FACULDADE DE DIREITO
Universidade de Lisboa

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 – 2.ª Época: 22.07.2024

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

I
Responda fundamentadamente às seguintes questões:

1. Como articula o disposto nos artigos 6.º/1 e 9.º, da Lei n.º 32/2008, na redacção dada pela Lei n.º 18/2024, com a injunção para apresentação ou concessão do acesso a dados prevista no artigo 14.º, da Lei do Cibercrime? **(3 valores)**

2. Como concilia o disposto no artigo 6.º/2, 3 e 4, da Lei n.º 32/2008, na redacção dada pela Lei n.º 18/2024, com o preceituado no artigo 12.º, da Lei do Cibercrime (preservação expedita de dados)? **(3 valores)**

3. Segundo os Acórdãos do Tribunal Constitucional n.^{os} 268/2022 e 800/2023, que direitos fundamentais obrigam à notificação ao titular dos dados do despacho que autoriza a transmissão dos mesmos às autoridades competentes para a investigação, detecção e repressão de crimes graves? Concorda com os argumentos usados por este Tribunal para impor essa notificação no âmbito de aplicação da Lei n.º 32/2008? São admitidas excepções à notificação no prazo referido? **(4,5 valores)**

4. Por que razão o artigo 6.º/7, da Lei n.º 32/2008 na redacção da Lei n.º 18/2024, exige mais para a conservação dos dados de tráfego e de localização, do que o artigo 9.º, da mesma Lei, para a transmissão de todas as categorias de dados previstas no artigo 4.º às autoridades competentes para a investigação, detecção e repressão de crimes graves? Justifica-se (ou não) essa diversidade de exigências e a diferenciação entre conservação e transmissão/acesso aos dados de base, de tráfego e de localização? **(4,5 valores)**

II
Atente agora nos factos objecto de um Acórdão do Tribunal da Relação de Évora:

a. O arguido AA, à data da prática dos factos, era técnico na área da informática, tendo particulares conhecimentos nessa área.

b. No dia 21.12.2017, AA acedeu de forma não concretamente apurada aos dados de acesso à conta do Instituto da Segurança Social da assistente DD, nomeadamente às credenciais de acesso às funcionalidades dessa conta.

c. Nesse mesmo dia, pelas 20h e 19m, através do seu computador com acesso à internet através do IP ..., AA fazendo uso desses dados, sem o conhecimento ou consentimento da assistente ou do Instituto da Segurança Social, acedeu a essa conta e, no campo respeitante ao NIB, apagou o NIB que constava nesse campo e introduziu o NIB ..., correspondente ao Banco ..., cuja titularidade pertence ao arguido.

d. Deste modo, o instituto da Segurança Social, em Janeiro de 2018, realizou o pagamento das prestações devidas à assistente DD, (...) [no] valor total de € 514,32, transferindo os montantes em dívida para o mencionado NIB da conta bancária do arguido AA.

e. No dia 24.01.2018, o arguido AA acedeu de forma não concretamente apurada aos dados de acesso à conta de e-mail ...., [pertencente] à assistente DD, nomeadamente às credenciais de acesso às funcionalidades dessa conta de e-mail.

f. Nesse mesmo dia, pelas 20h e 49m, através do seu computador com acesso à internet através do IP ..., o arguido fazendo uso dos dados de acesso a essa conta, sem o conhecimento ou consentimento da assistente, acedeu a essa conta.

g. No dia 06.02.2018, o arguido AA acedeu de forma não concretamente apurada aos dados de acesso à conta de Facebook da assistente DD, nomeadamente às credenciais de acesso às funcionalidades dessa conta.

h. Nesse mesmo dia, pelas 15h00m, através do seu computador com acesso à internet através do IP ..., o arguido AA fazendo uso dos dados informáticos de acesso à conta de Facebook da assistente DD, sem o conhecimento ou consentimento da mesma, acedeu [a essa conta] e alterou a palavra de acesso, impedindo que a assistente acedesse à mesma".

