Mestrado em Direito e Prática Jurídica – Especialidade: Direito Penal
2023/2024
Direito Penal V – Cibercrime e Prova Digital
Turmas A e B
Regência: Teresa Quintela de Brito
Exame – 1.ª Época: 7.06.2024

Duração: 1 h e 45 minutos + 15 minutos de tolerância

I

Leia o seguinte extracto de um Acórdão do Tribunal da Relação de Lisboa, de 30.06.2011:

"II - O bem jurídico protegido pelo crime de contrafacção de moeda (art. 262.º, do Código Penal), é a intangibilidade do sistema monetário, incluindo a segurança e credibilidade do tráfego monetário;
III - Para o efeito, o cartão de crédito constitui verdadeira moeda, tutelando aquele tipo legal a fiabilidade e confiança na circulação da moeda na versão moderna do chamado dinheiro de plástico;
IV - O bem jurídico protegido pelo crime de falsificação informática (art. 3, n.º 1, da Lei n.º 109/09), é a integridade dos sistemas de informação;
V - Tendo os agentes duplicado e utilizado cartões de crédito e tido acesso a dados que se encontravam em cartões de débito, produzindo com estes dados documentos não genuínos para os utilizar no levantamento de dinheiro ou pagamento de bens, praticaram, em concurso efectivo, aqueles dois crimes".

Responda fundamentadamente às seguintes questões:

1. Concorda (ou não) com a identificação do bem jurídico tutelado pela incriminação da falsidade informática (artigo 3.º/1, da LCib) realizada no ponto IV do Sumário deste Acórdão? Porquê? **(2 valores)**

2. Depois das modificações introduzidas pela Lei n.º 79/2021 à Lei do Cibercrime (designadamente, artigos 3.º a 3.º-G) e ao Código Penal (designadamente, artigo 267.º), qual deveria ser o enquadramento jurídico-penal da conduta descrita no ponto V do Sumário deste Acórdão? Porquê? **(3 valores)**

3. Quais os tipos legais de crime realizados e por qual(ais) deveriam ser punidos os agentes falsificadores que efectivamente usaram, num só dia e por várias vezes, ambos os tipos de cartões de pagamento para levantar dinheiro em máquinas ATM e para efectuar o pagamento de compras *online*, causando, assim, um prejuízo de valor consideravelmente elevado? Porquê? **(4 valores)**

II

Atente na seguinte decisão do Tribunal Constitucional, proferida no âmbito da fiscalização preventiva da constitucionalidade:

"Pelo exposto, o Tribunal decide, com referência ao Decreto n.º 167/XIV da Assembleia da República, (...) enviado ao Presidente da República para promulgação como lei, pronunciar-se pela

inconstitucionalidade das normas constantes do seu artigo 5.º, na parte em que altera o artigo 17.º da Lei n.º 109/2009 (...), por violação (...) dos artigos 26.º, n.º 1, 34.º, n.º 1, 35.º, n.ºs 1 e 4, 32.º, n.º 4, e 18.º, n.º 2, da Constituição da República Portuguesa".

Considere agora o conteúdo da alteração ao artigo 17.º, da LCib, vertida no artigo 5.º Decreto n.º167/XIV da Assembleia da República:

«Artigo 17.º - Apreensão de mensagens de correio eletrónico ou de natureza semelhante

1. Quando, no decurso de uma pesquisa informática ou de outro acesso legítimo a um sistema informático, forem encontradas, armazenadas nesse sistema informático ou noutro a que seja permitido o acesso legítimo a partir do primeiro, mensagens de correio eletrónico ou de natureza semelhante que sejam necessárias à produção de prova, tendo em vista a descoberta da verdade, a autoridade judiciária competente autoriza ou ordena por despacho a sua apreensão.
2. O órgão de polícia criminal pode efetuar as apreensões referidas no número anterior, sem prévia autorização da autoridade judiciária, no decurso de pesquisa informática legitimamente ordenada e executada nos termos do artigo 15.º, bem como quando haja urgência ou perigo na demora, devendo tal apreensão ser validada pela autoridade judiciária no prazo máximo de 72 horas.
3. À apreensão de mensagens de correio eletrónico e de natureza semelhante aplica-se disposto nos n.ºs 5 a 8 do artigo anterior [artigo 16.º, da LCib, inalterado].
4. O Ministério Público apresenta ao juiz, sob pena de nulidade, as mensagens de correio eletrónico ou de natureza semelhante cuja apreensão tiver ordenado ou validado e que considere serem de grande interesse para a descoberta da verdade ou para a prova, ponderando o juiz a sua junção aos autos tendo em conta os interesses do caso concreto".
5. (...)
6. No que se não encontrar previsto nos números anteriores, é aplicável, com as necessárias adaptações, o regime da apreensão de correspondência previsto no Código de Processo Penal».

