O crime de falsidade informática

Duarte Alberto Rodrigues Nunes
(Juiz de Direito)
(Doutor em Direito pela Faculdade de Direito da Universidade de Lisboa)

1. Introdução.

O crime de falsidade informática está previsto no art. 3.º da Lei n.º 109/2009, de 15 de setembro, nos termos do qual:

> «*1. Quem, com intenção de provocar engano nas relações jurídicas, introduzir, modificar, apagar ou suprimir dados informáticos ou por qualquer outra forma interferir num tratamento informático de dados, produzindo dados ou documentos não genuínos, com a intenção de que estes sejam considerados ou utilizados para finalidades juridicamente relevantes como se o fossem, é punido com pena de prisão até 5 anos ou multa de 120 a 600 dias.*
> *2. Quando as ações descritas no número anterior incidirem sobre os dados registados ou incorporados em cartão bancário de pagamento ou em qualquer outro dispositivo que permita o acesso a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado, a pena é de 1 a 5 anos de prisão.*
> *3. Quem, atuando com intenção de causar prejuízo a outrem ou de obter um benefício ilegítimo, para si ou para terceiro, usar documento produzido a partir de dados informáticos que foram objeto dos atos referidos no n.º 1 ou cartão ou outro dispositivo no qual se encontrem registados ou*

incorporados os dados objeto dos atos referidos no número anterior, é punido com as penas previstas num e noutro número, respetivamente.
4. Quem importar, distribuir, vender ou detiver para fins comerciais qualquer dispositivo que permita o acesso a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado, sobre o qual tenha sido praticada qualquer das ações prevista no n.º 2, é punido com pena de prisão de 1 a 5 anos.
5. Se os factos referidos nos números anteriores forem praticados por funcionário no exercício das suas funções, a pena é de prisão de 2 a 5 anos».

A essência do crime de falsidade informática reside na manipulação dos dados inseridos num sistema informático ou do seu tratamento por via desse mesmo sistema, acabando por resultar dessa manipulação a criação de documentos ou dados falsos, o que põe em causa a segurança e a fiabilidade dos documentos no tráfico jurídico-probatório, à semelhança do que sucede com os documentos "em sentido clássico" falsos no âmbito do crime de falsificação de documento p. e p. pelo art. 256.º do CP[1].

Como melhor veremos infra, está em causa a equiparação da adulteração de documentos eletrónicos à adulteração de documentos na aceção do art. 255.º, al. a), do CP no âmbito do crime de falsificação de documento p. e p. pelo art. 256.º do CP[2].

O crime de falsidade informática estava previsto na revogada Lei n.º 109/91, de 17 de agosto, mais concretamente no seu art. 4.º, o qual dispunha:

«*1 - Quem, com intenção de provocar engano nas relações jurídicas, introduzir, modificar, apagar ou suprimir dados ou programas informáticos ou, por qualquer outra forma, interferir num tratamento informático de*

[1] Cfr. FARIA COSTA, "Algumas reflexões sobre o estatuto dogmático do chamado "Direito penal informático"", *in* Direito Penal da Comunicação, p. 108, e JOÃO CARLOS BARBOSA DE MACEDO, "Algumas considerações acerca dos crimes informáticos em Portugal", *in* Direito Penal Hoje, p. 236.
[2] Cfr. PEDRO VERDELHO, "Lei n.º 109/2009, de 15 de Setembro", *in* Comentário das Leis Penais Extravagantes, I, pp. 505-506, JOÃO CARLOS BARBOSA DE MACEDO, "Algumas considerações acerca dos crimes informáticos em Portugal", *in* Direito Penal Hoje, p. 236, BENJAMIM SILVA RODRIGUES, Da Prova Penal, IV, pp. 126-127, GARCIA MARQUES/LOURENÇO MARTINS, Direito da Informática, 2.ª Edição, p. 683, e Relatório Explicativo da Convenção sobre o Cibercrime.

> *dados, quando esses dados ou programas sejam suscetíveis de servirem como meio de prova, de tal modo que a sua visualização produza os mesmos efeitos de um documento falsificado, ou, bem assim, os utilize para os fins descritos, será punido com pena de prisão até cinco anos ou multa de 120 a 600 dias.*
> *2 - Nas mesmas penas incorre quem use documento produzido a partir de dados ou programas informatizados que foram objeto dos atos referidos no número anterior, atuando com intenção de causar prejuízo a outrem ou de obter um benefício ilegítimo, para si ou para terceiros.*
> *3 - Se os factos referidos nos números anteriores forem praticados por funcionário no exercício das suas funções, a pena é de prisão de um a cinco anos.*»

Comparando o art. 4.º da Lei n.º 109/91 com o art. 3.º da Lei n.º 109/2009, verificamos que este preceito mantém algumas semelhanças com aquele ao nível dos elementos do tipo (objetivo e subjetivo), mantendo-se inalterado um dos elementos objetivos do tipo («introduzir, *modificar, apagar ou suprimir dados ou programas informáticos ou, por qualquer outra forma, interferir num tratamento informático de dados*») e, ao nível do tipo subjetivo, para além de a conduta apenas ser punível a título de dolo em qualquer das suas formas[3], continua a exigir-se um elemento subjetivo especial do tipo (designação que preferimos à de "dolo específico") (a «*intenção de provocar engano nas relações jurídicas*»); quanto ao uso de documento produzido a partir de dados informáticos que foram objeto dos atos referidos no n.º 1 de ambos os preceitos, um dos elementos objetivos do tipo mantém-se idêntico, apesar de a redação ser algo diversa[4], exige-se também um elemento subjetivo especial do tipo e as condutas apenas são puníveis a título de dolo; e, por fim, a pena aplicável às condutas previstas nos n.ºs 1 e 3 do art. 3.º da Lei n.º 109/2009 (correspondentes aos n.ºs 1 e 2 da Lei n.º 109/91) mantem-se igual, continuando o crime a ter natureza pública.

[3] Cfr. art. 14.º do CP.
[4] Anteriormente, dizia-se «*Nas mesmas penas incorre quem use documento produzido a partir de dados ou programas informatizados que foram objeto dos atos referidos no número anterior*» e agora diz-se «*Quem usar documento produzido a partir de dados informáticos que foram objeto dos atos referidos no n.º 1 (...), é punido com as penas previstas num e noutro número, respetivamente*».

