INTERCEÇÃO DE COMUNICAÇÕES PARA PROVA DOS CRIMES DE INJÚRIAS, AMEAÇAS, COAÇÃO, DEVASSA DA VIDA PRIVADA E PERTURBAÇÃO DA PAZ E DO SOSSEGO COMETIDOS POR MEIO DIFERENTE DO TELEFONE*

Sónia Raquel da Cruz Lopes

Abstract: *As an occult method of investigation, the interception of communications is an essential measure for investigating so-called computer crime, as it enables the competent authorities to obtain information relevant to the investigation and to gather the evidence necessary for punish the perpetrator of the crime. However, as a hidden method of investigation it is subject to the verification of certain requirements, being restricted to a catalog of crimes. Thus, we intend to understand whether the Portuguese legislator totally ignored the interests of the investigation in favor of the protection of fundamental rights, making it impossible to intercept communications for the proof of crimes of injury, coercion, deprivation of privacy and disturbance of peace and quiet or if on the contrary it allows the use of this means of obtaining evidence to prove the crimes referred to.*

Sumário: 1. Introdução. 2. A interceção de comunicações. 2.1. Em que consiste a interceção de comunicações?. 2.2. A interceção de comunicações enquanto método oculto de investigação. 3. A interceção de comunicações para prova dos crimes previstos no artigo 187.º, n.º 1, al. *e)*, do CPP, quando tais crimes são praticados por meio diferente do telefone. 3.1. A interceção de comunicações enquanto meio de obtenção de prova que comporta necessariamente a restrição do direito ao sigilo nas telecomunicações e, como tal, dependente de previsão legal, sob pena de originar uma proibição de prova. 3.2. Âmbito de aplicação do artigo 18.º, da Lei do Cibercrime. 3.3. Será possível recorrer à interceção de comunicações prevista no artigo 18.º, da Lei do Cibercrime para prova dos crimes de injúria, ameaça, coação, devassa da vida privada e perturbação da paz e do sossego quando cometidos por meio diferente do telefone?. 4.Conclusão.

Este artigo corresponde, no essencial, ao relatório apresentado na unidade curricular de Direito Penal IV do mestrado profissionalizante em Ciências Jurídico-Forenses da Faculdade de Direito da Universidade de Lisboa, em maio de 2016, sob orientação do Professor Doutor Paulo de Sousa Mendes.

1. INTRODUÇÃO

Com este estudo, pretendemos perceber melhor o regime da interceção de comunicações previsto no artigo 18.º, da Lei do Cibercrime (LC), nomeadamente se tal meio de obtenção de prova pode ser utilizado para a prova dos crimes de injúria, ameaça, coação, devassa da vida privada e perturbação da paz e do sossego, quando tais crimes são praticados por via informática.

Como sabemos, o Processo Penal tem por finalidade quer a descoberta da verdade material, a realização da justiça e o restabelecimento da paz jurídica, como também a proteção de direitos fundamentais. E, muitas vezes, estas finalidades entram em conflito e há necessidade de se proceder à restrição de direitos fundamentais, nomeadamente, Direitos, Liberdades e Garantias (DLG) e tal é permitido pela nossa Constituição da República Portuguesa (CRP), pelos artigos 18.º, n.º 2 e 34.º, n.º 4, pois se o primeiro estabelece que "a lei só pode restringir os direitos, liberdades e garantias, nos casos expressamente previstos na Constituição, devendo as restrições limitar-se ao necessário para salvaguardar outros direitos ou interesses constitucionalmente protegidos", o segundo determina que as "ingerências das autoridades públicas na correspondência, nas telecomunicações e nos demais meios de comunicação" não são proibidos "nos casos previstos na lei em matéria de processo criminal".

Ora, a interceção de comunicações constitui um desses casos, uma vez que implica necessariamente a restrição de direitos fundamentais. Todavia, tendo em consideração que este meio de obtenção de prova é um método oculto de investigação a sua aplicação é estritamente excecional e está sujeita a determinados pressupostos, como a existência de um catálogo de crimes.

Resta saber se este catálogo de crimes não veda a possibilidade de realizar uma interceção de comunicações para prova dos crimes de injúria, ameaça, coação, devassa da vida privada e perturbação da paz e do sossego, quando tais crimes são praticados através de um meio informático, como por exemplo o correio eletrónico, uma vez que o artigo 187.º do Código de Processo Penal (CPP) só permite a realização de uma interceção telefónica quando tais crimes são cometidos através do telefone. Parece-nos, todavia, que tal problema já encontra uma resposta na própria lei, mas de todo o modo, somos da opinião que não se justificaria uma tutela processual penal superior para as ofensas cometidas através do telefone.

Assim, optámos por dividir este estudo em dois grandes capítulos: no primeiro capítulo iremos debruçar-nos muito resumidamente sobre o conceito de interceção de comunicações, bem como abordaremos o facto da interceção de

comunicações ser um método oculto de investigação, o que acarreta maiores restrições aos direitos fundamentais e, por isso, deve obedecer a determinados pressupostos materiais, formais-procedimentais e orgânicos para que seja válida e legítima. Por sua vez, no segundo capítulo procederemos à análise do problema concreto, onde nos iremos debruçar, em primeiro lugar, na restrição do direito ao sigilo nas telecomunicações, tendo em consideração que se atendermos somente à redação da al. *e)*, do n.º 1, do artigo 187.º do CPP, a lei apenas possibilita o recurso à interceção de comunicações para prova dos crimes de injúria, ameaça, coação, devassa da vida privada e perturbação da paz e do sossego quando tais crimes são praticados através do telefone, pelo que a extensão a outros meios informáticos poderá consubstanciar uma intromissão ilegítima no direito ao sigilo das comunicações eletrónicas, o que, eventualmente, poderá dar lugar a uma proibição de prova, por falta de uma lei que legitime o recurso a este meio de obtenção de prova quando tais crimes são praticados por outro meio. Posteriormente, falaremos do âmbito de aplicação material do artigo 18.º, n.º 1, da LC, de modo a perceber qual o catálogo de crimes que pode legitimar o recurso a este meio de obtenção de prova e, por fim, iremos responder à questão por nós colocada, de modo a esclarecer se a lei prevê ou não o recurso à interceção de comunicações quando os crimes previstos na al. *e)*, do n.º 1, do artigo 187.º do CPP são praticados por meio diferente do telefone.

