FACULDADE DE DIREITO
Universidade de Lisboa

Mestrado em Direito e Prática Jurídica – Especialidade de Direito Penal
2021/2022
Direito Penal V – Cibercrime e Prova Digital
Regência: Teresa Quintela de Brito
Exame – 1.ª Época
24.06.2022

Duração: 1 h e 45 minutos

I
GRUPO DE RESPOSTA OBRIGATÓRIA

Considere os seguintes extractos da Exposição de Motivos e do articulado da Proposta de Lei n.º 11/XV/1.ª do Governo, de 26.05.2022, visando revogar a Lei n.º 32/2008 e alterar o artigo 6.º/2 da Lei n.º 41/2004:

"Não sendo possível que a lei determine a conservação de dados com o único intuito de investigar, detetar e reprimir a comissão de crimes, (...) deve ser possível garantir o acesso a dados que hoje já são conservados, para efeitos de faturação, pelas empresas que oferecem redes e ou serviços de comunicações eletrónicas, e cujo regime já se mostra conforme ao Regulamento (UE) 2016/679 (...) e às Leis n.º 58/2019 e 59/2019 (...)
O facto de existir uma finalidade comercial que justifica o tratamento de dados pessoais não significa que os mesmos não possam vir a ser acedidos, consultados ou utilizados, em respeito pelas referidas regras, com o propósito de proteção do interesse público, como, por exemplo, (...) [a] realização da Justiça, [a] segurança e paz públicas, valores que não podem deixar de ser, igualmente, coadunados com os direitos fundamentais de cada cidadão, em cumprimento do princípio constitucional da proporcionalidade.
(...) há que assinalar a introdução de alterações no artigo 6.º da Lei n.º 41/2004, inscrevendo-se aí um conjunto de dados essenciais para o exercício da atividade comercial das empresas que oferecem redes e ou serviços de comunicações eletrónicas. Estas alterações são motivadas, desde logo, pelos avanços tecnológicos ocorridos nos últimos dez anos em matéria de serviços e de equipamentos – (...) a única alteração a esta Lei ocorreu em 2012 – procurando também garantir-se a segurança da informação e a inviolabilidade das redes, bem como contribuir para a clareza das relações contratuais entre as empresas e os seus clientes.
Acresce que, numa perspetiva de investigação criminal, os dados gerados que importa aditar ao referido artigo 6.º, como identidade internacional de assinante móvel (IMSI), a identidade internacional do equipamento móvel (IMEI) e os códigos de utilizador, são, em si mesmos, dados de identificação e, nessa medida, dados de base que a jurisprudência europeia tem considerado suscetíveis de conservação e de tratamento".

Artigo 1.º - Objeto

A presente lei:

a) Estabelece as regras de acesso, para fins de investigação criminal, a dados tratados pelas empresas que oferecem redes e ou serviços de comunicações eletrónicas;
b) Procede à segunda alteração à Lei n.º 41/2004 (...)

Artigo 2.º - Âmbito de aplicação

A autoridade judiciária pode solicitar dados tratados nos termos do n.º 2 do artigo 6.º da Lei n.º 41/2004 (...) quando haja 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, quanto a crimes:

a) Previstos nos n.ºs 1 e 2 do artigo 187.º do Código de Processo Penal (...);
b) Previstos na Lei n.º 109/2009 (...); ou
c) Cometidos por meio de sistema informático, contanto que puníveis com pena de prisão de máximo igual ou superior a 1 ano.

(...)

Artigo 8.º - Alteração à Lei n.º 41/2004

O artigo 6.º da Lei n.º 41/2004 passa a ter a seguinte redação[1]:

1 - [...].

2 - [...]:

a) Número ou identificação, endereço e tipo de posto do assinante, códigos de utilizador, identidade internacional de assinante móvel (IMSI) e a identidade internacional do equipamento móvel (IMEI);

b) [...];

c) Data da chamada, grupo data/hora associado, serviço e número chamado;

d) Número de telefone, endereço de protocolo IP utilizado para estabelecimento da comunicação, porto de origem de comunicação, bem como os dados associados ao início e fim do acesso à Internet;

e) [*Anterior alínea d)*].

3 - [...].

4 - [...].

5 - [...].

6 - [...].

7- [...].»

Responda fundamentadamente às seguintes questões:

1. Há alguma diferença quanto ao tipo e âmbito dos dados conservados e transmissíveis ao processo penal ao abrigo da Lei n.º 32/2008, da Proposta de Lei n.º 11/XV/1.ª do Governo e da alteração que ela propõe ao artigo 6.º/2 da Lei n.º 41/2004? **(3 valores)**

---

[1] Eis a actual redacção do artigo 6.º da Lei n.º 41/2004, sob a epígrafe "Dados de tráfego":

"1 - Sem prejuízo do disposto nos números seguintes, os dados de tráfego relativos aos assinantes e utilizadores tratados e armazenados pelas empresas que oferecem redes e/ou serviços de comunicações eletrónicas devem ser eliminados ou tornados anónimos quando deixem de ser necessários para efeitos da transmissão da comunicação.