Contudo, também encontramos várias diferenças entre o art. 3.º da Lei n.º 109/2009 e o art. 4.º da Lei n.º 109/91.

Em primeiro lugar, no n.º 1 do art. 3.º da Lei n.º 109/2009, onde, no art, 4.º, n.º 1, da Lei n.º 109/91, se dizia «*quando esses dados ou programas sejam suscetíveis de servirem como meio de prova, de tal modo que a sua visualização produza os mesmos efeitos de um documento falsificado, ou, bem assim, os utilize para os fins descritos*», diz-se agora «*produzindo dados ou documentos não genuínos, com a intenção de que estes sejam considerados ou utilizados para finalidades juridicamente relevantes como se o fossem*»[5].

Em segundo lugar, nas condutas previstas no n.º 3 do art. 3.º da Lei n.º 109/2009 (que corresponde ao art. 4.º, n.º 2, da Lei n.º 109/91), na sequência do seu n.º 2, acrescentou-se uma nova conduta típica: «*Quem, atuando com intenção de causar prejuízo a outrem ou de obter um benefício ilegítimo, para si ou para terceiro, usar (...) cartão ou outro dispositivo no qual se encontrem registados ou incorporados os dados objeto dos atos referidos no número anterior*».

Em terceiro lugar, no art. 3.º, n.ºs 2 e 4, da Lei n.º 109/2009, introduziram-se duas novas condutas típicas: «*Quando as ações descritas no número anterior incidirem sobre os dados registados ou incorporados em cartão bancário de pagamento ou em qualquer outro dispositivo que permita o acesso a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado (...)*» (n.º 2) e «*Quem importar, distribuir, vender ou detiver para fins comerciais qualquer dispositivo que permita o acesso a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado, sobre o qual tenha sido praticada qualquer das ações prevista no n.º 2 (...)*» (n.º 4), sendo essas condutas, à semelhança da prevista no n.º 3, 2.ª parte, punidas de forma

[5] Tal modificação, segundo PEDRO DIAS VENÂNCIO, Lei do Cibercrime, p. 38, dever-se-á ao facto de o legislador ter pretendido adotar uma terminologia mais aproximada à utilizada no art. 7.º da CCiber, o qual dispõe que «*Cada Parte deverá adotar as medidas legislativas e outras que se revelem necessárias para classificar como (...) infrações penais (...) quando praticadas intencional e ilicitamente, a introdução, a alteração, o apagamento ou a supressão de dados informáticos dos quais resultem dados não autênticos, com o intuito de que esses dados sejam considerados ou utilizados para fins legais como se fossem autênticos, quer sejam ou não diretamente legíveis e inteligíveis*».

mais gravosa do que no caso das condutas do n.º 1 e 3.º, 1.ª parte: 1 a 5 anos de prisão, em lugar de 1 mês a 5 anos de prisão ou multa entre 120 e 600 dias.

E, em quarto lugar, no crime de falsificação informática qualificada (atualmente previsto no art. 3.º, n.º 5, da Lei n.º 109/2009 e, anteriormente, no art. 4.º, n.º 3, da Lei n.º 109/91), o limite mínimo da pena aplicável foi aumentado de 1 para 2 anos de prisão, mantendo-se o limite máximo em 5 anos.

Ainda acerca das semelhanças e das diferenças entre o art. 3.º, n.ºs 1 e 3.º, 1.ª parte, da Lei n.º 109/2009 e o art. 4.º, n.ºs 1 e 2, da Lei n.º 109/91, levanta-se a questão de saber se, na lei atual, o âmbito da criminalização é, ou não, mais restrito.

Na verdade, à luz do art. 4.º da Lei n.º 109/91, estariam abrangidas no tipo objetivo as interferências no tratamento de dados ou no funcionamento de programas informáticos que implicassem que estes pudessem vir a produzir documentos eletrónicos falseados («*introduzir, modificar, apagar ou suprimir dados ou programas informáticos ou, por qualquer outra forma, interferir num tratamento informático de dados, quando esses dados ou programas sejam suscetíveis de servirem como meio de prova, de tal modo que a sua visualização produza os mesmos efeitos de um documento falsificado, ou, bem assim, os utilize para os fins descritos*»). Mas, mas, à luz do art. 3.º, n.º 1, da Lei n.º 109/2009, ao falar-se em «*produzindo dados ou documentos não genuínos, com a intenção de que estes sejam considerados ou utilizados para finalidades juridicamente relevantes como se o fossem*», parece que o crime apenas se consumará com a efetiva produção de dados ou documentos não genuínos, *i.e.*, falseados[6].

E cremos que tal representa uma outra diferença face à Lei n.º 109/91, dado que da introdução, modificação, apagamento ou supressão de dados informáticos ou da interferência, de outro modo, num tratamento informático de dados resultará, desde logo, uma realidade material falseada, razão pela qual, quando a

[6] Cfr. PEDRO DIAS VENÂNCIO, Lei do Cibercrime, p. 39, PEDRO VERDELHO, "Lei n.º 109/2009, de 15 de Setembro", *in* Comentário das Leis Penais Extravagantes, I, p. 506, BENJAMIM SILVA RODRIGUES, Da Prova Penal, IV, p. 134, e DIANA VIVEIROS DE SIMAS, O Cibercrime, p. 79.

lei atual fala em «*produzindo dados ou documentos não genuínos*» está a exigir que da introdução, modificação, apagamento ou supressão de dados informáticos ou da interferência, de outro modo, num tratamento informático de dados resulte uma produção de dados ou documentos não genuínos.

Relativamente à fonte desta incriminação, a obrigação da criminalização das condutas que constituem o crime de falsidade informática resulta do art. 7.º da CCiber, bem como, na medida em que aí se impõe a punição da manipulação de dados informáticos (quando se fala em apagar, alterar e suprimir), do art. 4.º da Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de fevereiro (embora apenas no tocante "aos casos que não sejam de menor gravidade")[7].

