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 – 2.ª Época
27.07.2022

Duração: 1 h e 30 minutos

I
Hipótese

Enganado por uma página *web* falsa, Belmiro julgou ter acedido ao *site* do seu banco para efectuar um pagamento *online*, inseriu os respectivos códigos de acesso que foram interceptados por **Carlos**, o criador da página *web* falsa.

Na posse desses dados, **Carlos** usou-os para aceder à conta bancária de Belmiro, a partir da qual ordenou a transferência de €10.000 para a conta bancária de **Elsa**, a sua namorada, conforme previamente combinado entre ambos.

Além disso, **Carlos** inseriu no cartão de crédito de **Elsa** os dados informáticos relativos à conta bancária de Belmiro. **Elsa** utilizou o seu cartão de crédito, com os dados informáticos relativos à conta bancária de Belmiro, para efectuar uma compra numa ourivesaria no valor de €7.500.

Por quantos crimes e por quais deverá o Ministério Público deduzir acusação contra Carlos e Elsa?

Carlos: 6 valores; **Elsa:** 3 valores

II
Recolha de prova do Facebook e sua junção aos autos

Considere o Sumário do Acórdão do Tribunal da Relação do Porto de 13.04.2016, proc. n.º 471/15.0T9AGD-A.P1, Relator Renato Barroso:

"I – O documento obtido através de recolha de prova em suporte eletrónico consubstanciando uma impressão de uma publicação realizada pelo arguido no mural do seu perfil de *Facebook*, que opera através da internet e no âmbito de um sistema informático, é regulado pela lei do cibercrime.
II – Tal publicação não reveste o carácter de comunicação semelhante a correio eletrónico na medida em que foi colocado pelo próprio num perfil, público, acessível, livre e indiscriminadamente a qualquer pessoa que tenha perfil nessa rede social.
III – Todavia a sua junção aos autos está sujeita aos mecanismos do art. 16.º/1 e 3 da Lei do Cibercrime (Lei 109/2009 de 15/9).
IV - Caso tal documento contenha dados que sejam susceptíveis de revelar dados pessoais ou íntimos, que possam pôr em causa a privacidade de uma pessoa, devem ser apresentados, sob pena de nulidade, ao juiz que decidirá da sua junção tendo em conta os interesses do caso concreto".

Agora atente no Sumário do Acórdão do Tribunal da Relação do Porto de 5.04.2017, Proc. n.º 671/14.0GAMCN.P1, Relator Moreira Ramos:

"I – O Facebook é uma rede social que funciona através da *internet*, operando no âmbito de um sistema informático pelo que a recolha de prova está sujeita à Lei do Cibercrime - DL 109/2009 de 15/9.

II – Constitui prova legal a cópia de informação que alguém publicita no seu mural do Facebook sem restrição de acesso.

III – Só está sujeita à disciplina do art.º 16.º/1 e 3 da Lei do Cibercrime a apreensão da informação original inserta na plataforma, esteja ou não disponível".

Responda fundamentadamente às seguintes questões:

1. Qual dos acórdãos tem razão e porquê? **(4 valores)**
2. Estando em causa a apreensão da informação original inserta na plataforma do Facebook quem deve ordená-la ou autorizá-la e quem, porventura, decide da sua junção aos autos? **(3 valores)**
3. Se faltar a autorização legalmente exigida para a apreensão e/ou junção aos autos de dados informáticos, qual a consequência? **(2 valores)**

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

Os exames com caligrafia ilegível não serão corrigidos.

TÓPICOS DE CORRECÇÃO

I

1. Responsabilidade jurídico-penal de Carlos

a) Criação da página web falsa relativa a uma instituição bancária verdadeira: crime de falsidade informática (artigo 3.º/1 da LCib):

Carlos, com intenção de provocar engano nas relações jurídicas, introduziu dados informáticos e produziu dados não genuínos (a página web falsa) com a intenção de que os mesmos fossem usados como genuínos para finalidades juridicamente relevantes (realização de pagamentos e operações bancárias) pelos clientes do banco em causa. A página web criada parece ser efectivamente idónea para o efeito.

Crime doloso, com duplo elemento subjectivo especial da ilicitude, que acresce ao dolo de realização da conduta típica.