2 - É permitido o tratamento de dados de tráfego necessários à faturação dos assinantes e ao pagamento de interligações, designadamente:

a) Número ou identificação, endereço e tipo de posto do assinante;

b) Número total de unidades a cobrar para o período de contagem, bem como o tipo, hora de início e duração das chamadas efetuadas ou o volume de dados transmitidos;

c) Data da chamada ou serviço e número chamado;

d) Outras informações relativas a pagamentos, tais como pagamentos adiantados, pagamentos a prestações, cortes de ligação e avisos.

3 - O tratamento referido no número anterior apenas é lícito até final do período durante o qual a fatura pode ser legalmente contestada ou o pagamento reclamado. [Art. 10.º/1 da Lei 23/96 – Lei dos serviços públicos: "O direito ao recebimento do preço do serviço prestado prescreve no prazo de 6 meses após a sua prestação"].

4 - As empresas que oferecem serviços de comunicações eletrónicas só podem tratar os dados referidos no n.º 1 se o assinante ou utilizador a quem os dados digam respeito tiver dado o seu consentimento prévio e expresso, que pode ser retirado a qualquer momento, e apenas na medida do necessário e pelo tempo necessário à comercialização de serviços de comunicações eletrónicas ou à prestação de serviços de valor acrescentado.

5 - Nos casos previstos no n.º 2 e, antes de ser obtido o consentimento dos assinantes ou utilizadores, nos casos previstos no n.º 4, as empresas que oferecem serviços de comunicações eletrónicas devem fornecer-lhes informações exatas e completas sobre o tipo de dados que são tratados, os fins e a duração desse tratamento, bem como sobre a sua eventual disponibilização a terceiros para efeitos da prestação de serviços de valor acrescentado.

6 - O tratamento dos dados de tráfego deve ser limitado aos trabalhadores e colaboradores das empresas que oferecem redes e ou serviços de comunicações eletrónicas acessíveis ao público encarregados da faturação ou da gestão do tráfego, das informações a clientes, da deteção de fraudes, da comercialização dos serviços de comunicações eletrónicas acessíveis ao público, ou da prestação de serviços de valor acrescentado, restringindo-se ao necessário para efeitos das referidas atividades.

7 - O disposto nos números anteriores não prejudica o direito de os tribunais e as demais autoridades competentes obterem informações relativas aos dados de tráfego, nos termos da legislação aplicável, com vista à resolução de litígios, em especial daqueles relativos a interligações ou à faturação".

2. Considerando o objecto e o âmbito de aplicação da Proposta de Lei n.º 11/XV/1.ª do Governo e a alteração que faz ao artigo 6.º da Lei n.º 41/2004, deverá ou não de ter-se por tacitamente revogado o artigo 14.º/4 da Lei do Cibercrime? **(4 valores)**

3. No que respeita à entidade competente para solicitar os dados guardados pelas empresas que oferecem redes ou serviços de comunicações eletrónicas e aos pressupostos do acesso a esses dados considera que o regime resultante da Proposta de Lei n.º 11/XV/1.ª do Governo preserva melhor os direitos, liberdades e garantias dos cidadãos a que respeitam os dados do que a Lei n.º 32/2008? **(4 valores)**

RESPONDA A UM – E A UM SÓ – DOS GRUPOS SEGUINTES:

II

Atente nas seguintes passagens do Sumário do Acórdão do Tribunal da Relação de Lisboa, de 30.09.2021, proc. n.º 3546/20.0JFLSB-A.L1-9, Relatora Lígia Trovão:

(…)

II – A remissão que faz o art. 17.º da LCC para o regime da apreensão de correspondência previsto no CPP (art. 179.º/1) é expressa, (…) pelo que numa situação em que, previamente à realização de uma diligência [busca ao escritório do suspeito e pesquisa informática aos computadores, sistemas e suportes informáticos aí existentes], o MP pretende a apreensão de correspondência de qualquer tipo, terá a mesma que ser autorizada judicialmente, por forma a que seja controlado previamente o próprio acesso a tais elementos físicos ou informáticos (…), ali se incluindo a proporcionalidade e a necessidade do determinado;

(…)

IV– (…) encontrando-se em curso, em fase de inquérito, uma investigação com vista a apurar da eventual prática de um crime de abuso de poder, no decurso de uma busca não domiciliária autorizada pelo MP, a apreensão ordenada por esta autoridade judiciária (MP), de correspondência eletrónica e não eletrónica (física), encontrada no decurso de pesquisa informática, mesmo sem que o MP ou os OPC tivessem tomado conhecimento do respetivo conteúdo, necessita sempre de ser precedida de autorização prévia do Juiz de instrução criminal, sob pena de ser declarada nula tal apreensão nos termos do disposto no n.º 1 do art. 179.º do CPP *e do* arts. 17.º da Lei n.º 109/2009".

