FACULDADE DE DIREITO
UNIVERSIDADE DE LISBOA

**DIREITO PROCESSUAL PENAL**

4.º ANO – TURMA NOITE/2022-2023

*Regência*: Prof. Doutor Paulo de Sousa Mendes
*Colaboração*: Mestres João Gouveia de Caires e Licenciada Joana Reis Barata

*Exame escrito da época de recurso* – 16 de fevereiro de 2023

*Duração*: 90 minutos

***Hipótese***

**Jerónimo** trabalhava há já vários anos na ***Eles***, empresa de telecomunicações, enquanto informático. **Fernando**, amigo de longa data de **Jerónimo**, pediu-lhe que lhe fornecesse os dados referentes ao nome, morada e número de telefone de 50.000 clientes (de modo aleatório) para uma finalidade que não lhe podia revelar, a troco do pagamento de € 2.500. **Jerónimo**, considerando que se tratava de uma tarefa bastante simples atendendo aos seus conhecimentos informáticos, acedeu aos referidos dados e entregou-os a **Fernando**, recebendo o pagamento da referida quantia como compensação.

**Natércia**, responsável pelo tratamento daqueles dados, verificou que o sistema registava um movimento estranho associado à exportação de dados referentes a cerca de 50.000 clientes. Desconfiando do sucedido reportou ao seu superior hierárquico, **Gustavo**, que rapidamente denunciou a sua suspeita às autoridades de que os dados em causa tinham sido acedidos e utilizados para fins alheios à empresa.

***Responda, fundamentadamente, às seguintes questões:***

1. O **Ministério Público**, tendo tomado conhecimento da notícia do crime, procedeu à abertura de inquérito. Acontece, porém, que, pese embora tenha apurado que, de facto, foi cometido um crime, não conseguiu determinar quem teria procedido à recolha dos dados. Assim, procedeu ao arquivamento do mesmo. A ***Eles*** pretende agora reagir contra este despacho. Como a aconselharia a reagir? (*3 valores*)

   O meio mais adequado seria recorrer à intervenção hierárquica (artigo 278.º do CPP), uma vez que se desconhece o agente do crime e não pode existir requerimento de abertura de instrução (RAI) contra desconhecidos.

   — Análise das possibilidades de reação por parte do denunciante/ofendido/assistente perante o despacho de arquivamento do MP: intervenção hierárquica ou RAI;

— Comparação dos mecanismos de intervenção hierárquica e RAI e respetivas finalidades;
— Análise dos requisitos para apresentação de RAI e respetivos formalismos, concluindo pela impossibilidade de apresentação de RAI contra desconhecidos;
— Conclusão pela apresentação de intervenção hierárquica, indicação do prazo para o efeito e condições de procedibilidade;
— Discussão sobre eventual pedido de reabertura de inquérito (artigo 279.º do CPP) apenas seria admissível em caso de nova prova, o que não é o caso.

2. Admita agora que o **Ministério Público** apurou que foi **Jerónimo** quem acedeu aos referidos dados e que o acusou pela prática do crime de acesso ilegítimo (p. e p. no artigo 6.º, n.º 1, da Lei do Cibercrime[1]), mediante a apresentação de queixa pela ***Eles***. A ***Eles*** entende, porém, que **Jerónimo** deverá ser julgado por um crime de dano relativo a programas ou outros dados informáticos (p. e p. no artigo 4.º, n.º 1, da Lei do Cibercrime[2]), considerando que, tal como consta da acusação, os dados dos clientes acedidos foram apagados do sistema. Como deverá a ***Eles*** proceder? (*4 valores*)

   A ***Eles*** deverá apresentar uma acusação subordinada nos termos do artigo 284.º, n.º 1, do CPP.
   — Indicar a obrigatoriedade de a ***Eles*** se constituir como assistente e respetivos requisitos;
   — Explicação do regime da acusação subordinada e para que casos a mesma deverá ser utilizada: assistente pode também deduzir acusação por (i) factos acusados pelo MP, (ii) por parte deles, (iii) por outros que não importem alteração substancial daqueles e (iv) para alterar a qualificação jurídica dos factos acusados pelo MP;

---

1

***Artigo 6.º***
***Acesso ilegítimo***

1 - Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, de qualquer modo aceder a um sistema informático, é punido com pena de prisão até 1 ano ou com pena de multa até 120 dias.
(„„)