2. O bem jurídico.

Não existe unanimidade acerca do bem jurídico tutelado pelo crime de falsidade informática, havendo quem entenda que é a integridade dos sistemas informáticos, pretendendo o legislador, por via desta incriminação, impedir a prática de atos que atentem contra a confidencialidade, a integridade e a disponibilidade dos sistemas informáticos (na aceção ampla do art. 2.º, al. a), da Lei n.º 109/2009) e dos dados informáticos (na aceção do art. 2.º, al. b), da Lei n.º 109/2009)[8], bem como a utilização fraudulenta dos mesmos[9]; diversamente, entendem outros que é a segurança nas transações bancárias[10]; e, por fim, entende-se maioritariamente que é a segurança e a fiabilidade dos documentos no tráfico jurídico-probatório (*i.e.*, o mesmo bem jurídico tutelado pelo crime de

[7] Também a Diretiva 2013/40/UE do Parlamento Europeu e do Conselho de 12 de agosto de 2013, que revogou a Decisão Quadro n.º 2005/222/JAI, do Conselho impõe, no seu art. 5.º ("pelo menos nos casos que se revistam de alguma gravidade") a criminalização de algumas das formas de manipulação de dados informáticos referidas no art. 3.º da Lei n.º 109/2009 (mas não da falsidade informática), parecendo-nos que a nossa lei vigente, neste aspeto, está conforme às exigências decorrentes dessa Diretiva.

[8] Cfr. Acórdãos da RL de 30/06/2011, 10/07/2012, da RP de 21/11/2012, 24/04/2013 e 17/09/2014, *in www.dgsi.pt*.

[9] Cfr. Acórdãos da RP de 21/11/2012 e 24/04/2013, *in www.dgsi.pt*, citando o Preâmbulo da CCiber.

[10] Casos de JOÃO CARLOS BARBOSA DE MACEDO, "Algumas considerações acerca dos crimes informáticos em Portugal", *in* Direito Penal Hoje, p. 238 (*ad latus* de outros bens jurídicos) e do Acórdão da RL de 09/01/2007, *in www.dgsi.pt*.

falsificação p. e p. pelo art. 256.º do CP[11])[12], o que se deve à circunstância de o crime de falsidade informática e o crime de falsificação de documento p. e p. pelo art. 256.º do CP serem de tal modo semelhantes (apenas se distinguindo quanto ao *modus operandi*, em que releva a execução pelo meio informático) que, ao nível da visualização dos dados no sistema informático, esses dados acabam por se apresentar como um documento no seu significado "clássico"[13].

Passando a emitir a nossa opinião, consideramos que, consubstanciando-se o crime de falsidade informática na introdução, modificação, apagamento ou

[11] Cfr. HELENA MONIZ, "Art. 256º", *in* Comentário Conimbricense do Código Penal, II, pp. 680 e ss, PINTO DE ALBUQUERQUE, Comentário do Código Penal, p. 672, e LEAL HENRIQUES/SIMAS SANTOS, Código Penal Anotado, 2.º Vol., 3.ª Edição, p. 1097.

[12] Casos de GARCIA MARQUES/LOURENÇO MARTINS, Direito da Informática, 2.ª Edição, pp. 683 e ss, FARIA COSTA, "Algumas reflexões sobre o estatuto dogmático do chamado "Direito penal informático"", *in* Direito Penal da Comunicação, p. 109, FARIA COSTA/HELENA MONIZ, "Algumas reflexões sobre a criminalidade informática em Portugal", *in* BFDUC, 1997, p. 328, BENJAMIM SILVA RODRIGUES, Da Prova Penal, IV, pp. 126-127, PEDRO DIAS VENÂNCIO, "O Crime de Falsidade Informática", *in* JusNet 120/2010, LOPES ROCHA, "A lei da criminalidade informática (Lei n.º 109/01 de 17 de Agosto). Génese e técnica legislativa", *in* Cadernos de Ciência de Legislação, n.º 8, p. 73, PEDRO VERDELHO/ROGÉRIO BRAVO/MANUEL LOPES ROCHA, Leis do Cibercrime, I, p. 250, JOÃO CARLOS BARBOSA DE MACEDO, "Algumas considerações acerca dos crimes informáticos em Portugal", *in* Direito Penal Hoje, p. 238, JOEL TIMÓTEO RAMOS PEREIRA, Compêndio Jurídico da Sociedade da Informação, p. 522, PAULO ALEXANDRE GONÇALVES TEIXEIRA, O fenómeno do *Phishing*, p. 19, DIANA VIVEIROS DE SIMAS, O Cibercrime, pp. 79-80 e Acórdãos da RP de 30/04/2008 e 26/05/2015 e da RE de 19/05/2015, *in www.dgsi.pt*.
De acordo com o citado aresto da RE «*o crime de falsidade informática previsto no artigo 3º da Lei 109/2009 visa proteger a segurança das relações jurídicas enquanto interesse público essencial que ao próprio Estado de Direito compete assegurar e não, acrescentamos nós, a confidencialidade, integridade e disponibilidade de sistemas informáticos, de redes e de dados informáticos, que corresponde ao bem jurídico protegido pelos restantes tipos legais que, juntamente com a Falsidade informática, se encontram agrupados no capítulo que a Lei 109/2009 dedica, indistintamente, às disposições penais materiais.*», porquanto, «*Na verdade, a Convenção sobre Cibercrime do Conselho da Europa, de 2001, conhecida por Convenção Budapeste - adaptada ao direito interno português pela Lei 109/2009 -, prevê a Falsificação informática (art. 7º) no titulo II da secção de Direito penal material, sob a designação, Infracções relacionadas com computadores, enquanto no primeiro título da mesma secção se agrupam as Infrações contra a confidencialidade, integridade e disponibilidade de dados e sistemas informáticos (Acesso ilícito, Intercepção ilícita, Dano provocado nos dados, Sabotagem informática e Utilização indevida de dispositivos). Diferentemente destes últimos tipos penais (que correspondem, grosso modo, aos previstos no segundo capítulo da Lei 109/2009) os bens jurídicos protegidos pelo crime de Falsidade informática previsto no artigo 3º da Lei 109/2009, que se aproxima do crime de falsificação comum (art. 256º do C.Penal), são antes a segurança e credibilidade dos dados e documentos produzidos em computador mediante o tratamento informático de dados, sendo a esta luz que deve interpretar-se aquele tipo legal.*».

[13] Cfr. JOÃO CARLOS BARBOSA DE MACEDO, "Algumas considerações acerca dos crimes informáticos em Portugal", *in* Direito Penal Hoje, pp. 238-239.

supressão de dados informáticos ou na interferência, de qualquer outra forma, num tratamento informático de dados, a prática deste crime irá, inevitavelmente, colocar em causa a integridade do sistema informático onde tais dados se encontrem ou em que tenha lugar o seu tratamento, razão pela qual outra não poderá ser a conclusão senão a de que existe uma lesão da integridade desse sistema informático. Questão diversa é saber se é esse o bem jurídico que o legislador quis proteger com esta incriminação.