Crime material ou de resultado, consistindo este na produção, espácio-temporalmente separada da acção típica, de dados ou documentos informáticos não genuínos, idóneos a ser tomados como verdadeiros no tráfico jurídico probatório.

Crime de dano quanto ao bem jurídico da operacionalidade e integridade de dados e programas informáticos; crime de perigo face ao bem jurídico da fé pública nos dados e documentos informáticos no tráfico jurídico-electrónico probatório.

b) Captação dos dados relativos à conta bancária de Belmiro e dos códigos de acesso à mesma: crime de intercepção ilegítima (artigo 7.º da LCib)

Carlos, sem permissão legal e sem autorização de Belmiro (titular do direito do sistema ou de parte dele), através de meios técnicos, interceptou transmissões de dados informáticos provenientes do sistema informático de que Belmiro é titular.

Crime doloso e de dano para a integridade, segurança e confidencialidade dos dados e sistemas informáticos; crime de resultado espácio-temporalmente destacado da conduta típica, que se traduz na efectiva intercepção dos dados.

c) Usando os dados bancários e os códigos de acesso à conta bancária de Belmiro, acedeu ao sistema informático do banco em que se encontra alojada a conta de Belmiro: crime de acesso ilegítimo a um sistema informático (artigo 6.º/1 e 4, al. *a),* da LCib)

Crime doloso, de dano da segurança e confidencialidade dos sistemas informáticos; crime de resultado, consistente no efectivo acesso não autorizado a um dado sistema informático ou a parte dele.

d) Uso dos dados bancários de Belmiro e dos códigos de acesso à respectiva conta para realizar uma transferência no valor de €10.000 para a conta bancária de Elsa: crime de abuso de dados de pagamento (artigo 225.º/1, al. *d)*, e 5, al. *a)*, do CP)

Carlos, com intenção de obter para si e para terceiro (Elsa) enriquecimento ilegítimo, usou dolosamente dados respeitantes a dispositivo incorpóreo que permite o acesso a sistema de pagamento, e determinou a transferência de moeda, causando desse modo prejuízo patrimonial de valor elevado (porque superior a €5.100 – artigo 202.º, al. *a)*, do CP) a Belmiro.

Crime doloso a que acresce um elemento subjectivo especial respeitante a um resultado não compreendido no tipo objectivo (o enriquecimento ilegítimo). Logo, trata-se de um crime de resultado cortado ou parcial.

Crime de resultado, que se exprime na provocação de um prejuízo patrimonial. Crime de dano para o património.

Através desta conduta, Carlos realizou simultaneamente o crime de burla informática: com intenção de obter enriquecimento ilegítimo para si e para terceiro, causou dolosamente a Belmiro um prejuízo patrimonial de valor elevado, mediante utilização de dados sem autorização (artigo 221.º/1 e 5, al. *a)*, do CP)

Porém, o crime de abuso de dados de pagamento, agravado pelo valor elevado do prejuízo, enquanto norma especial relativa ao uso não autorizado de dados de pagamento, prevalece sobre a norma geral que descreve o crime de burla informática, apesar da identidade das respectivas penas legais.

e) Ordem falsa de transferência, da conta bancária de Belmiro para a de Elsa, da quantia de €10.000: crime de falsidade informática (artigo 3.º/1 da LCib)

Carlos, com intenção de provocar engano nas relações jurídicas bancárias, introduziu dolosamente, no sistema informático que aloja a conta bancária de Belmiro, os dados relativos a esta conta e os respectivos códigos de acesso, produzindo um documento electrónico não genuíno quanto à autoria da ordem de transferência, documento este apto a ser considerado para finalidades juridicamente relevantes como se fosse verdadeiro.