1. Diga fundamentadamente se concorda com a argumentação, a solução e a base legal invocada pelo Tribunal da Relação de Lisboa para o caso *sub judicio*. **(4 valores)**

2. Tratar-se-ia de um problema de mera nulidade da apreensão? Se não, qual seria esse problema e que consequências teria? **(3 valores)**

III

Considere os seguintes excertos do Sumário do Acórdão do Tribunal da Relação de Lisboa, de 17.12.2008, proc. n.º 10876/2008-3, Relator Carlos Almeida:

"V – O estabelecimento de uma ligação não autorizada à infra-estrutura de rede da "TV Cabo" [através de um cabo físico], que permite a fruição de um serviço não contratualizado e, por isso, não pago e [que] causa um prejuízo patrimonial àquela empresa, não consubstancia a prática de um crime de furto porquanto o sinal de televisão recebido por cabo não é uma coisa, no sentido em que este conceito é utilizado no artigo 203.º do CP, não sendo o sinal equiparável a qualquer forma de energia.

VI – Esses mesmos factos também não integram o tipo descrito no n.º 2 do artigo 221.º do CP (burla nas comunicações), uma vez que a ligação efectuada não se destina a «diminuir, alterar ou impedir, total ou parcialmente, o normal funcionamento ou exploração de serviços de telecomunicações», nem tem sequer esse efeito".

1. Diga fundamentadamente se concorda com a argumentação e as soluções apresentadas no Acórdão quanto ao afastamento dos crimes de furto e de burla nas comunicações. **(4 valores)**

2. No caso objecto do Acórdão verifica-se a previsão do artigo 3.º/3, 2.ª parte, da Lei do Cibercrime? E, se se verificasse a previsão desta norma, como deveria ser resolvido o concurso entre a burla nas comunicações que realizasse simultaneamente do tipo de falsidade informática, descrito no artigo 3.º/3, 2.ª parte, da Lei n.º 109/2009? **(3 valores)**

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

TÓPICOS DE CORRECÇÃO

I
GRUPO DE RESPOSTA OBRIGATÓRIA

1. **Há alguma diferença quanto ao tipo e âmbito dos dados conservados e transmissíveis ao processo penal ao abrigo da Lei n.º 32/2008, da Proposta de Lei n.º 11/XV/1.ª do Governo e da alteração que ela propõe ao artigo 6.º/2 da Lei n.º 41/2004?** ***(3 valores)***

Entre a Lei n.º 32/2008 e a Proposta de Lei n.º 11/XV/1ª do Governo *há, desde logo, uma diferença quanto à finalidade da conservação dos dados*.

Na primeira lei, os dados são exclusivamente conservados "para fins de investigação, detecção e repressão de crimes". Crimes que têm de ser graves [cfr. artigo 2.º/1, al. *g)*], fora do âmbito de aplicação da Lei do Cibercrime (Lei n.º 109/2009 – LCib), mas que, no âmbito de aplicação desta lei (artigo 1.º: cibercrime e recolha de prova em suporte electrónico), são os previstos no artigo 11.º/1, embora as disposições processuais da LCib não prejudiquem o regime da Lei n.º 32/2008, "em tudo o que não contrarie o disposto" na Lei n.º 109/2009 (artigo 28.º da LCib).

Na Proposta de Lei n.º 11/XV/1ª do Governo, os dados são exclusivamente tratados e conservados para efeitos de "facturação dos assinantes e [de] pagamento de interligações" (artigo 6.º/2 e 3, da Lei n.º 41/2004).

Porém, *o contexto em que os dados são tratados e conservados é idêntico* na Lei n.º 32/2008 e na Proposta de Lei n.º 11/XV/1ª do Governo: oferta de serviços de comunicações electrónicas publicamente disponíveis ou em redes públicas de comunicações (artigos 1.º/1, da Lei n.º 32/2008; e 1.º/2, da Lei n.º 41/2004).

Aparentemente há uma grande diferença quanto ao tipo de dados conservados e transmissíveis ao processo penal ao abrigo da Lei n.º 32/2008 e da Proposta de Lei n.º 11/XV/1ª do Governo.

A primeira lei (artigo 1.º/1) abrange os "*dados de tráfego* [cfr. artigos 2.º, al. *c)*, da LCib; 2.º/1, al. *d)*, da Lei n.º 41/2004; e 2.º/2, al. *c)*, da Lei Orgânica n.º 4/2017], *de localização* [artigos 2.º/1, al. *e)*, da Lei n.º 41/2004, e 2.º/2, al. *b)*, da Lei Orgânica n.º 4/2017] relativos a pessoas singulares ou colectivas, bem como os *dados conexos* necessários para identificar o assinante ou o utilizador registados" (*dados de base* – artigo 2.º/2, al. *a)*, da Lei Orgânica n.º 4/2017). Todos estes dados são tratados, conservados e transmissíveis ao processo penal, nos termos do artigo 9.º da Lei 32/2008, conjugado com o artigo 11.º/1, da LCib, no âmbito de aplicação desta Lei.

A *Lei n.º 41/2004* prevê o tratamento e conservação de *dados de tráfego* (artigo 6.º) e *de dados de localização* (artigo 7.º), sendo certo que *alguns dos dados de tráfego são igualmente dados de base*, definidos pela Lei Orgânica n.º 4/2017 como "os dados de acesso à rede pelos utilizadores, compreendendo a identificação e morada destes, e o contrato de ligação à rede".