Em 1.ª instância, o arguido AA foi condenado pela prática de **um crime de falsidade informática,** p. e p. pelo **artigo 3.º/1 e 3**, da Lei n.º 109/2009, na pena de 10 meses de prisão; **um crime de acesso ilegítimo,** p. e p. pelo **artigo 6.º/1 e 3**, da Lei n.º 109/2009, na pena de 6 meses de prisão; e de um **crime de dano relativo a programas ou outros dados informáticos,** p. e p. pelo **artigo 4.º/1,** da Lei n.º 109/2009, na pena de 6 meses de prisão. Operado o cúmulo jurídico das penas parcelares aplicadas, AA veio a ser condenado na pena única de 1 ano e 4 meses de prisão. Pena que o Tribunal da Relação de Évora confirmou.

5. Concorda com a qualificação jurídico-penal dos factos efectuada por ambos os tribunais e com a punição de AA em concurso efectivo de crimes? **(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.

GRELHA DE CORRECÇÃO

I

Responda fundamentadamente às seguintes questões:

1. Como articula o disposto nos artigos 6.º/1 e 9.º, da Lei n.º 32/2008, na redacção dada pela Lei n.º 18/2024, com a injunção para apresentação ou concessão do acesso a dados prevista no artigo 14.º, da Lei do Cibercrime? **(3 valores)**

R.: O *artigo 6.º/1, da Lei n.º 32/2008*, na redacção dada pela Lei n.º 18/2024, impõe aos *fornecedores de serviços de comunicações electrónicas* publicamente disponíveis ou de uma rede pública de comunicações o *dever de conservar*, para efeitos de detecção, investigação e repressão

de crimes graves (cfr. artigo 2.º/1, alínea *g)*, da mesma Lei), *os dados de base* (cfr. artigo 2.º/2, alínea *a)*, da Lei Orgânica n.º 4/2017) referidos nas respectivas alíneas *a)* e *b) e, ainda, os endereços de protocolo IP atribuídos à fonte de uma ligação*. Quanto a este tipo de dados, o dever de conservação é independente de autorização judicial, contrariamente ao que sucede com os dados de tráfego (cfr. artigo 2.º, alínea *c)*, da Lei do Cibercrime) e de localização (cfr. artigo 2.º/1, alínea *e*), da Lei n.º 41/2004). Estes só podem ser conservados pelos fornecedores de serviços mediante autorização judicial, nos termos do artigo 6.º/2, 5 e 7, da Lei n.º 32/2008.

Por sua vez, o artigo 9.º, da Lei n.º 32/2008, *condiciona a transmissão de todas as categorias de dados referidas no artigo 4.º* (de base, tráfego e localização), à existência de um *despacho fundamentado do juiz de instrução*, precedido de promoção pelo Ministério Público (n.ºs 1 e 2). O que, no caso de pendência de um procedimento criminal, parece limitar esta diligência à fase de inquérito.

Já o *artigo 14.º, da Lei do Cibercrime*, permite à *autoridade judiciária competente* – o Ministério Público no inquérito – *ordenar a quem tenha a disponibilidade de dados de base*, incluindo os fornecedores de serviço, *que comunique ao processo ou permita o acesso a dados específicos e determinados desse tipo, sob pena de punição por desobediência*. A injunção para apresentação ou concessão do acesso a dados pode ser emitida em todo o âmbito de aplicação das disposições processuais da Lei do Cibercrime (artigo 11.º/1): processos relativos a crimes previstos nesta Lei; cometidos por meio de um sistema informático; ou relativamente aos quais seja necessária a recolha de prova em suporte electrónico.

Considerando que a *injunção para apresentação ou concessão do acesso a dados* (artigo 14.º, da Lei do Cibercrime) se traduz na *transmissão de dados de base para os procedimentos criminais referidos no respectivo artigo 11.º/1*, logo se constata a sua *oposição ao disposto no artigo 9.º, da Lei n.º 32/2008, após a Lei n.º 18/2024, no âmbito de aplicação desta Lei*.

Oposição que se manifesta, pelo menos, *em três planos*. Primeiro: *o da entidade competente para autorizar a transmissão dos dados*. Sempre o juiz de instrução (artigo 9.º, da Lei n.º 32/2008) *vs.* a autoridade judiciária competente em função da fase do procedimento criminal, *i.e.*, o Ministério Público no inquérito (artigo 14.º, da LCib). Segundo: *o dos pressupostos da diligência*. Nos termos do artigo 9.º, da Lei n.º 32/2008, a transmissão de dados de base, tráfego ou localização, gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas, para fins de detecção, investigação e repressão de crimes graves, só é possível 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", devendo a decisão judicial de transmitir os dados "respeitar os princípios da adequação, necessidade e proporcionalidade, designadamente [quanto] à definição das categorias de dados a transmitir e das autoridades

competentes com acesso aos dados e à proteção do segredo profissional". Em contrapartida, a injunção para apresentação ou concessão do acesso a dados de base pode ser emitida assim que tal diligência se revele necessária à produção de prova tendo em vista a descoberta da verdade. Terceiro plano de oposição: *o do âmbito de aplicação da diligência.* Só detecção, investigação e repressão de crimes graves (artigo 9.º, da Lei n.º 32/2008) *vs.* todos os crimes a que alude o artigo 11.º/1, da LCib.