2

***Artigo 4.º***
***Dano relativo a programas ou outros dados informáticos***

1 - Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, apagar, alterar, destruir, no todo ou em parte, danificar, suprimir ou tornar não utilizáveis ou não acessíveis programas ou outros dados informáticos alheios ou por qualquer forma lhes afectar a capacidade de uso, é punido com pena de prisão até 3 anos ou pena de multa.
(…)

— No presente caso inexistiam factos novos, apenas pretendendo a **Eles** dar uma nova qualificação jurídica aos factos em causa, pelo que deveria fazer uma acusação subordinada (e não requerer a abertura da instrução);
— Valorização da menção ao propósito da abertura de instrução pelo assistente em caso de acusação – a introdução de factos novos de provoquem uma alteração substancial de factos. Menção à existência de uma corrente jurisprudencial, minoritária, que admite a abertura de instrução nestes casos, designadamente com a justificação de que a palavra "factos" não pode ser avaliada atomísticamente, desinserida do sistema processual penal, e em sentido puramente naturalístico, devendo antes ser interpretada na interligação com uma determinada ressonância jurídico-criminal, devendo nestes casos ser admissível a abertura da instrução.
— Sustentando-se o recurso à acusação subordinada, caso tenha sido utilizado o requerimento para a abertura da instrução o mesmo seria rejeitado por inadmissibilidade legal da instrução, nem havendo convite ao assistente a aperfeiçoá-lo ou convolar em acusação subordinada:
    - Inadmissibilidade de aplicação analógica do convite ao aperfeiçoamento do CPC via artigo 4.º do CPP, por se tratar de analogia *in malam partem.*

3. Admita que, no decurso da investigação, o **Ministério Público** procedeu à apreensão de centenas de mensagens de correio eletrónico que se encontravam no computador de **Jerónimo**, entre os quais se encontravam os e-mails trocados com **Fernando** de onde resultava o acordo entre si. O Defensor de **Jerónimo** entende, porém, que a prova obtida não poderá ser utilizada uma vez que *(i)* apesar de a pesquisa ter sido ordenada pelo Juiz de Instrução, a apreensão cautelar foi ordenada e efetuada pelo Ministério Público e *(ii)* o Ministério Público foi o primeiro a visualizar as mensagens em causa. Pronuncie-se:

    a) Sobre os argumentos aduzidos pelo Defensor de **Jerónimo** (*4 valores*); e

    Quanto à pesquisa ter sido ordenada pelo Juiz de Instrução e à existência de apreensão cautelar:
    — Análise do regime da pesquisa e apreensão de correio eletrónico (artigos 15.º e 17.º da Lei do Cibercrime);
    — Análise e tomada de posição fundamentada sobre o regime do artigo 17.º da Lei do Cibercrime, designadamente sobre a possibilidade de existir apreensão cautelar de mensagens de correio eletrónico ou se essa apreensão apenas poderá ocorrer mediante despacho prévio do Juiz de Instrução;
    — Menção quanto à possibilidade de requerer um despacho complementar ao Juiz de Instrução se, no decurso da pesquisa, surgirem elementos de prova relevantes que requerem a sua prévia autorização para serem apreendidos.
    Quanto ao facto de o MP ter sido o primeiro a visualizar as mensagens de correio eletrónico:

— Abordagem da discussão doutrinária e jurisprudencial a respeito da remissão efetuada do artigo 17.º da Lei do Cibercrime para o artigo 179.º do CPP;
— Discussão fundamentada sobre a (in)aplicabilidade de todos os seus requisitos, designadamente sobre a obrigação de ser o Juiz de Instrução o primeiro a visualizar as mensagens em causa.

b) Sobre a possibilidade de ser aberto inquérito contra **Fernando** com base na referida prova (*3 valores*).

Discutir-se a eventual extração de certidão para comunicação ao MP para proceder em conformidade;
— Mesmo que não se pudesse utilizar a prova contra o arguido deste processo, nada obsta a que a prova possa ser utilizada, pelo menos como notícia de crime, para efeitos de abertura de inquérito contra **Fernando**.
— Discutir entre fonte de informação para a abertura de inquérito (limite da admissibilidade no caso) de prova (que não poderia ser valorada como tal).
— Tendo o MP adquirido notícia da prática do crime por **Fernando**, no exercício de funções, estaria obrigado a abrir inquérito, em obediência ao princípio da legalidade/obrigatoriedade da ação penal (artigos 242.º, n.º 1, alínea *b)* e 262.º, n.º 2, do CPP)