2. A INTERCEÇÃO DE COMUNICAÇÕES

2.1. Em que consiste a interceção de comunicações

Em conformidade com o disposto no artigo 2.º, al. *e)*, da LC, a interceção é "o ato destinado a captar informações contidas num sistema informático, através de dispositivos eletromagnéticos, acústicos, mecânicos ou outros".

A doutrina italiana, à semelhança da lei portuguesa, para considerar uma dada operação como "interceção", considera fundamental a utilização adequada de um meio mecânico ou eletrónico de forma a superar a normal capacidade dos sentidos[1]. Por sua vez, a jurisprudência italiana, definiu interceção como a captação de uma comunicação dirigida a uma terceira pessoa que é realizada

1 Neste sentido, Fumu, 1990: 774, citando "utilizzazione di mezzi meccanici od eletronici idonei a suiperare le normali capacità de sensi".

sem impossibilitar a sua prossecução e sem que os interlocutores, ou pelo menos um deles, disso tomem conhecimento, consistindo na apreensão em tempo real do conteúdo de uma comunicação em curso[2].

Também o Acórdão do Tribunal da Relação de Lisboa, de 15 de julho de 2008[3], refere que "todas as comunicações por via eletrónica ocorrem durante certo lapso de tempo. Começam quando entram na rede e acabam quando saem da mesma"[4]. No entendimento de Pedro Verdelho[5], a comunicação é uma realidade dinâmica, vai de um lado para o outro, entre um emissor e um recetor. As mensagens de correio eletrónico, por exemplo, são uma comunicação enquanto circulam nas redes, entre o computador de origem e o de destino e é precisamente enquanto a comunicação circula nas redes que a interceção pode ser efetuada.

Deste modo, podemos chegar à conclusão que esta captação de informações ocorre em tempo real, isto é, no próprio momento em que a comunicação é efetuada ou, como refere Pedro Venâncio, "no seu trajeto do computador do emissor para o computador do recetor através da rede de servidores"[6].

Desta forma, Paulo Dá Mesquita refere que a interceção de comunicações é "outra via de intromissão processual no conteúdo das comunicações de correio eletrónico ou de natureza semelhante, é uma outra forma de «acesso legítimo a sistema informático», para além da busca informática"[7].

Com efeito, o artigo 18.º, da LC, que prevê o regime jurídico da interceção de comunicações aplica-se à interceção de dados de conteúdo e dados de tráfego, mas somente enquanto as comunicações ainda estão em curso[8]. Assim, "quando o momento do seu recebimento já pertence ao passado, qualquer contacto com a comunicação feita não tem qualquer correspondência com a

---

2 Neste sentido, Sentenza n.º 6 del 2000, Cassazione Penale, Sezioni Unite, 23 Febbraio 2000, Roma, onde refere que interceção telefónica consiste "nella captazione di comunicazioni che si svolgono fra terze persone realizzata senza impedirne la prosecuzione e senza che gli interlocutori (o almeno uno di essi) ne siano a conoscenza" e, posteriormente, refere que a interceção "consiste nel'apprensione in tempo reale del contenuto di una comunicazione in corso".

3 Proc. n.º 3453/2008-5.

4 *Idem*: 10.

5 Neste sentido, Verdelho, 2008: 164.

6 Venâncio, 2006: 22.

7 Mesquita, 2010: 120.

8 Neste sentido ver também Acórdãos do Tribunal da Relação de Évora, de 6 de janeiro de 2015, Proc. n.º 6793/11.2TDLSB-A.E1: 1; e de 20 de janeiro de 2015, Proc. n.º 648/14.6GCFAR-A.E1: 1.

ideia de interceção. As mensagens que depois de recebidas, ficam gravadas no recetor deixam de ter a natureza de comunicação em transmissão"[9], pelo que o regime a aplicar já não será o da interceção de comunicações.

2.2. A interceção de comunicações enquanto método oculto de investigação

Do exposto podemos retirar que a interceção de comunicações se trata de um método oculto de investigação, uma vez que os visados pela diligência só tomam conhecimento depois da medida ter sido levada a cabo.

Nas palavras de Manuel da Costa Andrade, "os métodos ocultos de investigação representam uma intromissão nos processos de ação, interação e comunicação das pessoas concretamente visadas, sem que estas tenham conhecimento do facto nem dele se apercebam"[10] e, por isso, continuam a interagir espontaneamente, podendo dessa forma contribuir para a sua autoincriminação.

No entanto, num verdadeiro Estado de Direito Democrático, como é o nosso, tal método de investigação oculto para subsistir tem que ser compatível com o núcleo essencial da dignidade da pessoa humana. Deste modo, o emprego de um método oculto de investigação, como o é a interceção de comunicações, tem de garantir a não ingerência naquela área nuclear da intimidade que é imprescindível para se salvaguardar a dignidade da pessoa humana. Desta forma, como menciona Rita Castanheira Neves, "é fundamental impor limites na investigação mesmo do criminoso mais hediondo, pois só assim se garantirá que há um espaço irredutível de dignidade humana que não é abalada pelas instâncias formais de controlo, as quais agem – não se pode esquecer – no cumprimento dos desígnios de um Estado de Direito"[11].