Responda às seguintes questões:

4. Considerando o actual artigo 17.º, da LCib, quais seriam as principais modificações que o artigo 5.º, do Decreto n.º 167/XIV da Assembleia da República, teria introduzido no regime da apreensão de mensagens de correio electrónico e equiparado, não fora a referida decisão de inconstitucionalidade? **(4,5 valores)**

5. Tendo em conta o teor da alteração ao artigo 17.º, da LCib, vertida no artigo 5.º do Decreto n.º 167/XIV da Assembleia da República, e as normas constitucionais invocadas para concluir pela inconstitucionalidade, quais terão sido, em seu entender, os principais argumentos usados pelo Tribunal constitucional para chegar à decisão de inconstitucionalidade? **(4,5 valores)**

Apreciação Global (organização e nível de fundamentação das respostas, capacidade de síntese, clareza de ideias e correcção da linguagem)**: 2 valores.**

Os exames (ou as respectivas partes) com caligrafia ilegível não serão avaliados.

TÓPICOS DE CORRECÇÃO

I

Responda fundamentadamente às seguintes questões:

1. Concorda (ou não) com a identificação do bem jurídico tutelado pela incriminação da falsidade informática (artigo 3.º/1, da LCib) realizada no ponto IV do Sumário deste Acórdão? Porquê?**(2 valores)**

Está incompleta a identificação do bem jurídico protegido pela incriminação da falsidade informática.

Trata-se de um crime informático em sentido estrito, pois: (i) o objecto da conduta é exclusivamente constituído por dados e programas informáticos (cfr. definição no artigo 2.º, alínea *b)*, da LCib); (ii) a conduta típica consiste em "introduzir, modificar, apagar ou suprimir dados informáticos ou por qualquer outra forma interferir num tratamento informático de dados"; e (iii) tutela um bem jurídico especificamente informático (integridade, confidencialidade e operacionalidade de dados e programas informáticos).

A este bem jurídico acresce outro, este sim característico da falsidade informática enquanto crime paralelo à falsificação de documentos (artigo 156.º, do CP) mas adaptado ao mundo digital: a integridade, fiabilidade e credibilidade dos dados e documentos electrónicos no tráfico jurídico-probatório.

A falsidade informática configura um crime material ou de resultado, porque a sua consumação depende da efectiva produção de dados ou documentos electrónicos não genuínos, como evento espácio-temporalmente destacado da conduta típica. O tipo objectivo já não exige que os dados ou documentos electrónicos contrafeitos sejam realmente utilizados para finalidades jurídicas como se fossem autênticos, induzindo em erro intervenientes no tráfico jurídico-probatório (crime de resultado cortado ou parcial).

Estamos perante um crime doloso que, ademais, comporta dois elementos subjectivos especiais da ilicitude: a intenção de provocar engano nas relações jurídicas e a de que os dados ou documentos contrafeitos sejam considerados ou utilizados para finalidades juridicamente relevantes como se fossem genuínos.

Para que esta segunda intenção não surja como uma inútil redundância da primeira e de modo a assegurar a ofensividade da conduta típica face ao bem jurídico característico da falsidade informática, deve a mesma ser interpretada como exigência de idoneidade objectiva dos dados ou documentos electrónicos contrafeitos para serem considerados ou usados como genuínos no tráfico jurídico-probatório. Deste modo, a falsidade informática configura-se como um crime de perigo abstracto-concreto para o bem jurídico da fiabilidade e credibilidade dos dados e documentos electrónicos no tráfico jurídico-probatório.