Uma vez que a *actual redacção do artigo 9.º, da Lei n.º 32/2008*, resultante da Lei n.º 18/2024, é posterior à Lei n.º 109/2009, deverá concluir-se que a primeira *veio derrogar o disposto no artigo 14.º, da LCib, em todo o âmbito de aplicação daquela Lei* (conservação e transmissão de dados gerados ou tratados no contexto do fornecimento de serviços de comunicações electrónicas publicamente disponíveis ou de uma rede pública de comunicações). O intuito manifestamente restritivo da conservação e transmissão de dados (de base, tráfego e localização) gerados ou tratados no mencionado contexto e a exigência de estrita legalidade de todas as restrições a direitos, liberdades e garantias (artigo 18.º/2 e 3, da CRP) obstam a uma interpretação do artigo 9.º, da Lei n.º 32/2008, no sentido de que este preceito apenas seria aplicável à transmissão dos dados (de base, tráfego e localização) gerados ou tratados nesse contexto para fins de investigação, detecção e repressão de crimes graves. Já quando se tratasse da investigação de crimes não graves, maxime dos referidos no artigo 11.º/1, da LCib, regeria esta Lei, incluindo o respectivo artigo 14.º. Só que tal interpretação, ademais, inutilizaria completamente o preceituado no artigo 9.º, da Lei n.º 32/2008.

Em suma: quando se trate de *dados de base, gerados ou tratados no contexto do fornecimento de serviços de comunicações electrónicas publicamente disponíveis ou de uma rede pública de comunicações, a injunção para a sua apresentação*: (i) *apenas será possível durante o inquérito*; (ii) *por crimes graves* na acepção do artigo 2.º/1, alínea *g)*, da Lei n.º 32/2008; e (iii) *terá sempre de provir do juiz de instrução*.

2. Como concilia o disposto no artigo 6.º/2, 3 e 4, da Lei n.º 32/2008, na redacção dada pela Lei n.º 18/2024, com o preceituado no artigo 12.º, da Lei do Cibercrime (preservação expedita de dados)? **(3 valores)**

R.: O artigo 12.º, da LCib, permite à autoridade judiciária competente (o Ministério Público no inquérito), sempre que isso for necessário à produção de prova, ordenar a quem tenha a disponibilidade ou o controlo de dados informáticos específicos, "incluindo dados de tráfego", "designadamente o fornecedor de serviço", que preserve esses dados quando exista "receio de que possam perder-se, alterar-se ou deixar de estar disponíveis". Tal preservação, com a duração máxima de 3 meses prorrogáveis até 1 ano, também pode ser ordenada pelo órgão de polícia criminal mediante autorização da autoridade judiciária competente, ou quando haja

urgência ou perigo na demora, devendo aquele, neste último caso, comunicar imediatamente a facto à autoridade judiciária competente e transmitir-lhe o relatório previsto no artigo 253.º, do CPP. Esta diligência de preservação expedita de dados, incluindo dados de tráfego e de localização, é admissível em todo o âmbito de aplicação das disposições processuais da Lei do Cibercrime (artigo 11.º/1).

Por seu turno, o artigo 6.º/2, da Lei n.º 32/2008, sujeita a conservação de dados de tráfego e de localização, gerados ou tratados no contexto do fornecimento de serviços de comunicações electrónicas publicamente disponíveis ou de uma rede pública de comunicações, a autorização judicial, que só será concedida em caso de necessidade para a realização da finalidade de detecção, investigação e repressão de crimes graves. O pedido de autorização judicial reveste carácter de urgência, devendo ser decidido no prazo máximo de 72 horas. Para salvaguardar a utilidade do pedido de autorização judicial para conservação dos dados de tráfego e de localização, o Ministério Público comunica de imediato aos fornecedores de serviço a apresentação do pedido, não podendo os dados em causa ser eliminados até à decisão final sobre a respectiva conservação.