Ora, se atentarmos na própria letra da lei, verificamos que, no caso da conduta prevista no art. 3.º, n.º 1, da Lei n.º 109/2009, exige-se uma "intenção de provocar engano nas relações jurídicas", o que representa uma clara alusão ao bem jurídico tutelado pelo crime de falsificação de documento "clássico" (*i.e.* a segurança e a fiabilidade dos documentos no tráfico jurídico-probatório), sendo que dúvidas não existirão de que a manipulação dos dados ou a interferência no seu tratamento é uma conduta similar à falsificação de outros documentos, apenas mudando o meio de executar essa falsificação, pois, no caso do crime de falsidade informática, é utilizado um meio informático para atingir um outro meio informático a fim de introduzir, modificar, apagar ou suprimir dados informáticos ou interferir, de qualquer outra forma, num tratamento informático de dados[14]. Ademais, a CCiber prevê o crime de falsificação informática no Título 2 da Secção de Direito penal material sob a epígrafe de "Infrações relacionadas com computadores" e não no Título 1 da mesma Secção, que inclui as "Infrações contra a confidencialidade, integridade e disponibilidade de dados e sistemas informáticos" (acesso ilícito, interceção ilícita, dano provocado nos dados, sabotagem informática e utilização indevida de dispositivos)[15].

Deste modo, consideramos que o bem jurídico tutelado pelo crime de falsidade informática é a segurança e a fiabilidade dos documentos no tráfico jurídico-probatório (onde se inclui a segurança nas transações bancárias),

[14] No mesmo sentido, GARCIA MARQUES/LOURENÇO MARTINS, Direito da Informática, 2.ª Edição, pp. 683 e ss, e FARIA COSTA, "Algumas reflexões sobre o estatuto dogmático do chamado "Direito penal informático"", *in* Direito Penal da Comunicação, p. 109.
[15] Cfr. Acórdão da RE de 19/05/2015, *in www.dgsi.pt*.

embora, pelas razões sobreditas, o crime de falsidade informática, ainda que de forma meramente reflexa, acabe por tutelar também a integridade dos sistemas informáticos.

E, da circunstância de o bem jurídico tutelado pelo crime de falsidade informática ser a segurança e a fiabilidade dos documentos no tráfico jurídico-probatório, decorre que, como refere OLIVEIRA ASCENSÃO[16], a manipulação de dados próprios do agente (ou do seu tratamento automático) inseridos num sistema informático igualmente do próprio agente (*v.g.* um comerciante alterar um programa informático para obter um resultado que vicia a sua própria escrituração) configura a prática do crime de falsidade informática, uma vez que, nesse caso, continuará a estar em causa a proteção da segurança e a fiabilidade dos documentos no tráfico jurídico-probatório, que também é lesada quando o agente manipula dados informáticos que lhe pertencem (ou manipula o seu tratamento automático) e inseridos num sistema informático que igualmente lhe pertence.

3. A natureza do crime.

Relativamente à natureza do crime de falsidade informática, começando pelo grau de lesão do bem jurídico, no caso das condutas previstas nos n.ºs 1, 2 e 4 (e 5, na parte em que a conduta concretamente adotada corresponda a alguma das condutas previstas nos n.ºs 1, 2 e 4), não ocorre qualquer lesão efetiva do bem jurídico, mas apenas a manipulação de dados informáticos ou do seu tratamento ou a importação/distribuição/venda/detenção, para fins comerciais, de dispositivo que permita o acesso a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado, o que, de acordo com as regras da experiência comum, é passível de criar um perigo para a segurança e a fiabilidade dos documentos eletrónicos no tráfico jurídico-probatório, pelo que

[16] OLIVEIRA ASCENSÃO, "Criminalidade informática", *in* Direito da Sociedade da Informação, II, p. 222.

estamos perante um crime de perigo[17]. Só que a lei não exige que o bem jurídico seja efetivamente, concretamente, colocado em perigo, limitando-se o legislador a presumir (e bem) que tais condutas são passíveis de constituir um perigo para a segurança e a fiabilidade dos documentos eletrónicos no tráfico jurídico-probatório e, por isso, trata-se de um crime de perigo abstrato[18].

Diversamente, no caso das condutas previstas no n.º 3 (e 5, na parte em que a conduta concretamente adotada corresponda às condutas previstas no n.º 3), em que há uma utilização efetiva do documento, a utilização do documento falso atinge a segurança e a fiabilidade que aquele tipo de documento merece ou deve merecer no tráfico jurídico-probatório e, por isso, trata-se de um crime de dano[19].

Passando à modalidade de consumação do ataque ao bem jurídico, no caso das condutas previstas nos n.ºs 1 e 2 (e 5, na parte em que a conduta concretamente adotada corresponda a alguma das condutas previstas nos n.ºs 1 e 2), resultando da atuação do agente uma modificação do mundo exterior (*in casu*, dos dados informáticos que foram objeto da manipulação), estamos perante um crime de dano[20].

Já, no caso das condutas previstas nos n.ºs 3 e 4 (e 5, na parte em que a conduta concretamente adotada corresponda a alguma das condutas previstas nos n.ºs 3 e 4), na medida em que da atuação do agente não resulta qualquer

[17] No mesmo sentido, JOÃO CARLOS BARBOSA DE MACEDO, "Algumas considerações acerca dos crimes informáticos em Portugal", *in* Direito Penal Hoje, p. 238; contra, DIANA VIVEIROS DE SIMAS, O Cibercrime, p. 79, que considera que se trata de um crime de resultado.

[18] No mesmo sentido, JOÃO CARLOS BARBOSA DE MACEDO, "Algumas considerações acerca dos crimes informáticos em Portugal", *in* Direito Penal Hoje, p. 238.

[19] Cfr., embora referindo-se ao crime de falsificação de documento "clássico", PINTO DE ALBUQUERQUE, Comentário do Código Penal, p. 672; contra, na medida em que não diferenciam consoante se trate de falsificação ou de uso de documento falso, considerando que se trata de um crime de perigo abstrato, JOÃO CARLOS BARBOSA DE MACEDO, "Algumas considerações acerca dos crimes informáticos em Portugal", *in* Direito Penal Hoje, p. 238 e, referindo-se ao crime de falsificação de documento "clássico", HELENA MONIZ, "Art. 256º", *in* Comentário Conimbricense do Código Penal, II, p. 681.