2. Depois das modificações introduzidas pela Lei n.º 79/2021 à Lei do Cibercrime (designadamente, artigos 3.º a 3.º-G) e ao Código Penal (designadamente, artigo 267.º), qual deveria ser o enquadramento jurídico-penal da conduta descrita no ponto V do Sumário deste Acórdão? Porquê? **(3 valores)**

Pretendia-se que os Alunos (i) identificassem as alterações trazidas pela Lei n.º 79/2021 à Lei do Cibercrime e ao Código Penal relevantes para o enquadramento jurídico-penal dos factos relatados no ponto V do Sumário do Acórdão; e que (ii) enquadrassem jurídico-penalmente estes factos na perspectiva da respectiva tipicidade.

Com a Lei n.º 79/2021, que transpôs a Directiva (UE) 2019/713 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, relativa ao combate à fraude e à contrafacção de meios de pagamento que não em numerário:

A *falsidade informática incidente sobre dados registados ou incorporados em cartão bancário de pagamento ou em qualquer outro dispositivo que permita aceder a sistema ou meio de pagamento*, prevista no *n.º 2 do artigo 3.º da versão originária da Lei do Cibercrime*, converteu-se no *tipo autónomo de contrafacção de cartões ou outros dispositivos de pagamento* (artigo 3.º-A, da LCib), punível com a mesma pena cominada pelo artigo 262.º/1, do CP, para a contrafacção de moeda. O n.º 2 do artigo 3.º da LCib ficou limitado à falsidade informática incidente sobre os dados registados, incorporados ou respeitantes a qualquer dispositivo que permita aceder a sistema de comunicações ou a serviço de acesso condicionado.

O *uso, com intenção de causar prejuízo a outrem ou de obter um benefício ilegítimo*, para si ou para terceiro, *de cartão ou outro dispositivo de acesso a sistema ou meio de pagamento contrafeitos, outrora previsto no artigo 3.º/3, da versão originária da LCib*, passou a constituir o *tipo autónomo de uso de cartões ou outros dispositivos de pagamento contrafeitos* (artigo 3.º-B, da LCib).

O *artigo 267.º/1, alínea c), do CP, deixou de equiparar os cartões de crédito a moeda em numerário*, de modo que a *contrafacção informática ou não informática deste tipo de cartões deixou de ser punida ao abrigo do artigo 262.º/1, do CP*, passando a sê-lo nos termos do artigo 3.º-A, da LCib, tal como a contrafacção de cartões de débito. Assim se pôs termo à situação absurda, anterior à Lei n.º 79/2021, em que a contrafacção informática de cartões de crédito era sancionada como crime de contrafacção de moeda (pena de prisão de 3 a 12 anos) e a contrafacção informática de cartões de débito como crime de falsidade informática (pena de prisão de 1 a 5 anos), nos termos do artigo 3.º/2, da LCib.

O artigo 225.º, do CP, foi alterado: o crime de uso de cartão de garantia ou de crédito converteu-se no de abuso de cartão de garantia ou de cartão, dispositivo ou dados de pagamento. Uma vez que o mero uso abusivo de dispositivo, corpóreo ou incorpóreo, que permita aceder a sistema ou a meio de pagamento, ou de dados registados, incorporados ou respeitantes a cartão de pagamento

ou a qualquer outro dispositivo, corpóreo ou incorpóreo, que permita aceder a sistema ou a meio de pagamento (artigo 225.º/1, alíneas *c)* e *d)*, do CP), *necessariamente envolve a utilização de dados sem autorização ou intervenção por qualquer outro modo não autorizada no processamento* (artigo 221.º/1, do CP), o *crime de abuso de cartão, dispositivo ou dados de pagamento configura-se como norma especial relativamente ao crime geral de burla informática*. Por outras palavras: o artigo 225.º afastou a aplicação do artigo 221.º, sempre que a provocação de prejuízo patrimonial se dê mediante utilização de dados de pagamento sem autorização ou intervenção por qualquer outro modo não autorizada no processamento de dados que permitam aceder a sistema ou meio de pagamento.