No entanto, *o artigo 2.º Proposta de Lei n.º 11/XV/1ª do Governo* apenas admite a transmissão ao processo penal dos dados de tráfego tratados nos termos do artigo 6.º/2, da Lei n.º 41/42004, *parecendo excluir* dessa transmissão *os dados de base e os dados de localização*.

Assim não acontece realmente.

Os *dados de tráfego* descritos no artigo 6.º/2, da Lei n.º 41/42004, já *incluem, naturalmente, os dados de base (necessários ao estabelecimento de uma comunicação electrónica e destinados a garanti-la)*. Atente-se nos dados referidos no actual artigo 6.º/2, al. *a)*, *b)* (tipo de chamadas efectuadas) e *c)* (serviço chamado), da Lei n.º 41/2004. São também (embora não só) dados de base os incluídos na alteração ao artigo 6.º/2 da Lei n.º 41/2004, prevista no artigo 8.º da Proposta de Lei n.º 11/XV/1ª do Governo. É o caso de todos os referidos na nova al. *a*) e em parte das als. *c)* (serviço chamado), e *d)* (número de telefone, endereço de protocolo IP utilizado para estabelecimento da comunicação, porto de origem da comunicação, dados associados ao início e fim do acesso à internet).

E quanto aos dados de localização? Com a Proposta de Lei n.º 11/XV/1ª do Governo, os dados de localização mantêm-se ou não transmissíveis ao processo penal?

O artigo 4.º/1, al. *f)*, da Lei n.º 32/2008, define dados de localização, aparentemente de olhos postos nos telemóveis, como os necessários "para identificar a localização do equipamento de comunicação móvel". O n.º 7 desse preceito esclarece que os dados em causa são: "o identificador da célula do início da comunicação" e "os dados que identifiquem a situação geográfica das células, tomando como ponto de referência os respectivos identificadores de célula durante o período em que se procede à conservação dos dados".

Por seu turno, o artigo 2.º/2, al. *b)*, da Lei Orgânica n.º 4/2017, define dados de localização do equipamento como: "os dados tratados numa rede de comunicações electrónicas ou no âmbito de um serviço de telecomunicações que indiquem a posição geográfica do equipamento terminal de um serviço de telecomunicações acessível ao público, *quando não deem suporte a uma concreta comunicação*". Sim, porque os últimos (dados de localização do equipamento aquando de uma concreta comunicação) integram-se nos dados de tráfego.

Acontece que *a redacção agora proposta pela Proposta de Lei n.º 11/XV/1ª do Governo para a al. d) do n.º 2 do artigo 6.º da Lei n.º 41/2004, inclui dados de localização do equipamento (telemóvel, Ipad, tablet) que acede à internet* através das referências a: "endereço de protocolo IP utilizado para o estabelecimento da comunicação"[2]; "porto de origem da comunicação"; e "dados associados ao

[2] Endereço IP é um endereço exclusivo que identifica um dispositivo na Internet ou numa rede local. O endereço IP é o identificador que permite que as informações sejam enviadas entre dispositivos numa rede: contém as informações de localização e torna o dispositivo acessível para comunicação. A Internet precisa de um meio de distinguir diferentes computadores, roteadores e sites. O endereço IP providencia isso, além de ser uma parte essencial do funcionamento da Internet. Explicação extraída de https://www.kaspersky.com.br/resource-center/definitions/what-is-an-ip-address

início e fim do acesso à internet", incluindo, naturalmente, os dados relativos à localização do equipamento aquando desse acesso. Portanto, pelo menos estes *dados de localização, inerentes a um dado acesso à internet*, e, portanto, incluídos nos dados de tráfego correspondentes a esse acesso, são conservados pelos fornecedores de redes e/ou serviços de comunicações electrónicas acessíveis ao público e, por isso, transmissíveis ao processo penal nos termos do artigo 2.º da Proposta de Lei n.º 11/XV/1ª do Governo.

De fora parecem ter ficado os dados de localização do equipamento de comunicação móvel (artigo 4.º/1, al. *f)*, e n.º 7, da Lei n.º 32/2008), *utilizado para estabelecer uma comunicação sem recurso à internet*. Com a revogação da Lei n.º 32/2008, a transmissão ao processo penal destes dados terá, porventura, de realizar-se através do artigo 189.º/2 do CPP, que, curiosamente, prevê regime mais restritivo do que o estalecido no artigo 2.º da Proposta de Lei n.º 11/XV/1ª do Governo para o acesso aos dados de localização conexos com dado acesso à internet.

Em suma, a Proposta de Lei n.º 11/XV/1ª do Governo continua a permitir a conservação pelos fornecedores de serviços de comunicações electrónicas, acessíveis ao público, dos dados de base, de tráfego e de localização de um equipamento que acedeu à internet. Todos esses dados são igualmente transmissíveis ao processo penal ao abrigo do artigo 2.º da Proposta.