[20] Neste sentido, referindo-se ao crime de falsificação de documento "clássico", PINTO DE ALBUQUERQUE, Comentário do Código Penal, p. 672, e, embora distinguido consoante a atividade e os interesses prosseguidos pelo tipo de crime (crime de mera atividade) e a atividade do agente (crime de resultado), HELENA MONIZ, "Art. 256º", *in* Comentário Conimbricense do Código Penal, II, pp. 681-682.

modificação do mundo exterior, apenas ocorrendo uma utilização do documento eletrónico falsificado ou a importação/distribuição/venda/detenção, para fins comerciais, de dispositivo que permita o acesso a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado, estaremos perante um crime de mera atividade[21].

Por fim, ainda quanto à modalidade de consumação do ataque ao bem jurídico, no caso das condutas previstas nos n.ºs 1 e 2 (e 5, na parte em que a conduta concretamente adotada corresponda a alguma das condutas previstas nos n.ºs 1 e 2), estamos perante um crime de execução vinculada, dado que, ainda que a descrição do tipo contenha uma enumeração meramente exemplificativa de várias formas possíveis de manipulação de dados informáticos ou do seu tratamento (como o demonstra a existência de uma cláusula geral), a falsificação terá de ser realizada através da manipulação de dados informáticos ou do seu tratamento (por introdução, modificação, apagamento, supressão, ou interferência de qualquer outro modo no tratamento informático de dados)[22].

E o mesmo sucede no caso das condutas previstas no n.º 4 (e 5, na parte em que a conduta concretamente adotada corresponda a alguma das condutas previstas no n.º 4), uma vez que, para preencher o *tatbestand* desse n.º 4, a atuação do agente terá de consistir na importação, distribuição, venda ou mera detenção, para fins comerciais (e não de uso pessoal) de dispositivo que permita o acesso a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado[23].

---

[21] Cfr., referindo-se ao crime de falsificação de documento "clássico", PINTO DE ALBUQUERQUE, Comentário do Código Penal, p. 672, e HELENA MONIZ, "Art. 256º", *in* Comentário Conimbricense do Código Penal, II, pp. 681-682.

[22] Neste sentido, embora referindo-se ao crime de burla informática e nas comunicações, ALMEIDA COSTA, "Art. 221º", *in* Comentário Conimbricense do Código Penal, II, p. 329, e Acórdãos do STJ de 20/09/2006 e 05/11/2008, *in www.dgsi.pt*; contra, JOÃO CARLOS BARBOSA DE MACEDO, "Algumas considerações acerca dos crimes informáticos em Portugal", *in* Direito Penal Hoje, p. 237.

[23] Contra, na medida em que não opera qualquer distinção consoante as diferentes condutas típicas do crime de falsidade informática, JOÃO CARLOS BARBOSA DE MACEDO, "Algumas considerações acerca dos crimes informáticos em Portugal", *in* Direito Penal Hoje, p. 237.

Diversamente, no caso das condutas previstas no n.º 3 (e 5, na parte em que a conduta concretamente adotada corresponda a alguma das condutas previstas no n.º 3), aí sim, estaremos perante um crime de execução livre, dado que a utilização do documento eletrónico falso poderá ocorrer de uma qualquer forma[24].

4. O crime de falsidade informática simples.

4.1. O tipo objetivo.

No que tange ao tipo objetivo deste crime, encontramos no art. 3.º, n.ºs 1 a 4, da Lei n.º 109/2009, cinco modalidades de conduta típica:

a) Introduzir, modificar, apagar ou suprimir dados informáticos ou por qualquer outra forma interferir num tratamento informático de dados, produzindo dados ou documentos não genuínos (n.º 1);

b) Introduzir, modificar, apagar ou suprimir dados informáticos ou por qualquer outra forma interferir num tratamento informático de dados, produzindo dados ou documentos não genuínos, sempre que os dados que sejam alvo dessa manipulação estejam registados ou incorporados em cartão bancário de pagamento ou em qualquer outro dispositivo que permita o acesso a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado (n.º 2);

c) Usar documento produzido a partir de dados informáticos que foram objeto de introdução, modificação, apagamento ou supressão ou cujo tratamento informático foi alvo de interferência por qualquer outra forma (n.º 3, 1.ª parte);

d) Usar documento produzido a partir de dados informáticos registados ou incorporados em cartão bancário de pagamento

[24] No mesmo sentido, JOÃO CARLOS BARBOSA DE MACEDO, "Algumas considerações acerca dos crimes informáticos em Portugal", *in* Direito Penal Hoje, p. 237.

ou em qualquer outro dispositivo que permita o acesso a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado e que foram objeto de introdução, modificação, apagamento ou supressão ou cujo tratamento informático foi alvo de interferência por qualquer outra forma (n.º 3, 2.ª parte);

e) Importar, distribuir, vender ou detiver para fins comerciais qualquer dispositivo que permita o acesso a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado, "*sobre o qual tenha sido praticada qualquer das ações previstas no n.º 2*" (n.º 4).

Relativamente à primeira modalidade de conduta típica (art. 3.º, n.º 1) e começando pelo conceito de "Dados informáticos", estes deverão ser entendidos na aceção do art. 2.º, al. b), da Lei n.º 109/2009.

Passando à questão de saber em que consiste o "*introduzir, modificar, apagar ou suprimir dados ou programas informáticos ou, por qualquer outra forma, interferir num tratamento informático de dados*", consideramos que os conceitos de "introduzir", "modificar", "apagar", "suprimir" e "interferir" deverão ser interpretados partindo do significado corrente de tais palavras, sendo que, de acordo com o Dicionário Houaiss da Língua Portuguesa,

a) "Introduzir" significa, entre outras coisas, «*fazer inclusão de; incluir, inserir*»;

b) "Modificar" significa, entre outras coisas, «*fazer ou sofrer alteração (em)*», sendo que o sentido que para aqui interessa é a vertente ativa ("*fazer alteração em*");

c) "Apagar" significa, entre outras coisas, «*fazer desaparecer ou desaparecer, sem deixar traço; eliminar(-se)*»;

d) "Suprimir" significa, entre outras coisas, «*agir no sentido de acabar com (algo); extinguir, eliminar, cancelar; tirar (uma parte) de (um todo); cortar, retirar; fazer desaparecer; ocultar, afastar*»; e

e) "Interferir" significa, entre outras coisas, «*interpor-se, misturar-se, alterando a estrutura ou as características (de algo); afectar*».

