attempts is the requirement to use the authorized passcode or password.

III. LEGAL DISCUSSION

Compelling a person to provide a fingerprint or thumbprint as part of a search warrant violates neither the Fifth nor the Fourth Amendment.

A. The Fifth Amendment Presents No Barrier to Obtaining a Person's Fingerprints

Compelling a person to provide his or her fingerprint does not implicate, let alone violate, the Fifth Amendment. "[B]oth federal and state courts have usually held that [the Fifth Amendment] offers no protection against compulsion to submit to fingerprinting." Schmerber v. California, 384 U.S. 757, 764 (1966). That is so because the Fifth Amendment privilege against self-incrimination only prevents the use against an accused[1] of testimonial or communicative evidence obtained from him. Id. As the Supreme Court explained in Schmerber, that prohibition does not apply to the use of a person's "body as evidence when it may be material." Id. at 763 (quoting Holt v. United States, 218 U.S. 245, 252-53 (1910)); see United States v. Dionisio, 410 U.S. 1, 5-6 (1973) ("It has long been held that the compelled display of identifiable physical characteristics infringes no interest protected by the privilege against compulsory self-incrimination."). The Ninth Circuit has held the same: "requests by

[1] It is, moreover, worth noting that the Fifth Amendment protects the accused, and as of this point, no person is being accused.

[redacted]

the prosecution for . . . fingerprint evidence from a defendant or a suspect are not prohibited by the Fifth Amendment right against self-incrimination because such evidence is not testimonial in nature." Commonwealth of Northern Mariana Islands v. Bowie, 243 F.3d 1109, 1120 n.5 (9th Cir. 2001); see also United States v. De Palma, 414 F.2d 394, 397 (9th Cir. 1969) ("Identifying physical characteristics are not evidence of a testimonial nature."); United States v. Sanudo-Duarte, 2016 WL 126283 (D. Ariz. 2016) (holding that defendant could be compelled to provide exemplar of his palm prints); Virginia v. Baust, CR14-1439 (Va. Cir. Ct. Oct. 28, 2014) (holding that defendant could be compelled to provide his fingerprint in order to unlock phone)

While the government does not know ahead of time the identity of every digital device or fingerprint (or indeed, every other piece of evidence) that it will find in the search, it has demonstrated probable cause that evidence may exist at the search location, and needs the ability to gain access to those devices and maintain that access to search them. For that reason the warrant authorizes the seizure of "passwords, encryption keys, and other access devices that may be necessary to access the device." A password, "key," or use of a fingerprint are all means of gaining access to other spaces or devices, and are seizable both to gain and maintain access. See, e.g., United States v. Shi, 525 F.3d 709, 731 (9th Cir. 2008) (authorizing seizure of keys and identification cards to show indicia of ownership); United States v. Honore, 450 F.2d 31, 33 (9th Cir. 1971). The fact that a successful unlocking of the device could also demonstrate a connection between the person and the device thus does not make the requested fingerprints testimonial, any more than does a

[redacted]

warrant's authorization to seize a person's keys. If anything, the connection raises a Fourth Amendment concern, which is discussed and dispatched below. Finally, as law enforcement will only be seeking to depress the fingerprints of those persons present at the search location for whom law enforcement has cause to believe may be a user of a device, neither the Fifth nor Fourth Amendment is violated.

B. The Fourth Amendment Permits the Acquisition of the Fingerprints

The requested warrant also does not violate anyone's Fourth Amendment rights. It is true that the Fourth Amendment is implicated when the government seeks fingerprints for investigatory purposes. See, e.g., United States v. Parga-Rosas, 238 F.3d 1209, 1215 (9th Cir. 2001); but see Dionisio, 410 U.S. at 4 ("The Fourth Amendment prohibition against unreasonable search and seizure applies only where identifying physical characteristics, such as fingerprints, are obtained as a result of unlawful detention of a suspect, or when an intrusion into the body, such as a blood test, is undertaken without a warrant, absent an emergency situation."). But the Fourth Amendment's requirements are satisfied when the taking of fingerprints is supported by reasonable suspicion. See Hayes v. Florida, 470 U.S. 811, 817 (1985) ("There is thus support in our cases for the view that the Fourth Amendment would permit seizures for the purpose of fingerprinting, if there is reasonable suspicion that the suspect has committed a criminal act, if there is a reasonable basis for believing that fingerprinting will establish or negate the suspect's connection with that crime, and if the procedure is carried out with dispatch."); United States v. Garcia-Beltran, 389 F.3d 864, 868 (9th Cir. 2004) ("[T]he Court has reaffirmed the

[redacted]

principle that the Fourth Amendment does not permit admission of fingerprint evidence resulting from a seizure without reasonable suspicion"); but see Davis v. Mississippi, 394 U.S. 721, 728 (1969) (holding that warrantless "dragnet" investigatory "[d]etentions for the sole purpose of obtaining fingerprints are no less subject to the constraints of the Fourth Amendment. It is arguable, however, that, because of the unique nature of the fingerprinting process, such detentions might, under narrowly defined circumstances, be found to comply with the Fourth Amendment even though there is no probable cause in the traditional sense.").

A fortiori, a search warrant based on probable cause, such as that sought here, would satisfy the Fourth Amendment, especially since law enforcement will not obtain the fingerprints from any person for whom they do not have cause to believe may be a user of a device. Because there is probable cause sufficient to seize the digital device, there is probable cause sufficient to seize "the key" to that device in the form of a person's fingerprint - similar to the provisions in the warrant to seize other keys. Moreover, while executing this provision of the search warrant may result in a brief detention of persons found at the Subject Premises, this too is consistent with Hayes because it will be done "with dispatch" and because it is done pursuant to the judicial authorization sought here. 470 U.S. at 814; see also Michigan v. Summers, 452 U.S. 692, 705 (1981) (a valid search warrant implicitly carries with it the limited authority to briefly detain the occupants on, or in the immediate vicinity of, the premises while the search is being conducted); United States v. Broussard, 80 F.3d 1025, 1033 (5th Cir. 1996) (holding that 10-to 15-minute detention of occupant was

[redacted]

reasonable while agents searched occupant's residence pursuant to valid search warrant).

IV. CONCLUSION

The government respectfully requests that the search warrant be issued with the procedures permitting the law enforcement personnel to depress the fingers of every person who is located at the SUBJECT PREMISES during the execution of the search and who is reasonably believed by law enforcement to be a user of a fingerprint sensor-enabled device that is located at the SUBJECT PREMISES and falls within the scope of the warrant.

ÍNDICE