2. **Considerando o objecto e o âmbito de aplicação da Proposta de Lei n.º 11/XV/1.ª do Governo e a alteração que faz ao artigo 6.º da Lei n.º 41/2004, deverá ou não de ter-se por tacitamente revogado o artigo 14.º/4 da Lei do Cibercrime? *(4 valores)***

Já se viu que o artigo 6.º/2, da Lei n.º 41/2004, apesar da epígrafe "Dados de tráfego", inclui também e naturalmente dados de base, caracterizados pela Lei n.º 32/2008 como "dados conexos [aos dados de tráfego e de localização] necessários para identificar o assinante ou o utilizador registado" (artigo 1.º/1); dados que são depois especificados no artigo 4.º/1, als. *a)*, *b)*, *d)* e *e)*, 2, 3 e 5, da Lei n.º 32/2008.

Por sua vez, o artigo 14.º/4 da LCib refere-se à injunção, dirigida pela autoridade judiciária competente (em função da fase do processo – artigo 1.º, al. *b)*, do CPP) aos fornecedores de serviço, público ou privado, para apresentação ou concessão do acesso a dados relativos a clientes ou assinantes, posto que se não trate de dados de tráfego ou de conteúdo. As diversas alíneas do artigo 14.º/4 identificam os dados em causa (essencialmente dados de base, embora incluindo alguns de localização), os quais coincidem com os descritos na redacção actual e proposta para o artigo 6.º/2 da Lei n.º 41/2004, als. *a)*, *c)* e *d)*. A única excepção é constituída pelos dados de localização do equipamento de comunicação, que o artigo 14.º/4, al. *c)*, da LCib, limita aos (geralmente) disponíveis com base num contrato ou acordo de serviço, e o artigo 6.º/2, al. *d)*, da Lei n.º 41/2004, na redacção proposta, estende ao endereço de protocolo IP utilizado para estabelecimento da comunicação e ao porto de origem da comunicação.

Em face disto, a conclusão a retirar vai no sentido da revogação tácita parcial do artigo 14.º/4 da LCib, no âmbito de sobreposição com o preceituado no artigo 2.º da Proposta de Lei n.º 11/XV/1ª do Governo, conjugado com a nova redacção do artigo 6.º/2 da Lei n.º 41/2004.

A revogação não é total, porque:

(i) A injunção prevista no artigo 14.º/4, da LCib, pode ser dirigida às entidades que facultem aos utilizadores dos seus serviços a possibilidade de comunicar por meio de um sistema informático, *não acessível ao público* (*v.g. intranets* de entidades públicas ou privadas – cfr. artigo 2.º, al. *d)*, da LCib). Em contrapartida, a Lei 41/2004 regula o tratamento e conservação dos dados pessoais no contexto da prestação de serviços de *comunicações electrónicas acessíveis ao público em redes de comunicações públicas* (art. 1.º/2);

(ii) O artigo 14.º/4, al. *c)*, da LCib, parece continuar a permitir à autoridade judiciária que aceda a dados de localização do equipamento de comunicações, geralmente disponíveis com base num contrato ou acordo de serviços, sempre que necessário à produção de prova, tendo em vista a descoberta da verdade (artigo 14.º/1), prescindindo, portanto, dos mais rigorosos pressupostos estabelecidos pelo artigo 2.º da Proposta de Lei n.º 11/XV/1ª do Governo.

3. No que respeita à entidade competente para solicitar os dados guardados pelas empresas que oferecem redes ou serviços de comunicações eletrónicas e aos pressupostos do acesso a esses dados considera que o regime resultante da Proposta de Lei n.º 11/XV/1.ª do Governo preserva melhor os direitos, liberdades e garantias dos cidadãos a que respeitam os dados do que a Lei n.º 32/2008? *(4 valores)*

Não, tudo ponderado, o regime de acesso aos dados tratados e preservados pelas empresas fornecedoras de serviços de comunicações electrónicas acessíveis ao público em redes de comunicações públicas, que resulta da Proposta de Lei n.º 11/XV/1ª do Governo, não preserva melhor os direitos, liberdades e garantias dos cidadãos do que o previsto no artigo 9.º da Lei n.º 32/2008, mesmo quando este é chamado a aplicar-se no âmbito de aplicação da Lei do Cibercrime (artigos 1.º e 11.º da Lei n.º 109/2009).

Assim sucede, porque:

a) O artigo 2.º da Proposta de Lei n.º 11/XV/1ª do Governo permite que a autoridade judiciária, competente em cada fase do processo, solicite os dados de tráfego, de base e de localização referentes aos assinantes, nos termos da nova redacção do artigo 6.º/2 da Lei n.º 41/2004. O que significa que, *no inquérito, essa competência cabe ao Ministério Público*. Em contrapartida, o artigo 9.º da Lei n.º 32/2008 reserva essa competência ao juiz de instrução, em conformidade com o artigo 32.º/4 da CRP, pois o acesso a dados de tráfego e de localização inerentes a dada comunicação electrónica representa grave

intrusão nos direitos à reserva da vida privada, ao sigilo das comunicações e à autodeterminação informativa (artigos 26.º/1, 34.º/1 e 4, 35.º/1 e 4, da CRP).