Contudo, se quanto às condutas de "introduzir" e "modificar" não se levantam grandes dúvidas [naquela, está em causa a inclusão de dados informáticos que não existiam nesse sistema informático (na aceção do art. 2.º, al. a), da Lei n.º 109/2009) e, nesta, está em causa a alteração de dados informáticos que já existiam nesse sistema informático], pela aparente sobreposição de "apagar" e "suprimir", surgirão dificuldades, que implicam – dado que o legislador goza da presunção do art. 9.º, n.º 3, do CC – que se encontre uma diferenciação entre ambas. Deste modo, consideramos que "apagar" consiste na eliminação de dados que se encontrem num sistema informático e "suprimir" consiste em reter, ocultar, tornar temporariamente indisponíveis dados que aí se encontrem[25].

E, quanto a "interferir", está em causa influenciar o modo de tratamento informático de dados, a fim de esse tratamento não ocorrer do modo como, sem a atuação do agente, ocorreria.

A Lei n.º 109/2009 não possui qualquer conceito de tratamento de dados informáticos, pelo que podemos socorrer-nos do Relatório Explicativo da Convenção sobre o Cibercrime, onde se refere que «*a expressão "tratamento de dados" significa que os dados no sistema informático são operados através da execução de um programa de computador. Um "programa de computador" é um conjunto de instruções passíveis de serem executadas pelo computador para obter o resultado*» e, desse modo, o tratamento de dados informáticos consiste na realização de operações relativas a esses dados executadas através da execução de um programa de computador (que, por sua vez, é um conjunto de instruções passíveis de serem executadas pelo computador para obter o resultado

[25] Cfr. JOEL TIMÓTEO RAMOS PEREIRA, Compêndio Jurídico da Sociedade da Informação, p. 522, e GARCIA MARQUES/LOURENÇO MARTINS, Direito da Informática, 2.ª Edição, p. 689.

pretendido). Assim, o agente vai influenciar essas operações com a finalidade de que elas sejam executadas de modo diverso daquele como seriam executadas se o agente não as influenciasse do modo como as influenciou.

Dado que a introdução, modificação, apagamento ou supressão de dados informáticos não deixam de ser formas de interferência no tratamento automático desses dados, a referência da Lei a "*ou por qualquer outra forma interferir num tratamento informático de dados*" significa que o legislador quis criar uma cláusula geral, de modo a que toda e qualquer interferência relativamente ao tratamento de dados por um sistema informático caiba nesta norma incriminatória, a fim de obstar a lacunas de punibilidade.

O legislador previu um outro elemento objetivo do tipo na primeira das condutas típicas referidas e que consiste em, por via da interferência no tratamento automático de dados informáticos, serem produzidos dados ou documentos não genuínos, sendo certo que, em face do bem jurídico protegido e do próprio elemento subjetivo especial do tipo "intenção de que estes sejam considerados ou utilizados para finalidades juridicamente relevantes", esses dados ou documentos terão de ser suscetíveis de servirem como meio de prova.

No entanto, o crime consuma-se mesmo que os documentos falsos ou contendo dados falsos não sejam impressos após a sua manipulação ilícita (como sucederá, por exemplo, nas transações bancárias, operações de contabilidade ou pagamentos) e, se a modificação dos dados incidir sobre documento já impresso ou sobre um registo em suporte digital não incorporado no computador que lhe deu origem, a conduta do agente deverá ser punida como crime de falsificação de documento p. e p. pelo art. 256.º do CP, uma vez que tais realidades são subsumíveis ao conceito de documento constante do art. 255.º, al. a), do CP[26].

A exigência de serem produzidos dados ou documentos não genuínos é facilmente compreensível, permitindo estabelecer um paralelismo entre as condutas previstas no art. 3.º, n.º 1, da Lei n.º 109/2009 e no art. 256.º, n.º 1, als. a)

[26] Cfr. GARCIA MARQUES/LOURENÇO MARTINS, Direito da Informática, 2.ª Edição, pp. 684-685.

a d), do CP (sendo que as condutas previstas no n.º 1 do art. 3.º, da Lei n.º 109/2009 corresponderão, no plano dos documentos eletrónicos às condutas das als. a) a d) do n.º 1, do art. 256.º do CP), em que se exige um resultado material (produção de um documento ou de um componente destinado a corporizá-lo, apor uma assinatura falsa, falsear o conteúdo de um documento genuíno ou de qualquer dos seus documentos), sendo que, como vimos, no crime de falsidade informática, está em causa a equiparação da adulteração dos dados informáticos ao crime de falsificação de documento "clássico" sempre que daí ocorra, quanto a um documento ou dado (eletrónicos), um efeito de adulteração similar ao que ocorre quando se adultera um documento (na aceção do art. 255.º, al. a), do CP) ou o seu conteúdo[27].

Na verdade, não podemos esquecer que foi por causa da impossibilidade ou grande dificuldade de subsumir o documento informático ao conceito de documento do art. 255.º, al. a), do CP sem infringir a proibição do recurso à analogia em matéria de normas penais positivas que o legislador criou o crime de falsidade informática[28], sendo que, como vimos, este crime tutela o mesmo bem jurídico que o crime de falsificação de documento previsto no CP. A impossibilidade ou, pelo menos, a grande dificuldade de subsumir o documento informático ao conceito de documento do art. 255.º, al. a), do CP resulta do facto de, apesar de os dados inseridos num sistema informático serem indubitavelmente a concretização de um pensamento humano (dado que os sistemas informáticos não pensam nem criam, limitando-se a, enquanto máquinas que são, trabalhar de acordo com as "ordens" que lhe são dadas pelo

[27] Cfr. PEDRO DIAS VENÂNCIO, Investigação e meios de prova na criminalidade informática, p. 12.