Com efeito, quando são alvo de um método oculto de investigação como a interceção de comunicações, os sujeitos visados pela diligência, uma vez que só tomam conhecimento da mesma quando esta já se encontra consumada, não têm qualquer possibilidade de reação ou defesa quanto a essa interceção, ainda que a mesma tenha sido regularmente decretada, o que significa que, tais meios de obtenção de prova, pela sua natureza oculta, sacrificam, no plano adjetivo-processual, o direito a recusar o testemunho, o princípio *nemo tenetur*

---

9 Acórdão do Tribunal da Relação de Lisboa, de 17 de julho de 2008, Proc. n.º 3453/2008-5: 10-11.

10 Costa Andrade, 2009: 105.

11 Neves, 2011: 98.

se ipsum accusare, e o direito ao silêncio, ao permitirem "a obtenção fraudulenta de "confissões" inconscientes e, como tais, não livres"[12].

Além disso, no plano material-substantivo, os métodos ocultos de investigação restringem diversos direitos fundamentais, não só do visado pela diligência, mas dos terceiros que com ele comunicam, designadamente o direito à reserva da intimidade da vida privada e familiar, o direito à inviolabilidade da correspondência e demais comunicações privadas e o direito à autodeterminação informacional e comunicacional.

Desta forma, o recurso à interceção de comunicações, enquanto método oculto de investigação, apresenta um elevado potencial de danosidade social, na medida em que comporta irremediavelmente a restrição de direitos fundamentais, pelo que só deve ser admitido excecionalmente, em função da verificação de determinados pressupostos cuja não verificação tornará ilegítimo o uso de tal meio (proibição de produção) e afetará também a possibilidade da sua valoração (proibição de valoração).

Como primeiro pressuposto temos, desde logo, o princípio da reserva de lei[13], isto é, só a lei (da Assembleia da República ou decreto-lei autorizado) pode autorizar e legitimar esta medida, em conformidade com o disposto nos artigos 18.º, n.º 2 e 165.º, n.º 1, al. *c)*, da CRP.

Todavia, como refere Manuel da Costa Andrade, "a lei deve permitir identificar com rigor e segurança tanto o bem jurídico ou o direito fundamental lesado ou atingido como o teor do respetivo sacrífico"[14]. A lei deve, ainda, identificar aquilo que a jurisprudência constitucional alemã apelida de "princípio da vinculação ao fim", ou seja, deve indicar o fundamento, o fim e os limites da interceção, de uma forma precisa e clara.

Como segundo pressuposto, exige-se a existência de um "catálogo" de crimes que legitimarão a interceção de comunicações. No entanto, tal catálogo deverá ser restrito a infrações suficientemente graves que justifiquem o recurso a este método oculto e deverá ser sempre definido segundo critérios de proporcionalidade. Consequentemente, a existência de um catálogo de

---

12 Costa Andrade, 2009: 107.

13 Também Víctor Moreno Catena alerta para a necessidade das diligências desta fase do processo penal respeitarem as leis em estrita conformidade com o princípio da legalidade. Neste sentido ver Catena, 2008: 78, onde refere "*como actividad realizada por servidores públicos y tendente al ejercicio del poder punitivo del Estado, las diligencias de esta fase del procedimiento deben sujetarse a las disposiciones legales, y practicarse, por tanto, cumpliendo estrictamente el principio de legalidad*".

14 Costa Andrade, 2009: 112.

crimes, torna inaplicável este meio de obtenção de prova a outro tipo de crimes.

O terceiro pressuposto para que a interceção de comunicações seja admissível é a verificação de uma "suspeita fundada em factos concretos e medidos a partir de critérios de plausibilidade e probabilidade"[15] da ocorrência da infração. Suspeita esta que terá de reportar-se ao momento em que a interceção de comunicações é autorizada pela autoridade competente.

O quarto pressuposto diz respeito à necessidade de se atender ao princípio da subsidiariedade, quer em relação aos outros métodos ocultos disponíveis, quer em relação aos métodos não ocultos. Desta forma, não deve recorrer-se à interceção de comunicações quando for possível alcançar o mesmo resultado recorrendo a um método não oculto. Todavia, se for necessário recorrer a um método oculto de investigação dever-se-á recorrer sempre ao que for menos lesivo.

De acordo com o quinto pressuposto e em conformidade com o disposto no artigo 18.º, da CRP, o recurso à interceção de comunicações deverá obedecer ao princípio da proporcionalidade. Este princípio deve estar presente quer no momento da escolha dos crimes que vão integrar o catálogo, quer no fundamento da suspeita, quer na ideia de subsidiariedade. Para além disso, Manuel da Costa Andrade refere a necessidade de se observar o princípio da proporcionalidade em sentido estrito, o que significa que "numa ponderação global, a gravidade da intromissão não seja desproporcionada face ao peso das razões que a justificam"[16].

O sexto pressuposto para que a interceção de comunicações seja legítima é a necessidade de salvaguardar a área nuclear da intimidade dos visados, pois só assim se salvaguardará o princípio fundamental da dignidade da pessoa humana.

Por último, temos um pressuposto de caráter orgânico-procedimental, relativo à entidade competente para decidir sobre a medida ou autorizar a sua realização. Tal competência deve estar sempre reservada ao juiz, salvo nos casos de "perigo na demora". Pretende-se, com a reserva do juiz, a tutela preventiva dos direitos fundamentais dos visados, pois, tal como refere João Conde Correia, só ao juiz compete declarar, no caso concreto, "qual dos interesses deve prevalecer. Se o interesse punitivo do Estado, se os direitos fundamentais, cuja restrição se pretende"[17].