b) O artigo 2.º da Proposta de Lei n.º 11/XV/1ª do Governo possibilita o acesso aos dados de tráfego e de localização inerentes a certa comunicação electrónica *em qualquer fase do processo*. Ao invés, do disposto no artigo 9.º/2 da Lei n.º 32/2008 extrai-se que o acesso a esses dados só pode ter lugar no inquérito, na medida em que o juiz autoriza a transmissão somente a requerimento do Ministério Público ou da autoridade de polícia criminal competente.

c) Ao contrário do artigo 9.º/3 da Lei n.º 32/2008, o artigo 2.º da Proposta de Lei n.º 11/XV/1ª do Governo *não limita subjectivamente as pessoas a quem respeitam os dados a transmitir*, ao suspeito ou arguido, ao intermediário e à vítima do crime, violando, consequentemente, os artigos 18.º/2, 34.º/1 e 4, e 35.º/1 e 4, da CRP, já que converte em regra a excepção, que deveria ser legitimada pela necessidade de assegurar a descoberta da verdade e a eficácia da perseguição penal ante a suspeita de envolvimento na prática de um crime por parte das pessoas cujos dados são transmitidos ao processo penal.

d) No que respeita ao âmbito objectivo da transmissão de dados, o artigo 2.º da Proposta de Lei n.º 11/XV/1ª do Governo *alarga genericamente o catálogo de crimes em que essa transmissão é possível a todos os previstos no artigo 187.º/1 e 2 do CPP*. Assim sucede, não obstante restringir o catálogo de crimes previsto no artigo 11.º/1 da LCib, que hoje se impõe à Lei n.º 32/2008 no âmbito de aplicação da Lei n.º 109/2009 (cfr. artigo 11.º/2 desta Lei).

e) Está *ausente* do artigo 2.º da Proposta de Lei n.º 11/XV/1ª do Governo uma norma como a vertida no artigo 9.º/4 da Lei n.º 32/2008, que fornece ao juiz um *critério de ponderação da necessidade e proporcionalidade da transmissão* de dados pessoais atendendo à respectiva categoria, às autoridades competentes com acesso aos dados e à protecção do sigilo profissional.

f) A notificação do titular dos dados transmitidos, prevista no artigo 3.º da Proposta de Lei n.º 11/XV/1ª do Governo, vai formalmente ao encontro do (único) fundamento de inconstitucionalidade do artigo 9.º da Lei n.º 32/2008, declarada pelo Acórdão do Tribunal Constitucional n.º 268/2022, por violação do direito à autodeterminação informativa (artigo 35.º/1 da CRP) e à tutela jurisdicional efectiva do titular dos dados transmitidos (artigo 20.º/1 da CRP). A verdade, porém, é que esta *notificação pode ser protelada pelo Ministério Público até ao despacho de encerramento do inquérito, sem qualquer possibilidade de controlo pelo juiz de instrução, pela CNPD* (que, nos termos do artigo 6.º da

Proposta, efectua apenas um controlo anual, anonimizado e posterior à transmissão de dados) e *pela/s pessoa/s a quem os dados respeitam*. O que se traduz numa gravíssima e inequívoca violação: (i) da reserva constitucional de juiz para actos instrutórios que directamente contendam com direitos fundamentais (artigo 32.º/4 da CRP); e (ii) do direito de acesso ao direito e aos tribunais por parte dos titulares dos dados transmitidos. Violação tanto mais grave e insuportável quanto o artigo 2.º da Proposta de Lei n.º 11/XV/1ª do Governo não limita o círculo de pessoas cujos dados pessoais e de comunicações são transmitidos ao processo penal.

Em suma: o artigo 2.º da Proposta de Lei n.º 11/XV/1ª do Governo estende aos dados de tráfego e de localização conexos com dada comunicação electrónica o regime do artigo 14.º/1 e 4, da LCib, apenas substituindo a mera necessidade da diligência para a produção de prova (no âmbito de aplicação do artigo 6.º/2 da Lei n.º 41/2004) pela exigência acrescida (mas não judicialmente controlável na fase de inquérito) da existência de razões para crer que a mesma é indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter. Este o único aspecto do regime consagrado no artigo 9.º da Lei n.º 32/2008 que o artigo 2.º da Proposta de Lei n.º 11/XV/1ª do Governo conservou.

RESPONDA A UM – E A UM SÓ – DOS GRUPOS SEGUINTES:

II

1. Diga fundamentadamente se concorda com a argumentação, a solução e a base legal invocada pelo Tribunal da Relação de Lisboa para o caso *sub judicio*. *(4 valores)*

O TRL tem razão na conclusão a que chega. Deveria ter sido previamente autorizada (ou ordenada) pelo juiz a apreensão:

(i) Da correspondência física fechada encontrada aquando de uma busca não domiciliária (artigos 174.º/3 e 179.º/1, do CPP); e

(ii) Do correio electrónico encontrado nos computadores, sistemas e suportes electrónicos existentes no escritório do suspeito, mesmo que localizado fora do programa informático destinado à recepção e envio de mensagens electrónicas. O que, aliás, sucede com a correspondência física fechada (a cujo regime foi equiparada a apreensão de correio electrónico e semelhante), seja qual for o local onde a mesma se encontre.