Tendo em conta os factos descritos no ponto V do Sumário do Acórdão:

A *duplicação de cartões de crédito*, com intenção de provocar engano nas relações jurídicas, realiza o tipo de contrafacção de cartões ou outros dispositivos de pagamento (artigo 3.º-A, da LCib), ainda que a falsificação se não faça "introduzindo, modificando, apagando, suprimindo ou interferindo, por qualquer outro modo, num tratamento informático de dados registados, incorporados, ou respeitantes a estes cartões ou dispositivos". O que permite o artigo 3.º-A ao não proceder a uma descrição taxativa e fechada das condutas falsificadoras (ao contrário do artigo 3.º/1 e 2), como evidencia o recurso à expressão "nomeadamente"; e resulta da supressão da equiparação dos cartões de crédito a moeda em numerário para efeitos do crime de contrafacção de moeda (artigo 267.º/1, alínea *c)*, do CP). Por outras palavras: com a Lei n.º 79/2021, a contrafacção de cartões de crédito foi banida do Código Penal e só encontra guarida no artigo 3.º-A, da LCib, mesmo que a falsificação se não faça por meio informático.

Também a *contrafacção de cartões de débito*, usando dados indevidamente acedidos respeitantes a cartões genuínos, realiza o tipo previsto no artigo 3.º-A, da LCib.

Já o mero *uso dos cartões de crédito e de débito para levantar dinheiro e pagar bens* – portanto, necessariamente com intenção de causar prejuízo ou de obter um benefício ilegítimo, para si ou para terceiro, e causando prejuízo patrimonial a outrem – configura o crime de mera actividade de uso de cartões ou outros dispositivos de pagamento contrafeitos (artigo 3.º-B, da LCib) e, ainda, o crime de resultado contra o património de abuso de cartão de garantia ou de cartão, dispositivo ou dados de pagamento (artigo 225.º/1, alínea *c)*, do CP).

No caso da *utilização de cartões de crédito ou de débito contrafeitos para fazer pagamento de bens em lojas, junto dos funcionários da "caixa"*, estará em causa igualmente um crime de burla clássica ou "triangular" ("burlão", "enganado" e "prejudicado"), descrito no artigo 217.º, do CP.

3. Quais os tipos legais de crime realizados e por qual(ais) deveriam ser punidos os agentes falsificadores que efectivamente usaram, num só dia e por várias vezes, ambos os tipos de cartões de pagamento para levantar dinheiro em máquinas ATM e para efectuar o

pagamento de compras *online*, causando, assim, um prejuízo de valor consideravelmente elevado? Porquê? **(4 valores)**

Agora pretendia-se que os Alunos, tendo em conta a especificação dos factos efectuada nesta pergunta e sem perder de vista o enquadramento jurídico-penal das condutas descritas no ponto V do Sumário realizado na pergunta anterior, resolvessem os problemas de concurso efectivo e aparente entre os tipos de crime identificados e realizados pelo comportamento global dos agentes.

Estaríamos perante um *concurso efectivo de dois crimes de contrafacção de cartões ou outros dispositivos de pagamento* (artigos 30.º/1 e 77.º, do CP): um respeitante aos cartões de crédito duplicados; outro relativo aos cartões de débito contrafeitos recorrendo a dados de cartões de débito genuínos, a que os agentes ilegitimamente acederam, realizando assim também o crime de acesso ilegítimo (artigo 6.º/4, alínea *b)*, da LCib). Contudo, este último parece configurar-se como um crime-meio para a realização do crime-fim de contrafacção de cartões de débito, que neste esgota o respectivo conteúdo de ilícito (concurso aparente de crimes na modalidade de consunção pura).

Sendo o *uso dos cartões de crédito e de débito contrafeitos levado a cabo pelos próprios falsificadores*, este *uso, só por si, nada acrescenta ao desvalor da própria contrafacção desses cartões* (concurso aparente na modalidade de consunção pura, estando-se estar perante um facto posterior não punível). Não seria de aplicar o artigo 3.º-B/3, da LCib, por o uso dos cartões contrafeitos não ser realizado por um terceiro, conluiado com o falsificador, mas pelos próprios falsificadores.