---

15 Rodrigues, 2010: 56.

16 Costa Andrade, 2009: 116.

17 Correia, 1999: 61.

3. A INTERCEÇÃO DE COMUNICAÇÕES PARA PROVA DOS CRIMES PREVISTOS NO ARTIGO 187.º, N.º 1, AL. *E)*, DO CPP, QUANDO TAIS CRIMES SÃO PRATICADOS POR MEIO DIFERENTE DO TELEFONE

3.1. A interceção de comunicações enquanto meio de obtenção de prova que comporta necessariamente a restrição do direito ao sigilo nas telecomunicações e, como tal, dependente de previsão legal, sob pena de originar uma proibição de prova

Como sabemos, o que está em causa no âmbito da interceção de comunicações é um valor constitucional – o da garantia do sigilo nas comunicações, constitucionalmente tutelado. Tal direito está também consagrado em alguns diplomas de direito internacional, nomeadamente, no artigo 12.º da Declaração Universal dos Direitos do Homem (DUDH), no artigo 17.º do Pacto Internacional de Direitos Civis e Políticos (PIDCP), no artigo 8.º da Convenção Europeia dos Direitos do Homem (CEDH) e no artigo 7.º da Carta dos Direitos Fundamentais da União Europeia (CDFUE).

Ao contrário do que sucede noutros países europeus, em Portugal o direito ao sigilo das comunicações (eletrónicas) tem um tratamento autónomo no artigo 34.º da CRP, que estabelece que "O domicílio e o sigilo da correspondência e dos outros meios de comunicação privada são invioláveis", acrescentando, o n.º 4 do mesmo preceito legal que "é proibida a ingerência das autoridades públicas na correspondência, nas telecomunicações e nos demais meios de comunicação…".

Além disso, o artigo 32.º, n.º 8, da CRP confere uma proteção constitucional reforçada ao sigilo nas comunicações eletrónicas, uma vez que comina com a nulidade as provas obtidas mediante abusiva intromissão na vida privada e nas telecomunicações.

Como referem Gomes Canotilho e Vital Moreira[18], "o conteúdo do direito ao sigilo da correspondência e dos outros meios de comunicação privada abrange toda a espécie de correspondência de pessoa para pessoa (…) e todas as telecomunicações (telefone, telegrama, telefax, etc.). A garantia do sigilo abrange não apenas o conteúdo da correspondência, mas o «tráfego» como tal (espécie, duração, intensidade de utilização)". Acrescentam ainda, estes autores, que "a Constituição não apenas garante o sigilo da correspondência e dos outros meios de comunicação privados (n.º 1) mas também proíbe toda a ingerência".

18 Gomes Canotilho e Vital Moreira, 2007: 544-545.

Também Pedro Gonçalves[19] refere que este direito abrange quer a proibição do acesso não autorizado de terceiros ao conteúdo das comunicações, a chamada vigilância ou interceção de comunicações, quer a proibição da divulgação e utilização por terceiros desse conteúdo e das circunstâncias (tais como a hora, a duração, os endereços, etc.) das comunicações estabelecidas.

No entanto, o direito ao sigilo das comunicações eletrónicas não é um direito absoluto e, por isso, nos termos da parte final do n.º 4, do artigo 34.º da CRP admite-se restrições em sede de processo criminal, cabendo à lei ordinária definir os limites em que essas restrições podem ter lugar. Como refere João Conde Correia, "a intervenção restritiva do legislador ordinário terá que constar da lei ou decreto-lei autorizado, com carácter geral e abstrato e não retroativo"[20].

De acordo com Benjamim Silva Rodrigues, "a inexistência de previsibilidade legal implicará a deslegitimação do uso de tais métodos ocultos de investigação"[21].

No entendimento de Manuel da Costa Andrade[22], a evolução tecnológica não tem "como reverso necessário e automático, o alargamento das autorizações legais de compressão ou invasão preexistentes, que terão de ser interpretadas e aplicadas no estrito respeito pelos seus limites legais". Deste modo, conclui dizendo que "o recurso a um novo meio técnico (oculto e invasivo) de investigação em processo penal só é possível depois de prévia – explícita e autónoma – legitimação legal".

Desta forma, caso não exista uma norma legal que permita o recurso à interceção de comunicações para a prova dos crimes de injúria, ameaça, coação, devassa da vida privada e perturbação da paz e do sossego, quando cometidos por meio informático, tal possibilidade só é admissível quando tais crimes sejam praticados através do telefone, tendo em consideração que o catálogo de crimes previsto no artigo 187.º, n.º 1, do CPP apresenta um elenco taxativo, o recurso a este meio de obtenção de prova só é admissível quando tais crimes são praticados através do telefone.

Nesta medida, atento somente ao artigo 187.º, n.º 1, al. *e)*, do CPP, a interpretação extensiva deste meio de obtenção de prova quando os crimes previstos

19 Gonçalves, 1999: 190.

20 Correia, 1999: 59.

21 Rodrigues, 2010: 54-55.

22 Costa Andrade, 2009: 113.

neste preceito legal são praticados por outro meio parece ter como consequência a intromissão ilegítima no direito ao sigilo das comunicações eletrónicas, por violar o princípio da legalidade[23].

Ora, nestes casos, à semelhança do que prevê o artigo 32.º, n.º 8, da CRP, os artigos 190.º e 126.º, n.º 3, do CPP preveem o regime da nulidade da prova como consequência da não verificação dos pressupostos exigidos, neste caso a não conformidade com o princípio da legalidade.

No entendimento de Paulo Pinto de Albuquerque[24], o artigo 126.º, n.º 3, do CPP comina uma nulidade relativa para a intromissão ilegítima nas telecomunicações, pois é sanável pelo consentimento *a posteriori* do titular do direito. Como refere o mesmo Autor, "a legitimidade para o consentimento depende da titularidade do direito em relação ao qual se verificou a intromissão ilegal. O consentimento pode ser dado *ex ante* ou *ex post* facto. Se o titular do direito pode consentir na intromissão na vida jurídica do seu direito, ele também pode renunciar expressamente à arguição da nulidade ou aceitar expressamente os efeitos do ato, tudo com consequência da sanação da nulidade da prova proibida."[25]

Também Manuel da Costa Andrade refere que "nas hipóteses previstas no n.º 3, *o consentimento afasta a proibição*: tanto a proibição de produção como a respetiva consequência. Consequência que persiste a *mesma – nulidade/proibição de valoração – se não houver consentimento*". Pelo contrário, "na constelação do n.º 1 a consequência – *nulidade/proibição de valoração* – persiste invariavelmente a mesma, haja ou não consentimento da pessoa atingida"[26].