Mas já a base legal invocada, relativamente à apreensão de correio electrónico, não deveria ter sido o artigo 17.º da LCib, em conjugação com o artigo 179.º do CPP.

Assim sucede porque, no caso, não se verifica a hipótese prevista no artigo 17.º da LCib: que, no decurso de uma pesquisa informática ou de outro acesso legítimo a um sistema informático, sejam (casualmente) encontradas, aí armazenadas, mensagens de correio electrónico e outras de natureza semelhante. Se assim não fosse, o artigo 17.º nada acrescentaria ao disposto nos artigos 15.º e 16.º/3, da LCib e estes preceitos poderiam ser usados para legitimar *fishing expeditions* de correio electrónico.

Ou seja, o artigo 17.º da LCib não pretende aplicar-se às situações em que *ab initio* pretende realizar-se uma busca (domiciliária ou não domiciliária) para apreender mensagens de correio electrónico e similares.

Nestes casos, por se tratar de situação não regulada pela Lei n.º 109/2009 e atenta a remissão operada pelo respectivo artigo 28.º, a norma a aplicar deverá ser a do artigo 189.º/1 do CPP. Estamos perante a apreensão de comunicações ou conversações transmitidas por meio técnico diferente do telefone, designadamente correio electrónico e outras formas de transmissão de dados por via telemática, que se encontram armazenadas em suporte digital.

O que implica, de facto, prévia autorização judicial, limitada à fase de inquérito, e verificação do estado de necessidade da investigação descrito no artigo 187.º/1 do CPP, o qual se não confunde com o "grande interesse para a descoberta da verdade ou para a prova", com que se bastam os artigos 17.º, da LCib, e 179.º/1, do CPP. Mais discutível é a limitação da diligência ao catálogo de crimes vertido no artigo 187.º/1 e 2, do CPP, em se estando no âmbito de aplicação da LCib (artigos 1.º e 11.º).

Graças à remissão do artigo 189.º/1 do CPP para o regime da intercepção de comunicações realizadas por meio de telefone (artigos 187.º e 188.º), não se suscita o problema da eventual exigência de que o juiz, que autorizou ou ordenou a apreensão de correio electrónico e semelhante, seja o primeiro a tomar conhecimento do seu conteúdo a fim de verificar e assegurar a cadeia de custódia da prova. Problema que se discute a propósito do âmbito e sentido da remissão do artigo 17.º da LCib para o regime da apreensão de correspondência física fechada, vertido no artigo 179.º do CPP.

Em suma: tratando-se ou não de busca domiciliária ou equiparada (artigo 177.º/5 e 6, do CPP), por estar em causa a apreensão de correio electrónico e semelhante (artigo 189.º/1, do CPP, *ex vi* artigo 28.º, da LCib) e de correspondência física fechada (artigo 179.º/1, do CPP), a busca e (toda a) apreensão deveriam ter sido previamente autorizadas pelo juiz.

2. Tratar-se-ia de um problema de mera nulidade da apreensão? Se não, qual seria esse problema e que consequências teria? *(3 valores)*

Faltando a prévia autorização judicial para a apreensão de correspondência física fechada e de correio electrónico e similar (encontrados no escritório do suspeito, nas computadores, sistemas e suportes informáticos aí existentes), verificar-se-ia uma intromissão abusiva na vida privada, na correspondência e nas telecomunicações (artigos 32.º/8, da CRP, e 126.º/3, do CPP). Ou seja: estar-se-ia perante a violação de uma proibição de produção de prova, geradora de uma proibição de valoração, não só da prova primária, mas de toda a prova secundária, dela dependente (efeito-à-distância das proibições de prova – artigos 32.º/1 e 8, da CRP, e 122.º, do CPP, por um argumento *a fortiori*).

O regime da violação das proibições de prova não se confunde com o das nulidades processuais (artigo 118.º/3, do CPP), no qual vigora, pelo contrário, o princípio do máximo aproveitamento dos actos processuais (artigo 122.º/3, do CPP).

III

1. Diga fundamentadamente se concorda com a argumentação e as soluções apresentadas no Acórdão quanto ao afastamento dos crimes de furto e de burla nas comunicações. *(4 valores)*

O TRL tem toda a razão quanto ao afastamento do crime de furto, pois o sinal de TV por cabo desviado não constitui uma coisa móvel alheia fisicamente quantificável, nem é susceptível de subtracção e apropriação exclusiva por parte do agente, com consequente afastamento do detentor originário. Também não está em causa o comportamento de "tomar", característico do furto, mas de fazer entregar sem prévia e remunerada contratualização do serviço, típico dos crimes de "enriquecimento" ou contra o património.

O disposto no artigo 277.º/1, al. *d)*, do CP, não contraria este entendimento dos conceitos de coisa e de subtracção para efeitos do crime de furto, nem, aliás, o poderia contrariar. Acontece que os conceitos jurídico-penais são moldados pelos tipos a que respeitam, não se impondo para todas as incriminações o mesmo conceito sistemático, por exemplo, de coisa, documento ou pessoa. Esta uma imposição dos princípios da legalidade e fragmentaridade da tutela penal.