Todavia, *o uso dos cartões de crédito e de débito contrafeitos para levantar dinheiro em máquinas ATM e para pagar compras online* realiza, simultaneamente, os tipos legais de *burla informática* (provocação de prejuízo patrimonial mediante utilização de dados sem autorização ou intervenção por qualquer outro modo não autorizada no processamento – artigo 221.º/1, do CP); *acesso ilegítimo* à parte do sistema informático em que estão alojados os dados relativos aos cartões de crédito e às contas bancárias dos legítimos titulares dos cartões de débito contrafeitos (artigo 6.º/1, da LCib); e de *abuso dos cartões de crédito e de débito* (provocação de prejuízo patrimonial, determinando, respectivamente, o levantamento e a transferência de moeda, através do uso necessariamente abusivo de dispositivos corpóreos ou incorpóreos contrafeitos que permitam aceder a sistema ou meio de pagamento – artigo 225.º/1, alínea *c)*, do CP).

Na resposta à pergunta anterior, já se disse que *entre os crimes de burla informática e de abuso de cartão de pagamento intercede uma relação de especialidade*, à luz da qual a norma geral (artigo 221.º/1) é afastada pela norma especial (artigo 225.º/1). Estamos, portanto, perante um concurso aparente de crimes.

Também o *crime de acesso ilegítimo à parte do sistema informático em que estão alojados os dados relativos aos cartões de crédito e às contas bancárias dos legítimos titulares dos cartões de débito contrafeitos* (artigo 6.º/1, da LCib), enquanto crime-meio intrinsecamente associado à prática do crime de uso

(necessariamente abusivo) de cartões de pagamento contrafeitos, *é afastado, por consunção pura, pela realização do crime-fim previsto no artigo 225.º/1, do CP*.

Poderíamos equacionar a existência de tantos crimes de uso (necessariamente abusivo) dos cartões contrafeitos de crédito, por um lado, e de débito, por outro, quantos os levantamentos e os pagamentos efectuados. Todavia, estamos perante *actos parcelares de execução de uma mesma e única decisão criminosa*: a de usar, em toda a medida possível, num curto espaço de tempo e antes de serem detectados, os cartões de crédito duplicados e os cartões de débito contrafeitos para provocar prejuízo patrimonial a outrem com intenção de obter enriquecimento ilegítimo. Fala-se nestes casos de *um único crime*, respectivamente, *de abuso dos cartões de crédito duplicados e de abuso dos cartões de débito contrafeitos*, *realizado através de uma pluralidade de actos parcelares mas em unidade material de acção*, porque em execução de uma mesma e única decisão criminosa, *sem que os agentes tivessem que renovar o processo de formação da vontade criminosa antes de utilizar cada um dos cartões de crédito duplicados e cada um dos cartões de débito contrafeitos*. Não se está perante dois crimes continuados de uso abusivo, respectivamente, dos cartões de crédito duplicados e dos cartões de débito contrafeitos (artigo 30.º/2, do CP) por faltar, à partida, a pluralidade de crimes (concurso efectivo) unificados num só crime, por força dos critérios referidos neste preceito.

Tratando-se de *cartões de pagamento com características distintas e contrafeitos por processos diferentes*, o que exigiu dois processos autónomos de formação da vontade criminosa por parte dos agentes, deveria afirmar-se a existência de um *concurso efectivo* (artigos 30.º/1 e 77.º, do CP) *de dois crimes de abuso de cartão de pagamento*: um relativo ao uso, necessariamente abusivo, dos cartões de crédito duplicados; outro, respeitante ao uso, necessariamente abusivo, dos cartões de débito contrafeitos.

A *autonomização de dois crimes de abuso de cartões de pagamento obsta à soma do valor do prejuízo causado pelo uso sucessivo de cada um dos tipos de cartões*, levando ao desaparecimento de um único crime previsto no artigo 225.º, do CP, do qual tenha resultado a provocação de um prejuízo de valor consideravelmente elevado [n.º 5, alínea *b)*].

Sendo ou não elevado o prejuízo causado pelo uso sucessivo de cada um dos tipos de cartões contrafeitos, a verdade é que *os agentes seriam sempre punidos em concurso efectivo pelos crimes-fim de abuso, respectivamente, dos cartões de crédito duplicados e dos cartões de débito contrafeitos, embora com a pena (mais grave) cominada para os crimes-meio de contrafacção dos cartões de crédito e de contrafacção dos cartões de débito* (artigo 3.º-A, da LCib), ao abrigo da figura da consunção impura.