No entendimento de Paulo de Sousa Mendes, "a tortura, a coação 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, por isso mesmo que a proibição agora é afastada quer pelo acordo do titular dos direitos em causa, quer pelas restrições à inviolabilidade desses direitos constantes do art. 34.º, n.os 2, 3 e 4, da CRP". Acrescenta ainda o mesmo Autor que "o art. 126.º repete a citada distinção entre as proibições absolutas e as proibições relativas de obtenção de provas. No caso do art. 126.º,

23 Neste sentido, Acórdão do Tribunal da Relação de Évora, de 5 de junho de 2012, Proc. n.º 12/12.1YREVR: 4.

24 Albuquerque, 2011: 335.

25 *Ibidem* (destaques eliminados).

26 Costa Andrade, 2009: 137.

n.os 1 e 2, 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 art. 126.º, n.º 3, a proibição é afastada pelo acordo do titular dos direitos em causa, ou então é removida mediante as ordens ou autorizações emanadas de certas autoridades, nos termos da lei."[27] Todavia, Paulo de Sousa Mendes salienta que "o art. 126.º, n.º 3, não contém um regime diverso do anterior", ou seja, do artigo 126.º, n.º 1, na medida em que o legislador cominou igualmente a nulidade, "a mesma espécie de nulidade – das provas obtidas dessa maneira, determinando que essas provas tão-pouco podem ser utilizadas."[28]

Não obstante as divergências doutrinárias, dir-se-á que, se o titular do direito não consentir, a prova obtida mediante intromissão nas telecomunicações é nula, em consequência de uma proibição de produção, e não pode ser utilizada (proibição de valoração), a não ser, eventualmente, para punir quem as obteve ilegitimamente. Ora, no entendimento de Pedro Verdelho, "a consagração deste princípio pretende estabelecer claramente que quem investiga não pode recorrer aos mesmos métodos de quem é investigado. Não se pode investigar sem respeito pelas regras legais e a prova reunida tem que cumprir os requisitos formais legalmente fixados"[29].

No entanto, João Conde Correia tem um entendimento diverso, pois, na sua opinião, o recurso à interceção de comunicações quando os crimes de injúria, ameaça, coação, devassa da vida privada e perturbação da paz e do sossego forem praticados por via de um sistema informático não seria uma solução arbitrária e, consequentemente, não consubstanciaria uma intromissão ilegítima no sigilo das comunicações eletrónicas, pois a própria "Constituição não prevê formas de utilização abusiva deste direito", aliás "é a própria Constituição que não protege essas formas de utilização do direito fundamental, nomeadamente quando estas integram um ilícito criminal"[30] e, tal como refere Vieira de Andrade, "se num caso hipotético ou concreto se põe em causa o conteúdo essencial de outro direito, se se atingem intoleravelmente valores comunitários básicos ou princípios fundamentais da ordem constitucional, deverá resultar

27 Sousa Mendes, 2015: 180.

28 *Idem*: 188.

29 Verdelho, 2004: 119-120.

30 Correia, 2014: 46.

para o intérprete a convicção de que a proteção constitucional do direito não quis ir tão longe"[31].

João Conde Correia[32] salienta ainda que "o sigilo das comunicações eletrónicas não foi concedido para, a seu coberto, se poder insultar, ameaçar ou coagir outrem ou para se poder devassar a sua vida privada". Ora no entendimento do mesmo Autor, "nestes casos, apesar da sua reduzida relevância penal, o Estado deve ter legitimidade para intervir", pois nada justifica "destacar as ofensas cometidas por telefone, conferindo-lhes uma tutela processual penal muito superior às cometidas por via informática".

3.2. Âmbito de aplicação material do artigo 18.º da Lei do Cibercrime

Ao contrário das disposições processuais previstas nos artigos 12.º a 17.º da LC, cujo âmbito de aplicação se encontra regulamentado no artigo 11.º do referido diploma, o artigo 18.º consagra o seu próprio âmbito de aplicação. Ora, podemos constatar que o âmbito de aplicação desta disposição legal é bastante mais restrito e tal deve-se ao facto de este meio de obtenção de prova, enquanto método oculto de investigação, ser bastante mais restritivo e intrusivo dos direitos fundamentais do que a generalidade dos outros meios de obtenção de prova previstos na presente lei, como já tivemos oportunidade de explicar.

Com efeito, como método oculto de investigação, a interceção de comunicações só é admissível, para além dos outros pressupostos cumulativamente exigíveis para a legitimidade e validade da prova, relativamente a um catálogo específico de crimes e só poderá ser autorizada durante a fase de inquérito, "se houver razões para crer que a diligência é indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter".

Desta forma, o artigo 18.º, n.º 1, da LC prevê que o recurso à interceção de comunicações só é admissível em processos relativos a crimes previstos na LC ou a crimes "cometidos por meio de um sistema informático ou em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico, quando tais crimes se encontrem previstos no artigo 187.º do Código do Processo Penal". Desta forma, o artigo 18.º da LC aplicar-se-á somente às medidas de interceção de comunicações em tempo real quanto aos crimes previstos na LC (falsidade informática, dano relativo a programas ou outros

31 Vieira de Andrade, 2012: 276.

32 Correia, 2014: 46.

dados informáticos, sabotagem informática, acesso ilegítimo, interceção ilegítima e reprodução ilegítima de pograma protegido), em conformidade com o disposto na al. *a)*, do n.º 1, do artigo 18.º da LC, independentemente do meio de comunicação utilizado (correio eletrónico, telemóvel, telefone, etc) e será também aplicável aos crimes previstos no artigo 187.º, n.º 1, do CPP, mas somente quando estes forem cometidos por meio de sistemas informáticos ou relativamente aos quais seja necessário recolher prova em suporte eletrónico.