No âmbito de aplicação da Lei n.º 32/2008, o n.º 4 do artigo 6.º derrogou o disposto no artigo 12.º, da LCib. Hoje, a *preservação expedita de dados de tráfego e de localização, gerados no contexto do fornecimento de serviços de comunicações electrónicas publicamente disponíveis ou de uma rede pública de comunicações:* (i) *apenas é admissível após a apresentação de pedido de autorização judicial para a sua conservação pelo Ministério Público*; (ii) *por ordem deste* (já não de órgão de polícia criminal em caso de urgência ou perigo na demora); (iii) *para finalidades de detecção, investigação e repressão de crimes graves* (já não em todo o âmbito de aplicação da Lei do Cibercrime), e (iv) *somente até à decisão final sobre o pedido de conservação*.

3. Segundo os Acórdãos do Tribunal Constitucional 800/2023, que direitos fundamentais obrigam à notificação ao titular dos dados do despacho que autoriza a transmissão dos mesmos às autoridades competentes para a investigação, detecção e repressão de crimes graves? Concorda com os argumentos usados por este Tribunal para impor essa notificação no âmbito de aplicação da Lei n.º 32/2008? São admitidas excepções à notificação no prazo referido? **(4,5 valores)**

R.: Segundo o Tribunal Constitucional, a notificação ao titular dos dados da respectiva transmissão às autoridades competentes para a detecção, investigação e repressão de crimes graves – quando essa comunicação não seja susceptível de comprometer as investigações, nem a vida ou integridade física de terceiros –, impõe-se sob pena de violação do disposto nos artigos 35.º/1 e 20.º/1, em conjugação com o n.º 2 do artigo 18.º, todos da CRP. O Tribunal Constitucional entende que a ausência de tal notificação implicaria uma restrição desproporcionada dos direitos à autodeterminação informativa e à tutela jurisdicional efectiva,

"por prejudicar a viabilidade prática do exercício do controlo judicial de acessos abusivos ou ilícitos aos dados conservados".

Apesar da presunção de inocência do suspeito ou arguido (artigo 32.º/2, da CRP), estes argumentos afigura-se discutíveis, pois a transmissão dos dados de base, tráfego ou localização: (i) *só é legalmente admissível relativamente a arguido/suspeito*, ao *intermediário e à vítima do crime*, mediante consentimento expresso ou presumido desta; (ii) *se existirem razões para crer que tal diligência é indispensável* à descoberta da verdade ou que a prova seria, de outro modo, impossível ou muito difícil de obter; (iii) *se for adequada, necessária e proporcional para a detecção, investigação e repressão de crimes graves*; e (iv) *depende à partida de autorização judicial*, precedida de promoção (fundamentada) pelo Ministério Público. Neste quadro, não se vislumbra a hipótese prática de uma restrição desproporcionada dos direitos à autodeterminação informativa e à tutela jurisdicional efectiva (do arguido, suspeito ou intermediário de crime grave), tanto mais que a necessidade, para a transmissão, de autorização prévia do juiz de instrução já assegura o controlo judicial de acessos abusivos ou ilícitos aos dados conservados (artigo 9.º, da Lei n.º 32/2008). Dados que, no caso de dados de tráfego e de localização, só puderam *ab initio* ser conservados mediante autorização judicial "reforçada", nos termos do artigo 6.º/2 e 7, da Lei n.º 32/2008.

As excepções à notificação do titular dos dados do despacho que autoriza a sua transmissão, no prazo de 10 dias a contar da respectiva prolação, estão descritas no artigo 9.º/8. Tais excepções só são admitidas na fase de inquérito e não podem subsistir para lá dos 10 dias ulteriores à data em que for proferido despacho de encerramento do inquérito.