O crime de acesso ilegítimo ao sistema informático que aloja a conta bancária de Belmiro, pela sua instrumentalidade, não tem autonomia punitiva quanto a este outro crime de falsidade informática (consunção, sob a forma de facto anterior e concomitante não punível).

f) Inserção no cartão de crédito de Elsa dos dados informáticos relativos à conta bancária de Belmiro: crime de contrafacção de cartão de pagamento (artigo 3.º-A da LCib)

Carlos, com intenção de provocar engano nas relações jurídicas, dolosamente contrafez cartão que permite o acesso a sistema ou meio de pagamento, introduzindo os dados respeitantes à conta bancária de Belmiro e modificando os dados incorporados no cartão de crédito de Elsa.

g) Concurso de crimes

Apesar de ter realizado o tipo de todos os crimes referidos, Carlos não deverá ser efectivamente punido por todos eles, sob pena de violação do princípio da proibição da dupla valoração e punição dos mesmos factos (artigo 29.º/5 da CRP).

Assim, haverá concurso efectivo, real (várias condutas naturalísticas) e heterogéneo (artigo 30.º/1 e 77.º do CP) entre os seguintes crimes:

- *Falsidade informática* (criação da página web falsa relativa a instituição bancária autêntica) *e intercepção ilegítima* de dados informáticos provenientes do sistema bancário de que é titular Belmiro (artigos 3.º/1 e 7.º da LCib);
- *Abuso de dados de pagamento* (artigo 225.º/1, al. *d)*, do CP). Este crime consome indubitavelmente o crime-meio de acesso ilegítimo ao sistema informático que aloja a conta bancária de Belmiro (artigo 6.º/1 da LCib).
- Mais discutível é a consunção, pelo crime previsto no artigo 225.º/5, al. *a)*, do CP, do crime de falsidade informática (artigo 3.º/1 da LCib), pois o tipo de abuso de dados de pagamento não contempla nem esgota todo o conteúdo de ilícito desta parte do comportamento de Carlos. Com efeito, neste momento, além do património de Belmiro, Carlos lesa ou coloca em perigo bens jurídicos tipicamente informáticos. Lesa a integridade dos dados informáticos; coloca em perigo o bem jurídico da fé pública nos dados e documentos informáticos no tráfico jurídico-electrónico probatório. O que talvez apontasse para a hipótese de concurso efectivo entre os crimes de abuso de dados de pagamento e de falsidade dos documentos electrónicos relativos à ordem de transferência (supostamente efectuada pelo legítimo titular da conta bancária).
- Ainda que se sustente o concurso aparente entre estes dois crimes, a verdade é que sempre se tratará de uma *consunção impura*. Carlos será punido pelo crime-fim de abuso de dados de pagamento, mas com a pena mais grave cominada para o crime de falsidade informática: prisão até 5 anos ou multa de 120 a 600 dias, por confronto com prisão até 5 anos e multa de 10 (artigo 47.º/1 do CP) a 600 dias, prevista no artigo 255.º/5, al. *a)*, do CP. Deste modo, contemplar-se-á a afectação de bens especificamente informáticos, além do bem jurídico do património de Belmiro, tornado dispensável e até, porventura, ilegítima à luz do artigo 29.º/5 da CRP a solução do concurso efectivo entre estes dois crimes.

- Crime de contrafacção de cartão de crédito (artigo 3.º-A da LCib).

2. Responsabilidade jurídico-penal de Elsa:

Ao utilizar o seu próprio cartão de crédito, embora contrafeito mediante a inserção dos dados bancários relativos a Belmiro, para efectuar uma compra numa ourivesaria no valor (elevado) de €7.500, Elsa realizou os seguintes tipos de crime:

- Crime de *burla clássica qualificada* (artigos 217.º e 218.º/1 do CP), pois, com intenção de obter para si enriquecimento ilegítimo, por meio de erro ou engano sobre factos que astuciosamente provocou (de que era a titular da conta bancária cujos dados serviram para efectuar o pagamento), dolosamente determinou o empregado da ourivesaria à prática de um acto de disposição patrimonial (a entrega das jóias) que causou a outra pessoa (o dono da ourivesaria) um prejuízo de valor elevado, pois este não estava a receber um pagamento válido pelas jóias entregues;
- *Uso,* com intenção de causar prejuízo a outrem (Belmiro), *de cartão de crédito contrafeito de conluio com o falsificador* (Carlos) – artigo 3.º-B/1 e 3 da LCib. Crime de mera actividade e de perigo para a fé pública nos cartões, dispositivos e dados de pagamento;
- *Abuso de dispositivo incorpóreo* (os dados informáticos relativos à conta bancária de Belmiro inscritos no respectivo cartão de crédito) *que permite acesso a sistema ou meio de pagamento*, determinando o pagamento de moeda e causando, desse modo, prejuízo patrimonial de valor elevado ao legítimo titular da conta bancária (artigo 225.º/1, al. *c)*, e 5, al. *a)*, do CP).