Além disso, a conduta descrita no artigo 277.º/1, al. *d)*, do CP (crime de perigo comum e concreto), não consiste em "subtrair" um serviço de comunicações, mas em provocar impedimento ou perturbação na exploração de serviços de comunicações, por via de uma acção de *subtrair, desviar, destruir, danificar ou tornar não utilizável, total ou parcialmente, coisa ou energia* (esta sim, fisicamente delimitável e quantificável) *que serve tais serviços*.

Algo de semelhante sucede com a incriminação descrita no artigo 204.º/1, al. *j)*, do CP, que não se traduz em "subtrair" a exploração de serviços de comunicações, mas na acção

de subtrair coisa móvel alheia (que não o próprio serviço de comunicações), impedindo ou perturbando, por qualquer forma, a exploração de serviços de comunicações.

O TRL já não tem razão ao excluir o crime de burla nas comunicações (artigo 221.º/2, do CP). Este ocorre logo que alguém, com intenção de obter benefício ilegítimo (no caso a imediata fruição de um serviço de *Pay-TV* não contratualizado), causa a outrem (o fornecedor do serviço) um prejuízo patrimonial (não pagamento do serviço), usando programas, dispositivos electrónicos ou *outros meios (não electrónicos*, como um cabo físico de ligação à infra-estrutura da rede) *destinados a* diminuir, alterar ou impedir, total ou parcialmente, o normal funcionamento ou exploração de serviços de telecomunicações, sem se exigir a efectiva diminuição, alteração ou impedimento do funcionamento do serviço em causa. Basta a idoneidade do dispositivo ou meio para afectar a normal exploração comercial do serviço.

2. **No caso objecto do Acórdão verifica-se a previsão do artigo 3.º/3, 2.ª parte, da Lei do Cibercrime? E, se se verificasse a previsão desta norma, como deveria ser resolvido o concurso entre a burla nas comunicações que realizasse simultaneamente do tipo de falsidade informática, descrito no artigo 3.º/3, 2.ª parte, da Lei n.º 109/2009? *(3 valores)***

Não se verifica no caso a modalidade de falsidade informática prevista no artigo 3.º/3, 2.ª parte, da LCib: actuando com intenção de causar prejuízo a outrem ou de obter um benefício ilegítimo, usar *dispositivo electrónico* que permite acesso a serviço de comunicações e de acesso condicionado (como é o de *Pay-TV*), *cujos dados informáticos foram manipulados* nos termos do n.º 1 daquele artigo 3.º, i.e., mediante introdução, modificação, apagamento, supressão de dados informáticos ou qualquer outra forma de interferir num *tratamento informático de dados*, *que se traduza na produção de dados não genuínos*.

O que, definitivamente, não sucede com a ligação, através de um cabo físico, à infra-estrutura da rede da "TV Cabo". Tal ligação não produz *dados informáticos não genuínos*, mediante *interferência num tratamento informático* de dados, porque o que está em causa é a *mera fruição de um serviço de acesso condicionado não contratualizado, inexistindo qualquer falsificação informática.*

Se o dispositivo de acesso ao serviço de comunicações fosse um dispositivo electrónico cujos dados informáticos tivessem sido objecto de viciação informática, visando o respectivo utilizador a obtenção de um benefício ilegítimo (fruição de serviço de acesso condicionado não contratualizado), com dolo quanto à provocação de um prejuízo patrimonial ao fornecedor, realizar-se-ia tanto a previsão do artigo 3.º/3, da LCib, como a do artigo 221.º/2, do CP.

Apesar da diversidade dos bens jurídicos directamente tutelados por cada uma destas incriminações (o património, na burla; a integridade, fiabilidade e a confiança dos dados e documentos electrónicos no tráfico jurídico-probatório, na falsidade informática), o agente não deve ser responsabilizado em concurso efectivo de crimes, sob pena de dupla valoração e punição do mesmo facto (uso de dispositivo electrónico contrafeito para aceder a serviço de acesso condicionado não contratualizado) e consequente violação do artigo 29.º/5, da CRP.

Assim, deve afirmar-se um concurso aparente de crimes, na modalidade de consunção, sendo o agente responsabilizado pelo crime-fim (a burla nas comunicações), mas com a pena aplicável ao crime-meio (falsidade informática). Só deste modo se esgota o conteúdo de ilícito do facto global do agente, que se não limitou a atentar contra o património de outrem, violando também bens jurídicos especificamente informáticos. Conduta para a qual o artigo 3.º/3 da LCib comina uma pena mais grave do que a estabelecida para o crime-fim (consunção impura).

Só assim não sucederá, se o prejuízo causado pela burla nas comunicações, realizada com recurso a dispositivo electrónico contrafeito, for de valor consideravelmente elevado. Neste caso, a ponderação do desvalor global da conduta do agente impõe que se lhe aplique a pena mais grave cominada para o crime-fim (artigo 221.º/5, al. *b)*, do CP).

Lisboa, 15 de Julho de 2022

Teresa Quintela de Brito