A punição pelo concurso efectivo dos dois crimes-fim, se bem que com a pena prevista para os dois crimes-meio de contrafacção de cartões de crédito e de contrafacção de cartões de débito funda-se na necessidade de: (i) evitar a violação do "non bis in idem" (artigo 29.º/5, da CRP), já que o desvalor da contrafacção dos cartões de pagamento ficou confinado ao uso dos mesmos com intenção de obter enriquecimento ilegítimo (artigo 225.º/1, do CP), já que aqueles nunca saíram

da posse dos falsificadores; (ii) considerar a totalidade dos bens jurídicos atingidos pelas condutas do agente (a integridade, autenticidade e credibilidade dos meios de pagamento diversos da moeda em numerário e o património das pessoas e entidades que sofreram prejuízo patrimonial); e de (iii) apreciar de forma esgotante o conteúdo de ilícito do comportamento global do agente. Conteúdo este que não seria totalmente ponderado, caso os agentes fossem punidos com a pena cominada para os crimes-fim de abuso de cartões de crédito e de abuso de cartões de débito, pois o tipo de crime contra o património, previsto no artigo 225.º, do CP, não contempla a afectação do bem jurídico tutelado pela incriminação da contrafacção de cartões e outros dispositivos de pagamento (a integridade, autenticidade e credibilidade dos meios de pagamento diferentes da moeda em numerário).

II

Responda às seguintes questões:

6. Considerando o actual artigo 17.º, da LCib, quais seriam as principais modificações que o artigo 5.º, do Decreto n.º 167/XIV da Assembleia da República, teria introduzido no regime da apreensão de mensagens de correio electrónico e equiparado, não fora a referida decisão de inconstitucionalidade? **(4,5 valores)**

As principais diferenças são as seguintes:

Eliminação da epígrafe do artigo 17.º e do n.º 1 da Proposta *da expressão incorrecta "registos de comunicações de natureza semelhante" a mensagens de correio electrónico*, pois neste preceito não está em causa a apreensão de dados de tráfego de quaisquer comunicações, mas sim a apreensão de dados de conteúdo correspondentes a mensagens de correio electrónico e equiparadas (*i.e.*, "qualquer mensagem textual, vocal, sonora ou gráfica", ainda que não enviada por uma rede pública de comunicações, que se encontre armazenada na rede ou no equipamento terminal do destinatário – artigo 2.º/1, alínea *b)*, da Lei n.º 41/2004).

Permissão de apreensão de quaisquer mensagens de correio electrónico ou outras de natureza semelhante que, no decurso de uma pesquisa informática ou de outro acesso legítimo a um sistema informático, sejam encontradas armazenadas nesse sistema ou noutro a que seja permitido o acesso legítimo a partir do primeiro (*v.g.* caixa do *webmail* do visado), *desde que "necessárias à produção de prova, tendo em vista a descoberta da verdade", mediante ordem ou autorização da autoridade judiciária competente em função da fase do processo*. O que significa por ordem ou mediante autorização do Ministério Público na fase de inquérito (artigos 1.º, alínea *b)*, e 263.º, do CPP).

Neste ponto, o n.º 1 da Proposta afasta-se completamente do actual artigo 17.º, da LCib, que exige *ab initio* uma ordem ou autorização de apreensão pelo juiz, mesmo na fase de inquérito. Apreensão que, nos termos do actual artigo 17.º, também *ab initio*, apenas pode ter por objecto

mensagens de correio electrónico e outras de natureza semelhante que, fundada e expectavelmente, possam ser "de grande interesse para a descoberta da verdade ou para a prova".

O que se traduz numa *dupla diminuição das exigências*: *quanto à entidade competente para ordenar ou autorizar a apreensão*; e *quanto às mensagens a apreender* (as meramente necessárias à produção de prova e à descoberta da verdade, sem se exigir a demonstração de que as mensagens a apreender sejam, expectavelmente, de grande interesse para a descoberta da verdade ou para a prova).