[28] Neste sentido, FARIA COSTA/HELENA MONIZ, "Algumas reflexões sobre a criminalidade informática em Portugal", *in* BFDUC, 1997, pp. 326 e ss, GARCIA MARQUES/LOURENÇO MARTINS, Direito da Informática, 2.ª Edição, pp. 685-686, LOPES ROCHA, "A lei da criminalidade informática (Lei n.º 109/01 de 17 de Agosto). Génese e técnica legislativa", *in* Cadernos de Ciência de Legislação, n.º 8, p. 74, e, referindo-se apenas ao crime de falsificação de documento "clássico", Relatório Explicativo da Convenção sobre o Cibercrime.
No fundo, o legislador fez, ao nível da Lei penal, aquilo que, ao nível do Direito privado, já fizera no DL n.º 290-D/99, de 2 de agosto: equiparar o documento eletrónico ao documento escrito.

respetivo operador, ainda que por via de um programa informático – que é criado por pessoas –), acabam por não conter em si qualquer declaração de vontade ou de um facto ou uma qualquer declaração humana, sendo que o crime de falsificação "clássico" pressupõe que o documento inclua uma declaração idónea a provar um facto juridicamente relevante[29].

A manipulação dos dados informáticos tanto pode ocorrer no *input* como no *output*[30], havendo que destrinçar o momento em que a manipulação é realizada e o momento em que se verificam os efeitos dessa manipulação.

Assim, se a manipulação ocorrer na fase de *input* (*i.e.* a integração dos dados informáticos no sistema informático), os programas instalados no sistema informático não são alterados, apenas trabalhando com dados falsos e, por isso, o tratamento dos dados vai gerar um resultado falso; daí que, quando o *input* é falso, o *output* também será falso por força da falsificação dos dados integrados.

E o mesmo sucederá se a manipulação ocorrer, não na fase de integração dos dados informáticos, mas na fase do seu tratamento, em que os dados ficam intactos, sendo antes os programas que são alvo de modificação fraudulenta. Aqui, o *output* é falso em virtude de os dados serem inseridos corretamente, mas serem alvo de um tratamento incorreto por via da modificação do programa.

Em ambos os casos, verificados que estejam os demais elementos do tipo, a conduta é subsumível ao crime de falsidade informática.

Diversamente, a manipulação pode ocorrer na fase de *output*, em que, tanto os dados informáticos como o seu tratamento estão corretos, sendo a manipulação efetuada já ao nível do resultado final por via da sua modificação já

[29] Cfr. FARIA COSTA/HELENA MONIZ, "Algumas reflexões sobre a criminalidade informática em Portugal", *in* BFDUC, 1997, p. 326, LOPES ROCHA, "A lei da criminalidade informática (Lei n.º 109/01 de 17 de Agosto). Génese e técnica legislativa", *in* Cadernos de Ciência de Legislação, n.º 8, p. 73, GARCIA MARQUES/LOURENÇO MARTINS, Direito da Informática, 2.ª Edição, pp. 685-686, e OLIVEIRA ASCENSÃO, "Criminalidade informática", *in* Direito da Sociedade da Informação, II, p. 221.

[30] Assim, FARIA COSTA/HELENA MONIZ, "Algumas reflexões sobre a criminalidade informática em Portugal", *in* BFDUC, 1997, pp. 324-325, JOSÉ ANTÓNIO VELOZO/LOPES ROCHA, "Criminalidade informática: modos de execução", *in* ScIvr, T. XXXV pp. 175 e ss, e JOÃO CARLOS BARBOSA DE MACEDO, "Algumas considerações acerca dos crimes informáticos em Portugal", *in* Direito Penal Hoje, pp. 237-238.

depois de impresso ou de a modificação incidir sobre um registo em suporte digital não incorporado no computador que lhe deu origem. Porém, como vimos, na medida em que os objetos da manipulação ao nível do *output* são subsumíveis ao conceito de documento constante do art. 255.º, al. a), do CP, quando a manipulação ocorre na fase de *output*, o agente comete, não o crime de falsidade informática p. e p. pelo art. 3.º da Lei n.º 109/2009, mas sim o crime de falsificação de documento p. e p. pelo art. 256.º do CP.

Ainda quanto à produção de documento ou dados não genuínos, cumpre convocar aqui a distinção entre falsidade material e falsidade ideológica, consistindo aquela na criação de um documento falso em si mesmo e esta na introdução de um conteúdo falso num documento genuíno[31], porquanto o documento ou dados que resultam da manipulação tanto podem ser em si mesmo falsos como serem genuínos, mas o seu conteúdo ser falso, tudo dependendo do modo como a manipulação foi realizada.

O crime de falsidade informática não está limitado à manipulação de dados informáticos (ou do seu tratamento) alheios, pelo que se o agente manipular os dados ou o seu tratamento no âmbito de um programa ou sistema informático seu, desde que se verifiquem os demais elementos objetivos e subjetivos do tipo, comete o crime de falsidade informática[32].

Uma das condutas que poderão ser subsumidas ao crime de falsidade informática é o *Phishing* quando a conduta do agente abranja a criação de páginas na Internet similares às de entidades legítimas (*v.g.* Bancos) com a finalidade de obter elementos bancários ou outros através da indução da vítima em erro[33].

---

[31] Cfr. HELENA MONIZ, "Art. 256º", *in* Comentário Conimbricense do Código Penal, II, p. 676.

[32] Cfr. OLIVEIRA ASCENSÃO, "Criminalidade informática", *in* Direito da Sociedade da Informação, II, p. 222.

[33] Cfr. JOÃO CARLOS BARBOSA DE MACEDO, "Algumas considerações acerca dos crimes informáticos em Portugal", *in* Direito Penal Hoje, p. 236 (nota 52).
Acerca do conceito de *Phishing*, de acordo com o Acórdão do STJ de 18/12/2013, *in www.dgsi.pt*, «*Os ataques cibernautas tornaram-se comuns, tendo surgido novas modalidades de actuações ilícitas como o phishing e o pharming, que visam essencialmente as instituições de crédito.*

Outra conduta que poderá ser subsumida ao crime de falsidade informática é o *Carding*, que consiste numa técnica de obtenção e manipulação de dados contidos na face ou nas bandas magnéticas de cartões de crédito, débito ou de comunicações eletrónicas, bem como na implementação de dados ou elementos de identificação noutros suportes técnicos. Ora, apenas e só na parte em que o *Carding* consista na manipulação de dados contidos nas bandas magnéticas de cartões de crédito, débito ou de comunicações eletrónicas,