Todavia, atentos à redação do artigo 187.º, n.º 1, al. *e)*, do CPP, a aplicação de tal medida aos crimes de injúria, ameaça, coação, devassa da vida privada e perturbação da paz e do sossego só é possível quando tais crimes são cometidos através do telefone. Posto isto:

3.3. Será possível recorrer à interceção de comunicações prevista no artigo 18.º da Lei do Cibercrime para prova dos crimes de injúria, ameaça, coação, devassa da vida privada e perturbação da paz e do sossego quando cometidos por meio diferente do telefone?

Ora, aplicando-se aos crimes previstos no artigo 187.º, n.º 1, do CPP, a interceção de comunicações poder-se-á aplicar aos crimes de injúria, ameaça, coação, devassa da vida privada e perturbação da paz e do sossego, pois estes crimes fazem ainda parte do catálogo.

Todavia, em conformidade com o disposto na al. *e)*, do n.º 1, do artigo 187.º do CPP, tal meio de obtenção de prova só pode ser aplicado a tais crimes quando os mesmos são cometidos através do telefone e é precisamente aqui que se levanta o problema por nós colocado.

Na discussão do Plenário na Assembleia da República da proposta de lei n.º 109/X, a 14 de março de 2007, o Ministro da Justiça Alberto Costa[33] referiu que aquilo que se pretendia era proceder a uma revisão onde se alargasse o "âmbito dos crimes que podiam justificar interceções eletrónicas, abrangendo nomeadamente a ameaça da prática de crime e a evasão". Acrescentou ainda que "um Direito Processual Penal de inspiração liberal deve ser forte na defesa dos direitos das pessoas e forte nos instrumentos de combate ao crime. É assim que passa a estar prevista a obtenção de dados sobre transmissão por via telemática, seja qual for a natureza do suporte". Pretendia com isto dizer que esta revisão do CPP tinha em vista "robustecer a posição pública e suprir lacunas,

33 Diário da Assembleia da República, I.ª Série, n.º 59, de 15 de março de 2007: 25.

visando equiparar melhor a justiça na ação contra o crime", introduzindo-se "novas soluções hoje requeridas".

Todavia, já nesta altura, o Conselheiro Pinto Monteiro alertou, que havia uma falha na proposta de lei, pois havendo a possibilidade legal prevista na al. *e)*, do n.º 1, do artigo 187.º do CPP de realização de interceções telefónicas no decurso da investigação de alguns crimes cometidos por telefone, a proposta não previa a realização de interceção de comunicações por via eletrónica, se esta for a via pela qual os crimes foram praticados[34] e na altura a lacuna manteve-se.

Neste sentido Carlos Adérito Teixeira[35] afirma existir uma dificuldade na "aplicação do regime das escutas telefónicas ao correio eletrónico em torno do catálogo de crimes, previsto no artigo 187.º do CPP, em particular face ao disposto na al. *e)*, do n.º 1, ao prever-se ali os crimes de injúria, ameaça, coação, devassa da vida privada e perturbação da paz e do sossego, quando cometidos através do telefone". No seu entendimento, "esta formulação típica não parece consentir a extensão de regime aos (mesmos) crimes cometidos através de outros meios para efeito de se considerarem de catálogo e legitimadores da "interceção" desses meios para obtenção de prova", devido, sobretudo a duas razões: "por um lado, porque em matéria de restrição de direitos – que uma interceção sempre representa – não são admissíveis extensões do âmbito do regime que o legislador estabeleceu; por outro lado, não se poderá dizer que a *mens legislatoris* visaria incluir no catálogo os crimes cometidos através do telefone ou através de "quaisquer outros meios" (a que alude no art. 189.º) porque, em outros lugares do artigo onde se enuncia o catálogo, quando entendeu ser abrangente, usou a expressão "meio de comunicação" (cfr. n.º 4 e n.º 7 do art. 187.º) e não telefone". Desta forma, conclui dizendo que não se pode "lançar mão desta via de obtenção de prova quando praticados os crimes daquela al. e) por meios técnicos diferentes do telefone, mesmo admitindo ser esse o único meio de prova, porquanto instrumento do crime".

Rita Castanheira Neves[36] partilha do mesmo entendimento, ao referir que tal extensão não parece ser possível "dada a específica metodologia que deve seguir a interpretação da lei penal e processual penal, atento o respeito ao princípio da legalidade". Desta forma, defende que "deveria ter sido o legislador a ter a preocupação de logo estabelecer na parte final da agora alínea *e)* do n.º 1

34 Neste sentido, Verdelho, 2008: 161.

35 Teixeira, 2008: 284.

36 Neves, 2011: 167.

do artigo 187.º do Código do Processo Penal a expressão *quando cometidos através de meio técnico de comunicação*. Para além disso, tal interpretação seria *in male partem*, sendo, por isso, inconstitucional".

Todavia, há entendimentos diversos, pois de acordo com Joel Timóteo Pereira[37] será possível a interceção de correio eletrónico em investigações de crimes de injúria, ameaça, coação, devassa da vida privada e perturbação da paz e do sossego se estes forem cometidos através de e-mail, ou seja, em vez de vedar o acesso a estas comunicações eletrónicas, enquanto meio de obtenção de prova, nas investigações daqueles específicos crimes, devido ao facto de o catálogo de crimes consagrar a expressão "quando cometidos através do telefone", o Autor equipara os demais meios de comunicação a esta expressão.