4. Por que razão o artigo 6.º/7, da Lei n.º 32/2008 na redacção da Lei n.º 18/2024, exige mais para a conservação dos dados de tráfego e de localização, do que o artigo 9.º, da mesma Lei, para a transmissão de todas as categorias de dados previstas no artigo 4.º às autoridades competentes para a investigação, detecção e repressão de crimes graves? Justifica-se (ou não) essa diversidade de exigências e a diferenciação entre conservação e transmissão/acesso aos dados de base, de tráfego e de localização? **(4,5 valores)**

R.: O disposto no artigo 6.º/2, 3 e 7, da Lei n.º 32/2008, pretendeu ir ao encontro da decisão de inconstitucionalidade, vertida nos Acórdãos n.ºs 268/2022 e 800/2023, da conservação generalizada e indiferenciada de dados de tráfego e de localização relativos às comunicações electrónicas de todos os utilizadores e assinantes, pelo prazo de 3 meses, prorrogáveis até 6 meses, excepto se o respectivo titular se tiver oposto à prorrogação da conservação (para lá dos 3 meses) perante as autoridades competentes. Somente para a prorrogação da conservação por prazos sucessivos de 3 meses até ao máximo de 1 ano (mesmo no caso de oposição à prorrogação do respectivo titular) se exigia autorização judicial, requerida pelo Procurador-Geral da República (artigo 6.º/2 e 3, da Lei n.º 32/2008, na redacção do Decreto n.º 91/XV, da Assembleia da República).

Nos dois Acórdãos, o Tribunal Constitucional entendeu que a conservação dos dados de tráfego e de localização gerados pelas comunicações electrónicas da globalidade dos utilizadores e assinantes, "sem qualquer diferenciação, exceção ou ponderação face ao objetivo prosseguido" (detecção, investigação e repressão de criminalidade grave), permitia a "criação de uma base de dados autónoma – indiferenciada e generalizada – para efeitos de investigação criminal", sendo "claros" os riscos de "extrapolação" quanto ao uso desses dados. O que, segundo o Tribunal Constitucional, se traduzia numa violação particularmente intensa e desproporcional dos direitos fundamentais à reserva da intimidade da vida privada e à autodeterminação informativa (artigos 26.º/1 e 35.º/1, em conjugação com o artigo 18.º/2, da CRP) de todos os utilizadores e assinantes, na ausência de qualquer relação "direta [e] objetiva com os objetivos da ação penal".

Por estar em causa a *conservação de dados de tráfego e de localização de utilizadores e assinantes que não são suspeitos/arguidos, vítimas ou intermediários de crime grave* (cfr. artigo 9.º/2, da Lei n.º 32/2008), o actual artigo 6.º/2, 3 e 7, da mesma Lei, sujeita tal diligência a *autorização judicial urgente, prévia e pontual*, deferida a um colégio constituído pelos presidentes das secções criminais do Supremo Tribunal de Justiça e por um juiz designado pelo Conselho Superior da Magistratura, de entre os juízes mais antigos daquelas secções.

Já para a *transmissão de todas as categorias de dados (de base, tráfego e localização), relativos a suspeito/arguido, vítima ou intermediário, em contexto de estado de necessidade probatório para fins de detecção, investigação e repressão de crimes graves*, o artigo 9.º, da Lei n.º 32/2008, considera *suficiente despacho fundamentado do juiz de instrução*, precedido de promoção do Ministério Público. Por seu turno, a notificação dessa transmissão de dados, ao suspeito/arguido, vítima ou intermediário, possibilita novo controlo judicial de eventual acesso abusivo ou ilícito aos dados conservados.

Dir-se-ia que a diversidade de regimes, para a conservação de dados de tráfego e de localização e para a transmissão de todas as categorias de dados, se justifica à luz do carácter subjectivamente generalizado e indiferenciado da conservação, por confronto com a respectiva transmissão "selectiva", limitada ao suspeito/arguido, vítima ou intermediário de crime grave e, ademais, estritamente adequada, necessária e proporcional.

Contudo, a *primeira perplexidade* surge perante o disposto no artigo 6.º/6, da Lei n.º 32/2008, que proíbe os fornecedores de aceder a quaisquer categorias de dados conservados, considerando que a *efectiva lesão dos direitos à reserva da intimidade da vida privada e à autodeterminação informativa apenas ocorre com o acesso ou a transmissão dos dados*. Acesso ou transmissão para a qual o artigo 9.º, da mesma Lei, reputa suficiente despacho fundamentado do juiz de instrução. Ou seja: parece incompreensível que se exija mais para a mera conservação

(sem acesso) dos dados de tráfego e de localização, do que para a transmissão e o acesso a todas as categorias de dados; momento em que se dá realmente a violação dos direitos à reserva da intimidade da vida privada e à autodeterminação informativa.