O n.º 2 da Proposta possibilita uma *apreensão cautelar*, sujeita a validação pela autoridade judiciária competente no prazo máximo de 72 horas, *por parte dos OPC*, sem prévia autorização desta autoridade, no decurso de pesquisa informática legitimamente ordenada e executada nos termos do artigo 15.º, bem como em caso de urgência ou perigo na demora (cfr. artigos 249.º/1, 2, alínea *c*), do CPP). Deste modo, *consagra-se para o âmbito da apreensão de correio electrónico e similar o regime previsto no artigo 16.º/2 e 4, da LCib, para a apreensão de dados informáticos quando não esteja em causa o sigilo da correspondência e dos outros meios de comunicação privada* (artigos 34.º/1, da CRP). O que contraria a opção vertida no actual artigo 17.º, da LCib, e no artigo 252.º/2, do CPP, os quais pretenderam autonomizar e sujeitar a um regime mais exigente a apreensão de conteúdos relativos a comunicações privadas, do que a apreensão daqueles que somente possam pôr em causa a privacidade do respectivo titular ou de terceiro (cfr. artigo 16.º/3, da LCib).

Quanto à *remissão do n.º 3 da Proposta para o disposto nos n.os 5 a 8 do artigo 16.º, nada tem de inovador ou contrário ao actual artigo 17.º*, pois a apreensão de correio electrónico e similar constitui um caso especial de apreensão de dados, devendo evidentemente respeitar o preceituado nos n.os 5 e 6 do artigo 16.º, da LCib, os quais remetem para o regime geral dos artigos 180.º-182.º, do CPP. Por outro lado, tratando-se sempre da apreensão de dados informáticos, naturalmente se aplicarão as formas de apreensão previstas nos n.os 7 e 8 do artigo 16.º, da LCib. A única forma de apreensão de correio electrónico e similar que poderá suscitar dúvidas é a referida no n.º 7, alínea *d)* (eliminação não reversível ou bloqueio do acesso a dados), tendo em conta o que se dispõe no artigo 35.º/1, da CRP ("todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito").

O *n.º 4 da Proposta* corresponde basicamente ao disposto no artigo 179.º/3, do CPP, mas eliminando muitas das dúvidas actualmente suscitadas pela remissão genérica do artigo 17.º, da LCib, para o regime da apreensão de correspondência física. Em causa neste n.º 4 da Proposta já não está a apreensão do correio electrónico e similar, mas *a junção aos autos, para valerem como prova, das mensagens que o Ministério Público enquanto "dominus" do inquérito seleccionou para esse efeito – tendo, claro, previamente tomado conhecimento do respectivo conteúdo* – por as considerar "de grande interesse

para a descoberta da verdade ou para a prova". Ao juiz, cabe somente ponderar a junção aos autos destas mensagens, considerando os interesses conflituantes no caso concreto, permitindo-se, assim, a valoração no processo das mensagens apreendidas com intervenção apenas do Ministério Público.

Ao invés, o actual artigo 17.º, da LCib: (i) exige a intervenção do juiz para a apreensão *ab initio* de correio electrónico; depois, graças à remissão para o artigo 179.º/3, do CPP, requer nova intervenção do juiz para: (ii) este se certificar da autenticidade e integridade das mensagens antes apreendidas ("o juiz que tiver ordenado ou autorizado a diligência é o primeiro a tomar conhecimento do conteúdo da correspondência apreendida"), e (iii) decidir da sua junção aos autos, para efeitos de valoração como prova, posto que se revelem de grande interesse para a descoberta da verdade e para a prova e que a essa valoração se não oponham os interesses do caso concreto.

O n.º 6 da Proposta, depois de tudo o que foi regulado pelos números anteriores, limitou a remissão para o regime geral da apreensão de correspondência ao disposto no n.º 2 e à parte final do n.º 3 do artigo 179.º do CPP. De notar que a aplicação do n.º 1 do artigo 179.º à apreensão de correio electrónico e similar já é hoje impedida pela Lei do Cibercrime, tendo em conta o âmbito de aplicação das respectivas normas processuais, com excepção dos artigos 18.º e 19.º, incluindo, portanto, o artigo 17.º (cfr. artigo 11.º/1).