De novo, apesar da realização de todos estes tipos de ilícito, o artigo 29.º/5 da CRP obsta à punição de Elsa por todos eles. De modo a esgotar o conteúdo de ilícito da conduta global desta agente, a mesma deverá ser punida em concurso efectivo ideal (uma só conduta naturalística) e heterogéneo (artigos 30.º/1 e 77.º do CP) pelos crimes de:

- *Burla clássica qualificada* (artigo 218.º/1 do CP), ante a lesão do património do dono da ourivesaria; e de
- *Abuso de dispositivo (incorpóreo) de pagamento* em razão do prejuízo patrimonial elevado causado a Belmiro (artigo 225.º/1, al. *c)*, e 5, al. *a)*, do CP), embora punível com a pena mais grave cominada para o crime-meio de uso de cartão de pagamento contrafeito de conluio com o falsificador (prisão de 3 a 12 anos, por confronto com prisão até 5 anos ou multa até 600 dias). Estamos, uma vez mais, perante a figura da *consunção impura*, imposta pela necessidade de contemplar de forma esgotante o conteúdo de ilícito do comportamento de Elsa e a pluralidade de bens jurídicos por ele afectados.

II

Responda fundamentadamente às seguintes questões:

1. Qual dos acórdãos tem razão e porquê? *(4 valores)*

Primeiro importa identificar o que há de comum ao posicionamento assumido por ambos os acórdãos, para depois os diferenciar.

Ambos os acórdãos coincidem, embora só o afirme explicitamente o Acórdão de 2016, em que a publicação que alguém faz no respectivo mural na rede social Facebook não constitui uma comunicação semelhante a correio electrónico, cuja apreensão se sujeite ao regime do artigo 17.º da LCib. Não está em causa uma comunicação privada, mas uma publicação efectuada pelo titular do perfil no respectivo mural, publicação acessível a qualquer pessoa que tenha perfil na mesma rede social.

Além disso, ambos os acórdãos sustentam que a recolha de prova na rede social Facebook, que se encontra alojada num sistema informático, sujeita-se à Lei do Cibercrime, sempre que se trate de recolha de prova em suporte electrónico não livremente acessível ao público (artigo 11.º/1, al. *c)*, da LCib).

Diferenciam-se um do outro, na medida em que o Acórdão de 2016 pretende que a impressão de uma publicação realizada pelo arguido no mural do seu perfil no Facebook constitui apreensão de dados informáticos, como tal sujeita ao disposto no artigo 16.º da LCib.

Já o Acórdão de 2017 considera que a cópia de informação que alguém publicita no seu mural do Facebook, sem restrição de acesso, não configura apreensão de dados informáticos em suporte electrónico, de modo que se não rege pela Lei do Cibercrime, mas, subentende-se, pelas regras gerais relativas à prova documental (artigos 164.º e ss. do CPP).

Segundo este Acórdão, somente a apreensão de informação (original), inserta na plataforma em se aloja o Facebook, e, portanto, não acessível a terceiros, se deve realizar nos termos do artigo 16.º da LCib. Quer se trate ou não de informação disponível para terceiros, só neste último caso se tratará de apreensão de dados informáticos em suporte electrónico.

A razão assiste ao Acórdão de 2017, por todas as razões já apresentadas e, ainda, por a impressão de uma publicação feita por alguém no respectivo mural do perfil no Facebook não se traduzir numa qualquer das formas de apreensão de dados informáticos previstas no artigo 16.º/7 da LCib. Com efeito, a cópia dos dados, a que se refere o n.º 7, al. *c)*, reporta-se à cópia digital em suporte informático autónomo, não à impressão em papel de uma publicação no mural do Facebook. A não sujeição desta última situação ao regime da apreensão de dados informáticos alojados em um sistema informático (artigo 16.º da LCib) não obsta a que se possa e deva discutir se a impressão em

causa e a sua junção aos autos representa uma insuportável intromissão na vida privada do arguido ou de terceiros, ao abrigo dos artigos 32.º/8 da CRP, e 126.º/3 do CPP.