A *segunda perplexidade* é suscitada pela *ausência de critérios legais de densificação e ponderação da necessidade de conservação* (subjectivamente generalizada e indiferenciada) *dos dados de tráfego e de localização de quaisquer utilizadores ou assinantes*, para finalidades de detecção, investigação e prevenção de crimes graves, bem como pela *falta de fixação de um limite temporal máximo para a conservação dos dados*. O único limite é o que resulta do preceituado no artigo 11.º/2, da Lei n.º 32/2008.

Se se atender aos riscos inerentes à criação de uma base autónoma (indiferenciada e generalizada) de dados de tráfego e de localização para fins de investigação criminal e ao potencial lesivo (grave e desproporcional) da conservação desse tipo de dados para os direitos fundamentais à reserva da vida privada e à autodeterminação informativa, mal se compreende o referido *vazio legal*. Este *transforma a autorização judicial urgente, prévia e pontual* (por um colégio de juízes do Supremo Tribunal de Justiça*) para a conservação de dados de tráfego e de localização* numa *mera formalidade, ou* numa *manifestação de arbitrariedade e discriminação de certos utilizadores ou assinantes*.

I

5. Concorda com a qualificação jurídico-penal dos factos efectuada por ambos os tribunais e com a punição de AA em concurso efectivo de crimes? **(5 valores)**

R.: O comportamento global de AA. realiza uma pluralidade de tipos legais de crime que tutelam distintos bens, valores ou interesses. Porém, a pluralidade de tipos legais de crime e de bens jurídicos atingidos não constitui critério bastante para a afirmação de um concurso efectivo de crimes (cfr. artigo 30.º/1, do CP).

A *primeira etapa da conduta de* AA., descrita em b., corresponde à prática de um *crime de acesso ilegítimo a sistema informático* (artigo 6.º/1, da LCib), porventura *agravado* nos termos do n.º 5, alínea *a)*, por o agente, através do acesso, ter tomado conhecimento de dados confidenciais protegidos por lei (as credenciais de acesso à conta do Instituto da Segurança Social da assistente). Neste caso, a pena legal é de prisão de 1 a 5 anos.

O *segundo comportamento de* AA. está descrito em c.. Traduz-se na comissão de *novo crime de acesso ilegítimo* (artigo 6.º/1), agora ao sistema informático em que se encontra alojada a conta do Instituto da Segurança Social da assistente, *e,* ainda, de um *crime de falsidade informática* (artigo 3.º/1, da LCib) quando, com intenção de provocar engano nas relações jurídicas, apagou os dados informáticos correspondentes ao NIB da assistente, inserindo os correspondentes ao

NIB da conta bancária de que era titular. Desse modo, AA. produziu dados informáticos não genuínos, com conhecimento de que os mesmos eram aptos a ser tomados como genuínos para finalidades juridicamente relevantes (a transferência das prestações da segurança social devidas à assistente). *Enquanto crime-fim mais gravemente punido, a falsidade informática* (prisão até 5 anos ou multa de 120 a 600 dias) *consome o crime-meio* que constitui *o segundo crime de acesso ilegítimo* (prisão até 1 ano ou multa até 120 dias).

O tribunal *a quo* e o tribunal *ad quem* não têm razão, ao invocarem o artigo 3.º/3, da LCib. AA. limitou-se a falsificar os dados informáticos correspondentes ao NIB do beneficiário das prestações da segurança social devidas à assistente; não usou esses dados. Mas, mesmo que AA. o tivesse feito, o uso de dado ou documento electrónico falsificado pelo próprio falsificador não constitui novo crime de falsificação que se autonomize do primeiro.

O *crime de falsidade informática* (artigo 3.º/1, da LCib) encontra-se, de facto, numa *relação de concurso efectivo com o primeiro crime de acesso ilegítimo* agravado (artigos 30.º/1 e 77.º, do CP).

O facto descrito em d. traduz-se na *consumação do crime de burla clássica* (artigo 217.º/1, do CP), cuja execução AA. iniciara com a falsificação do NIB do beneficiário das prestações sociais devidas à assistente. Esta falsificação induziu astuciosamente em erro o funcionário do Instituto da Segurança Social, o qual, determinado por esse erro, ordenou a transferência daquelas prestações para o NIB do arguido. O crime de burla clássica, na forma simples, não foi sequer considerado pelos tribunais *a quo* e *ad quem*, que parecem tê-lo confundido erroneamente com o crime de falsidade informática previsto no artigo 3.º/3, da LCib.