7. Tendo em conta o teor da alteração ao artigo 17.º, da LCib, vertida no artigo 5.º do Decreto n.º 167/XIV da Assembleia da República, e as normas constitucionais invocadas para concluir pela inconstitucionalidade, quais terão sido, em seu entender, os principais argumentos usados pelo Tribunal constitucional para chegar à decisão de inconstitucionalidade? **(4,5 valores)**

Seguindo a ordem das normas da Constituição invocadas, o Tribunal Constitucional terá argumentado que:

A *apreensão de correio electrónico e similar pode comprimir consideravelmente a reserva da intimidade da vida privada* (artigo 26.º/1, da CRP), considerando que hoje, perante a utilização massiva do correio electrónico para tratar dos mais diversos assuntos da vida pessoal, familiar e profissional, a respectiva apreensão permite devassar e conhecer todas vertentes da vida da pessoa atingida pela diligência.

A apreensão de mensagens de correio electrónico e outras de natureza semelhante *atinge, de forma grave, o sigilo da correspondência e dos outros meios de comunicação privada*, cuja inviolabilidade se encontra consagrada no artigo 34.º/1, da CRP. Face ao artigo 17.º, da LCib, é irrelevante se as mensagens em causa foram ou não lidas pelo destinatário, contrariamente à correspondência física, cuja apreensão apenas se sujeita ao exigente regime previsto no artigo 179.º, do CPP, enquanto a comunicação ainda estiver em curso. Pelo contrário, o artigo 17.º, da LCib, ao exigir a intervenção inicial do juiz e ao remeter para o artigo 179.º, do CPP, optou por sujeitar a apreensão do correio

electrónico e similar ao regime das comunicações em curso, sem considerar se as mensagens em causa tinham ou não sido lidas/abertas pelo respectivo destinatário. A esta conclusão chegou o Acórdão de Fixação de Jurisprudência do STJ, n.º 10/2023.

As mensagens de correio electrónico e outras de natureza similar são dados pessoais (cfr. artigo 4.º/1, do RGPD) *informatizados*, aos quais os respectivos titulares têm direito de acesso e, ainda, o direito de conhecer a finalidade a que se destinam (artigo 35.º/1, da CRP). Além disso, só em casos excepcionais previstos na lei é permitido o acesso a dados pessoais de terceiro, ainda que por parte das autoridades competentes para a perseguição criminal (artigos 35.º/4 e 18.º/1, da CRP). Ora, a Proposta de alteração ao artigo 17.º, da LCib, de algum modo vem banalizar a apreensão de correio electrónico e similar, ao permitir a sua apreensão: (i) mediante ordem ou autorização do Ministério Público sempre que este, sem qualquer controlo judicial *a priori*, considere tal diligência necessária para a prova e a descoberta da verdade; e (ii) por OPC, no decurso de pesquisa informática legitimamente ordenada e executada nos termos do artigo 15.º ou em caso de urgência ou perigo na demora, ainda que sujeita a validação subsequente pela autoridade judiciária competente.

Os *n.os 1 e 2 da Proposta desrespeitam a reserva de juiz*, sempre que estejam em causa actos instrutórios que directamente contendam como direitos fundamentais (artigo 32.º/4, da CRP), como sucede com a apreensão de correio electrónico e similar. Esta comprime de forma grave os direitos à reserva da intimidade da vida privada, ao sigilo da correspondência e dos outros meios de comunicação privada e a excepcionalidade do acesso a dados pessoais informatizados por terceiro.

Finalmente, os n.os 1 e 2 da Proposta representam uma *compreensão inadequada, desnecessária e desproporcional de direitos fundamentais de qualquer cidadão* (não apenas do suspeito, arguido ou intermediário – cfr. artigo 179.º/1, alínea *a)*, do CPP), *aquando da investigação de qualquer um dos crimes a que se aplica o regime processual da Lei n.º 109/2009* (cfr. respectivo artigo 11.º/1), independentemente da respectiva gravidade (artigo 18.º/2, da CRP). Compressão que não é compensada pela intervenção subsequente do juiz, somente para decidir e ponderar a junção aos autos (e consequente valoração) das mensagens apreendidas, lidas e seleccionadas pelo Ministério Público por este entender que são de grande interesse para a descoberta da verdade e da prova.

Lisboa, 9 de Julho de 2024.

Teresa Quintela de Brito