2. **Estando em causa a apreensão da informação original inserta na plataforma do Facebook quem deve ordená-la ou autorizá-la e quem, porventura, decide da sua junção aos autos?** ***(3 valores)***

Neste caso, como se viu na resposta anterior, rege o artigo 16.º/1 da LCib. Assim, a apreensão de dados informáticos, sob uma das formas previstas no respectivo n.º 7, deve ser ordenada ou autorizada pela autoridade judiciária competente, que, no inquérito, é o Ministério Público (artigos 1.º, al. *b*), e 263.º/1, do CPP).

Os OPC poderão preceder à apreensão, sem prévia autorização da autoridade judiciária, nos casos descritos no artigo 16.º/2, devendo, no entanto, tal apreensão ser submetida a validação pela autoridade judiciária competente no prazo máximo de 72 horas (artigo 16.º/4 da LCib).

Quando o conteúdo dos dados apreendidos seja susceptível de revelar dados pessoais ou íntimos que possam pôr em causa a privacidade do respectivo titular ou de terceiro, a respectiva junção aos autos (para efeitos de valoração como meio de prova) deverá ser decidida pelo juiz, em função de uma ponderação dos interesses conflituantes no caso concreto (artigo 16.º/3 da LCib). Esta intervenção judicial é necessária para dar cumprimento à reserva constitucional de juiz, sempre que, como é o caso, se trate de diligências instrutórias que directa e gravemente contendam com direitos fundamentais (artigo 32.º/4 da CRP).

3. **Se faltar a autorização legalmente exigida para a apreensão e/ou junção aos autos de dados informáticos, qual a consequência?** ***(2 valores)***

Se os OPC, fora dos casos previstos no artigo 16.º/2 da LCib e sem consentimento do respectivo titular (artigos 178.º/4 e 174.º/5, al. *b)*, do CPP, *ex vi* artigo 28.º da LCib), efectuarem uma apreensão de dados informáticos sem prévia autorização da autoridade judiciária, a prova obtida não poderá ser valorada no processo penal, por ter sido produzida mediante intromissão abusiva na vida privada (artigos 32.º/8 da CRP, e 126.º/3 do CPP). A violação desta proibição de obtenção de prova produzirá efeito à distância, contaminando as provas secundárias alcançadas a partir da prova primária maculada (artigos 32.º/1 e 8 da CRP, e 122.º do CPP, *a fortiori*).

Ao contrário da al. *a)* do n.º 4 do artigo 15.º, o n.º 4 do artigo 16.º não comina expressamente a nulidade para a falta de validação, pela autoridade judiciária competente, da apreensão realizada por OPC. No entanto, idêntico vício se impõe também neste caso. De contrário, inutilizar-se-ia o disposto no artigo 16.º/1 da LCib, no que concerne à licitude e legalidade da apreensão de dados informáticos. Mais: não se trata de mera nulidade processual dependente de arguição nos termos do artigo 120.º/1, al. *d)*, do CPP (*ex vi* artigo 28.º da LCib), mas da violação de uma proibição de

produção de prova mediante intromissão abusiva (i.e., não legalmente autorizada) na vida privada (artigo 118.º/3 do CPP).

Verificando-se a hipótese prevista no artigo 16.º/3 da LCib, a junção aos autos sem intervenção judicial (e consequente valoração como meio de prova) dos dados informáticos altamente pessoais, apreendidos no inquérito por ordem ou autorização do Ministério Público, traduz-se numa violação da reserva de juiz (artigo 32.º/4 da CRP) e numa intromissão abusiva na vida privada. Intromissão abusiva por ausência da intervenção e ponderação judicial legalmente impostas. Agora está-se perante a violação de uma proibição, não de obtenção, mas de valoração da prova. Proibição de valoração que porventura implica a proibição de valorar a prova derivada da prova primária ilegitimamente valorada.

Lisboa, 5 de Agosto de 2022

Teresa Quintela de Brito