4. Admita que, em sede de julgamento, é descoberto que, para além de terem sido acedidos os dados pessoais dos clientes em causa, **Jerónimo** também acedeu aos dados de cartão para pagamento, o que consubstancia a prática do crime p. e p. no artigo 6.º, n.º 3, da Lei do Cibercrime. No final do julgamento, o Juiz, depois de **Jerónimo** se ter pronunciado sobre as questões em causa, condenou-o *(i)* pela prática do crime previsto no artigo 6.º, n.º 3, da Lei do Cibercrime[3], aplicando, contudo, uma pena de apenas 1 ano de prisão (atendendo a que era essa a pena máxima correspondente ao crime pelo qual **Jerónimo** vinha inicialmente acusado); e ainda *(ii)* pela prática de um crime de sabotagem informática (p. e p. no artigo 5.º, n.º 1, da Lei do Cibercrime[4]) uma vez que, conforme resultava da

---

3

***Artigo 6.º***
***Acesso ilegítimo***

1 – (…)
2 –Na mesma pena incorre quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas, um conjunto executável de instruções, um código ou outros dados informáticos destinados a produzir as ações não autorizadas descritas no número anterior.
3 - A pena é de prisão até 2 anos ou multa até 240 dias se as ações descritas no número anterior se destinarem ao acesso para obtenção de dados registados, incorporados ou respeitantes a cartão de pagamento ou a qualquer outro dispositivo, corpóreo ou incorpóreo, que permita o acesso a sistema ou meio de pagamento.
(…)

4

***Artigo 5.º***
***Sabotagem informática***

acusação, o sistema da empresa esteva sem funcionar durante dois dias inteiros devido à elevada quantidade de dados extraídos em simultâneo. Pronuncie-se sobre a validade da decisão final (*4 valores*).

Quanto à condenação pelo crime previsto no artigo 6.º, n.º 3, da Lei do Cibercrime:

- Quanto ao facto de **Jerónimo** também ter acedido aos dados de cartão para pagamento, tal facto configura uma ASF à luz do critério quantitativo previsto no art.º 1.º/*f)* do CPP, uma vez que passa a estar em causa um crime punível com pena mais elevada:
    - Justificação de que estamos perante um facto novo não autonomizável, pelo facto de este não pode ser destacado daquele processo e submetido a um novo processo sem violar o princípio *ne bis in idem*;
- Identificação do regime legal aplicável – art. 359.º/1/3 do CPP): o **Juiz** deveria ter comunicado o novo facto e perguntado se o arguido, assistente e **MP** estariam de acordo em prosseguir o julgamento, atendendo à nova factualidade. Tal informação não consta do enunciado, dizendo-se apenas que **Jerónimo** se pronunciou sobre o facto em causa, o que não bastaria para efeitos da existência de um "acordo", nos termos do artigo 359.º/3 (que neste caso seria possível, continuando a ser competente o Tribunal Singular), pelo que a decisão seria nula (art.º 379.º1/*b)* e 2 do CPP), dependendo de arguição tempestivamente suscitada em sede de recurso ordinário (art.os 410.º/2 e 3 e 411.º/1 do CPP);
- Justificação de que, à luz da lei vigente, não podendo ser tomado em consideração o facto novo, não seria admissível a decisão do juiz, ainda que apenas aplicasse a pena correspondente ao crime pelo que o arguido vinha acusado.

Quanto à condenação pelo crime de sabotagem informática (p. e p. no artigo 5.º, n.º 1, da Lei do Cibercrime)

- Identificação de que estamos diante de uma alteração da qualificação jurídica, pelo que seria admissível que o Juiz condenasse o arguido também por esse crime
- Análise do regime da alteração da qualificação jurídica (artigo 358.º, n.º 3, do CPP), sendo que no caso é dito que **Jerónimo** se terá pronunciado sobre as questões em causa, pelo que nenhuma irregularidade/nulidade existe a este respeito.

---

1 - Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, entravar, impedir, interromper ou perturbar gravemente o funcionamento de um sistema informático, através da introdução, transmissão, deterioração, danificação, alteração, apagamento, impedimento do acesso ou supressão de programas ou outros dados informáticos ou de qualquer outra forma de interferência em sistema informático, é punido com pena de prisão até 5 anos ou com pena de multa até 600 dias.
(…)

— Valorização da menção à doutrina que se debruça sobre a impossibilidade de alterar livremente a qualificação jurídica dos factos em sede de julgamento e respetivas consequências.

Para realizar o exame, pode usar: Constituição da República Portuguesa (CRP), Código Penal (CP), Código de Processo Penal (CPP) e Lei da Organização do Sistema Judiciário (LOSJ).

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

***Nota: as respostas com grafia ilegível não serão avaliadas.***