O *crime de burla clássica não consome a falsidade informática* praticada por AA., porque a falsificação dos dados electrónicos correspondentes ao NIB do beneficiário das prestações sociais em causa não esgota o seu conteúdo de desvalor na prática deste crime de burla. Pelo contrário, os dados electrónicos falseados permanecem no tráfico jurídico-probatório, aptos a serem usados como genuínos para novas transferências de prestações sociais devidas à assistente. Transferências que constituirão outros tantos crimes de burla (artigo 217.º, do CP).

Este crime de burla encontra-se em relação de concurso efectivo com o primeiro crime de acesso ilegítimo agravado e com o crime de falsidade informática.

O quarto comportamento de AA. encontra-se vertido em e. e f.. Como não foi possível apurar se a obtenção dos dados de acesso à conta de *e-mail* da assistente se deu por via de acesso ilegítimo a um sistema informático, deverá considerar-se apenas provada a prática do crime de acesso ilegítimo à conta de *e-mail* da assistente (artigo 6.º/1, da LCib). Este crime de acesso ilegítimo entra em relação de concurso efectivo com os crimes de acesso ilegítimo agravado

[artigo 6.º/5, alínea *a)*], falsidade informática (artigo 3.º/1, da LCib) e burla clássica (artigo 217.º/1, do CP).

A última etapa da conduta de AA. está descrita em g. e h.. Novamente, não foi possível determinar se a obtenção dos dados de acesso à conta de *Facebook* da assistente resultou do acesso ilegítimo a um sistema informático. Certo é somente o acesso ilegítimo ao sistema informático em que se encontra alojada a conta de *Facebook* da assistente, sem autorização desta (artigo 6.º/1, da LCib). O mesmo se diga da prática subsequente do crime de dano informático (artigo 4.º/1), quando AA. alterou a palavra-passe de acesso à conta do Facebook da assistente (dados informáticos de que esta é titular), impedindo-a de aceder a essa conta.

Qual a relação entre estes crimes de acesso ilegítimo à conta de *Facebook* da assistente e de dano informático? Está-se perante crimes com diferentes objectos de ataque e que protegem bens ou interesses jurídicos distintos. A incriminação de acesso ilegítimo tutela a segurança, inviolabilidade, confidencialidade e confiança nos sistemas informáticos (cfr. artigo 2.º, alínea *a)*, da LCib). A incriminação do dano informático visa garantir a integridade, acessibilidade e operacionalidade dos dados e programas informáticos (cfr. artigo 2.º, alínea *b)*, da LCib). Não obstante a diversidade dos objectos da conduta e dos bens ou interesses jurídicos tutelados, pode admitir-se um concurso aparente entre os dois crimes quando o titular do sistema informático ilegitimamente acedido e o titular dos dados ou programas informáticos danificados seja o mesmo. O que parece suceder no caso *sub judicio*, já que a assistente é tanto a titular da parte do sistema informático em que está alojada a sua conta de *Facebook*, como a titular dos dados informáticos destruídos pelo arguido. Assim sendo, deverá entender-se que o crime-meio de acesso ilegítimo é consumido pelo crime-fim de dano informático, aliás, mais gravemente punível.

Em suma: AA. deveria ter sido punido por um *concurso efectivo, real e heterogéneo*, dos crimes de acesso ilegítimo agravado aos dados de acesso à conta da assistente no Instituto da Segurança Social (artigo 6.º/5, alínea *a)*, da LCib), de falsidade informática (artigo 3.º/1, da LCib), de burla clássica simples (artigo 217.º/1, do CP), de acesso ilegítimo à conta de *e-mail* da assistente (artigo 6.º/1) e de dano informático (artigo 4.º/1, da LCib).

A referência dos tribunais *a quo* e *ad quem* ao artigo 6.º/3, da LCib, tem em vista a anterior redacção deste preceito que agravava a pena do crime de acesso ilegítimo para prisão até 3 anos ou multa, quando esse acesso tivesse sido conseguido através da violação de regras de segurança. Hipótese actualmente descrita no artigo 6.º/4, alínea *a)*.

Lisboa, 15 de Agosto de 2024

Teresa Quintela de Brito