Nas palavras de João Conde Correia[38] numa interpretação literal da norma teremos de excluir todos os crimes não incluídos no catálogo restritivo do artigo 18.º, n.º 1, da LC, o que revela, que o propósito de "responder ao diagnóstico de uma carência do ordenamento jurídico nacional relativa à recolha de prova eletrónica"[39] não foi alcançado.

Todavia, no seu entender, o catálogo de crimes constante do artigo 187.º, n.º 1, do CPP "deverá, numa interpretação atualista, incluir os crimes de injúria, ameaça, coação ou devassa da vida privada cometidos através de sistema informático. O que ali é autorizado para os crimes praticados através do telefone é aqui permitido para os crimes cometidos através de um sistema informático", pois de acordo com a Exposição de Motivos da Proposta de Lei n.º 289/X, "o propósito do legislador, embora muito mal expresso, foi, justamente, permitir a «realização de interceção de comunicações eletrónicas e, sobretudo a obtenção de dados de tráfego» nos «processos crimes em que se investiguem crimes cometidos por via das redes de comunicações»". Deste modo, "a remissão legal é, assim, para o tipo de crime em causa e não para a forma como ele é cometido, pois essa passa necessariamente por um sistema informático, como resulta da primeira parte da alínea *b)*, do número um do artigo 18.º («cometidos por meio de um sistema informático»)"[40].

No nosso entendimento e tal como refere João Conde Correia, o que está aqui em causa não é o catálogo de crimes, porque os crimes de injúria, ameaça,

37 Pereira, 2004: 1000-1001.

38 Correia, 2014: 45.

39 Mesquita, 2010: 97.

40 Correia, 2014: 45-46.

coação, devassa da vida privada e perturbação da paz e do sossego fazem parte do catálogo de crimes previsto no artigo 187.º, n.º 1, do CPP. O que está aqui em causa é o meio como esses crimes do catálogo foram praticados. Deste modo, somos do entendimento que é possível recorrer quer à interceção de dados de conteúdo, quer à interceção de dados de tráfego, porque tal é permitido pelo n.º 3, do artigo 18.º, da LC, para prova dos crimes de injúria, ameaça, coação, devassa da vida privada e perturbação da paz e do sossego quando cometidos por meio diferente do telefone, pois tal não violará o princípio da legalidade, uma vez que é a própria lei, nomeadamente, o artigo 18.º, n.º 1, al. *b)*, da LC, que prevê tal possibilidade ao estabelecer que é admissível o recurso à interceção de comunicações nos crimes previsto no catálogo do artigo 187.º do CPP, quando tais crimes são cometidos por meio de um sistema informático.

Ora, de acordo com a al. *a)*, do artigo 2.º da LC, sistema informático é "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 autonomizado 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, proteção e manutenção", o que, a nosso ver, significa que se pode recorrer à interceção de comunicações quando esta comunicação é transmitida por meio técnico diferente do telefone, nomeadamente correio eletrónico, mensagens trocadas através de processos de comunicação instantânea, entre outros.

Assim, concordamos com João Conde Correia quando refere que a remissão legal é para o tipo de crime em causa, ou seja, para os crimes do catálogo, onde se insere precisamente os crimes de injúria, ameaça, coação, devassa da vida privada e perturbação da paz e do sossego e não para a forma como ele é cometido, pois o artigo 18.º, n.º 1, al. *b)* permite o recurso à interceção de comunicações para a prova dos crimes previstos no artigo 187.º do CPP precisamente quando tais crimes são praticados por meio de um sistema informático, ou seja, esta possibilidade não está vedada exclusivamente ao uso do telefone para a prática de tais crimes, pois essa prática pode ocorrer por outros meios, designadamente, o correio eletrónico.

Consequentemente, não estamos também, no presente caso, perante uma proibição de prova relativa, pois não estamos perante uma intromissão ilegítima no direito ao sigilo das comunicações eletrónicas, pois a própria lei prevê a possibilidade de se recorrer à interceção de comunicações para prova

dos crimes previstos no artigo 187.º, n.º 1, al. *e)*, do CPP, quando tais crimes são praticados por meio de um sistema informático, pelo que tal ingerência é admissível à luz do artigo 34.º, n.º 4, da CRP e, portanto, legítima.

4. CONCLUSÃO

O desenvolvimento das novas tecnologias de informação facilitaram a comunicação entre os vários agentes de uma sociedade. Todavia, como referimos, também abriram caminho a uma nova forma de criminalidade, a chamada criminalidade informática. E, de forma a fazer face a esta nova forma de criminalidade, os Estados têm recorrido cada vez mais aos métodos ocultos de investigação, como a interceção de comunicações, uma vez que são métodos que permitem, mais facilmente, a descoberta das infrações e a respetiva punição do seu agente.

De facto a CRP permite o recurso à interceção de comunicações, na medida em que prevê, no artigo 34.º, n.º 4, a possibilidade de ingerência das autoridades públicas nas telecomunicações "nos casos previstos na lei em matéria de processo criminal". Todavia, tendo em consideração que a interceção de comunicações prevista no artigo 18.º da LC é um método oculto de investigação e, como tal, um método de obtenção de prova que tem subjacente uma elevada danosidade social pelo facto de implicar a ingerência por parte do Estado nas comunicações eletrónicas e, consequentemente, a restrição de direitos fundamentais, implica, para a sua validade e legitimidade, como já tivemos oportunidade de expor, a verificação de determinados pressupostos, como a existência de um catálogo de crimes e a observância do princípio da legalidade, sob pena de originar uma proibição de prova relativa.

Com efeito, o artigo 18.º, n.º 1, da LC prevê que só se poderá recorrer à interceção de comunicações em tempo real quando está em causa um crime previsto na LC, independentemente do meio de comunicação utilizado, ou quando está em causa um dos crimes previstos no artigo 187.º, n.º 1, do CPP, mas somente quando estes forem cometidos por meio de sistemas informáticos ou relativamente aos quais seja necessário recolher prova em suporte eletrónico.

Posto isto, o problema que importava esclarecer era se a interceção de comunicações poderá ser aplicável aos crimes de injúria, ameaça, coação, devassa da vida privada e perturbação da paz e do sossego quando tais crimes são praticados por meio diferente do telefone, uma vez que o artigo 187.º, n.º 1, al. *e)*, do CPP só prevê tal possibilidade quando tais crimes são cometidos através do telefone.

Na nossa opinião, poder-se-á recorrer à interceção de comunicações para prova dos crimes anteriormente referidos quando tais crimes são praticados por meio diferente do telefone, pois tal não violará o princípio da legalidade, uma vez que o próprio artigo 18.º, n.º 1, al. *b)*, da LC prevê expressamente essa possibilidade ao dispor que "é admissível o recurso à interceção de comunicações em processos relativos a crimes cometidos por meio de um sistema informático (…) quando tais crimes se encontrem previstos no artigo 187.º do Código do Processo Penal", não se cingindo, por isso, aos crimes cometidos através do telefone.

Assim, apesar da doutrina ainda não ser unânime quanto a esta questão, pensamos que tal querela doutrinária já não tem sentido atualmente, uma vez que, a nosso ver, a própria lei responde diretamente à questão por nós suscitada.

BIBLIOGRAFIA

Albuquerque, Paulo Pinto de

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

Andrade, José Carlos Vieira de

2012 *Os direitos fundamentais na Constituição Portuguesa de 1976*, 5.ª ed., Coimbra: Almedina.

Andrade, Manuel da Costa

2009 *Bruscamente no Verão Passado – A reforma do Código do Processo Penal, Observações críticas sobre uma lei que podia e devia ter sido diferente*, Coimbra: Coimbra Editora.

Canotilho, José Joaquim Gomes e Moreira, Vital

2007 *Constituição da República Portuguesa Anotada*, 4.ª ed. revista, Vol. I, Coimbra: Coimbra Editora.

Catena, Víctor Moreno

2008 "Los elementos probatórios obtenidos com la afectación de derechos fundamentales durante la investigación penal" in: *Prueba y Processo Penal – Análisis especial de la prueba prohibida en el sistema español e en el derecho comparado*, Valencia: Tirant Lo Banch, pp. 75-106.

Correia, João Conde

1999 "Qual o significado da 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*, n.º 79, pp. 45-67.

2014 "Prova digital: as leis que temos e a lei que devíamos ter" in: *Revista do Ministério Público*, Ano 35, n.º 139, pp. 29-59.

Fumu, Giacomo

1990 "Sub art. 266-271", in: AA. VV., *Commento al nuevo codice di procedura penale, coordinato da M. Chiavario*, Volume II, Torino: UTET, pp. 771-804.

Gonçalves, Pedro

1999 *"Direito das Telecomunicações"*, Coimbra: IJC e Almedina.

Mendes, Paulo de Sousa

2015 *Lições de Direito Processual Penal*, 2.ª reimp., Coimbra: Almedina.

Mesquita, Paulo Dá

2010 *Processo Penal, Prova e Sistema Judiciário*, Coimbra: Coimbra Editora.

Neves, Rita Castanheira
2011 *As Ingerências nas Comunicações Eletrónicas em Processo Penal – Natureza e respetivo Regime Jurídico do Correio Eletrónico enquanto meio de obtenção de prova*, Coimbra: Coimbra Editora.
Pereira, Joel Timóteo Ramos
2004 *Compêndio Jurídico da Sociedade de Informação – Notas Práticas, Legislação e Jurisprudência*, Lisboa: Quid Juris?
Rodrigues, Benjamim Silva
2010 *Da Prova Penal – Tomo II – Bruscamente… A(s) Face(s) Oculta(s) dos Métodos Ocultos de Investigação Criminal*, 1.ª ed, Carcavelos: Rei dos Livros.
Teixeira, Carlos Adérito
2008 "Escutas telefónicas: a mudança de paradigma e os velhos e os novos problemas", in: *Revista do CEJ: Jornadas sobre a Revisão do Código de Processo Penal*, 1.º Semestre, n.º 9 (Especial), pp. 241-295.
Venâncio, Pedro Dias
2006 "Investigação e meios de prova na criminalidade informática", in *Compilações doutrinais Verbo Jurídico*, também disponível em http://www.verbojuridico.net/doutrina/tecnologia/meiosprovacriminalidadeinformatica.pdf.
Verdelho, Pedro
2004 "A obtenção de prova no ambiente digital", in: *Revista do Ministério Público*, Ano 25, julho-setembro, n.º 99, pp. 117-136.
2008 "Técnica no Novo C.P.P.: Exames, Perícias e Prova Digital", in: *Revista do CEJ: Jornadas sobre a Revisão do Código de Processo Penal*, 1.º Semestre, n.º 9 (Especial), pp. 145-171.

Jurisprudência

Acórdão do Tribunal da Relação de Lisboa, de 17 de julho de 2008, Proc. n.º 3453/2008-5, Relator: Simões de Carvalho.
Acórdão do Tribunal da Relação de Évora, de 5 de junho de 2012, Proc. n.º 12/12.1YREVR, Relatora: Maria Fernanda Palma.
Acórdão do Tribunal da Relação de Évora, de 6 de janeiro de 2015, Proc. n.º 6793/11.2TDLSB-A.E1, Relator: João Gomes de Sousa.
Acórdão do Tribunal da Relação de Évora, de 20 de janeiro de 2015, Proc. n.º 648/14.6GCFAR-A.E1, Relator: João Gomes de Sousa.
Sentenza n.º 6 del 2000, Cassazione Penale, Sezioni Unite, 23 Febbraio 2000, Roma.