---

O phishing (do inglês fishing «pesca») pressupõe uma fraude electrónica caracterizada por tentativas de adquirir dados pessoais, através do envio de e-mails com uma pretensa proveniência da entidade bancária do receptor, por exemplo, a pedir determinados elementos confidenciais (número de conta, número de contrato, número de cartão de contribuinte ou qualquer outra informação pessoal), por forma a que este ao abri-los e ao fornecer as informações solicitadas e/ou ao clicar em links para outras páginas ou imagens, ou ao descarregar eventuais arquivos ali contidos, poderá estar a proporcionar o furto de informações bancárias e a sua utilização subsequente, cfr Pedro Verdelho, in Phishing e outras formas de defraudação nas redes de comunicação, in Direito da Sociedade De Informação, Volume VIII, 407/419: Maria Raquel Guimarães, in Cadernos de Direito Privado, nº41, Janeiro/Março de 2013; Mark A Fox, Phishing, Pharming and Identity Theft in The Banking Industry, in Journal of international banking law and regulation, editado por Sweet and Maxwel (2006), Issue 9, 548/552; Roberto Flor, Phishing, Identity Theft e Identity Abuse. Le Prospecttive Applicative Del Diritto Penale Vigente, in Revista Italiana di Diritto e Procedura Penale, Fasc 2/3-Aprile-Settembre 2007, 899/9446.

A outra modalidade de fraude on line é o pharming a qual consiste em suplantar o sistema de resolução dos nomes de domínio para conduzir o usuário a uma pagina Web falsa, clonada da página real, cfr ibidem.

O processo baseia-se, sumariamente, em alterar o IP numérico de uma direcção no próprio navegador, através de programas que captam os códigos de pulsação do teclado (os ditos keyloggers), o que pode ser feito através da difusão de vírus via spam, o que leva o usuário a pensar que está a aceder a um determinado site – por exemplo o do seu banco – e está a entrar no IP de uma página Web falsa, sendo que ao indicar as suas chaves de acesso, estas serão depois utilizadas pelos crackers, para acederem à verdadeira página da instituição bancária e aí poderem efectuar as operações que entenderem, cfr ibidem.».

E, complementarmente, de acordo com o Acórdão da RP de 07/10/2014, *in www.dgsi.pt*, «*O phishing, numa primeira etapa, consiste na apropriação de informações de outra pessoa (como nome, informações de conta e senha bancária), para serem utilizadas fraudulentamente nas fases seguintes da trama (transferências de numerários de contas correntes e aplicações financeiras.*

O pharming é um ataque de phishing mais sofisticado sem o uso da "isca" (o e-mail com a mensagem enganosa). O vírus reescreve arquivos do PC que são utilizados para converter os endereços de Internet (URL´s) em números que formam os endereços IP (números decifráveis pelo computador.

Assim, um computador com esses arquivos comprometidos leva o internauta para o site falso, mesmo que este digite corretamente o endereço do site intencionado.

A mais sofisticada e perigosa forma de pharming é conhecida como "DNS (Domain Name System) poisoning" (traduzindo para o português, seria algo como "envenenamento do DNS"), por possibilitar um ataque em larga escala. Nessa modalidade, o ataque é dirigido a um servidor DNS, e não a um computador de um internauta isoladamente.».

estaremos perante um crime de falsidade informática, na modalidade p. e p. pelo art. 3.º, n.º 2, da Lei n.º 109/2009[34].

No que tange à segunda modalidade de conduta típica (art. 3.º, n.º 2), vale aqui o que referimos quanto à primeira conduta típica, apenas havendo que aditar alguns aspetos relativos às especificidades desta segunda conduta típica, que exige que a conduta do agente incida sobre dados informáticos que estejam registados ou incorporados em cartão bancário de pagamento ou em qualquer outro dispositivo que permita o acesso a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado.

Assim, estando em causa a especial necessidade de proteger os dados financeiros[35], caberá nesta segunda conduta típica, desde logo, a manipulação de dados informáticos registados ou incorporados, por exemplo, num cartão de débito ou crédito ou dispositivos (desde logo, computadores) que permitam o acesso a redes de pagamentos ou transferências de dinheiro como as redes Multibanco, Visa, Mastercard, American Express, Paypal, etc., ou do seu tratamento[36].

No caso de dados informáticos registados ou incorporados em dispositivo que permita o acesso a sistema de comunicações trata-se de manipular dados informáticos (ou o seu tratamento) registados ou incorporados em dispositivos que permitam aceder a uma rede de dispositivos na qual circulam informações entre um emissor e um recetor (sendo o sistema de informação o canal de transmissão dessa mensagem do emissor para o recetor), independentemente de se tratar de sistemas de comunicação por cabo ou *Wireless*, cabendo aí uma plêiade de realidades como as comunicações via satélite, telefónicas (fixas ou móveis), sistemas de distribuição de sinal de televisão por cabo, *Wired Neworks*,

[34] Contra, considerando, embora à luz da Lei n.º 109/91, que se tratará de um crime de falsificação de documento, JOEL TIMÓTEO RAMOS PEREIRA, Compêndio Jurídico da Sociedade da Informação, p. 523.
[35] Cfr. PEDRO DIAS VENÂNCIO, "O Crime de Falsidade Informática", *in* JusNet 120/2010.
[36] Cfr. PEDRO VERDELHO, "A nova Lei do Cibercrime", *in* ScIvr, T. LVIII, pp. 724-725.

etc.[37]. Assim, poderá estar em causa, por exemplo, a falsificação relativamente a cartões SIM (enquanto identificação do seu titular para efeitos de acesso a uma dada rede móvel), que, combinados com *hardware*, permitam aceder a sistemas de comunicações[38].

Quanto aos dados informáticos registados ou incorporados em dispositivo que permita o acesso a serviço de acesso condicionado, este serviço consiste em serviços que, ou não estão acessíveis ao público em geral ou, estando, implicam, por exemplo, o pagamento de uma contrapartida específica (v.*g.* monetária). Assim, por exemplo, nos termos do art. 8.º da Lei n.º 27/2007, de 30 de julho (Lei da Televisão), os serviços de programas televisivos podem ser generalistas ou temáticos e de acesso condicionado ou não condicionado e, dentro destes, de acesso não condicionado livre ou de acesso não condicionado com assinatura, sendo que são de acesso condicionado os serviços de programas televisivos disponibilizados ao público mediante contrapartida específica, não se considerando como tal a quantia devida pelo acesso à infraestrutura de distribuição, bem como pela sua utilização. Assim, poderá estar em causa, por exemplo, a falsificação relativamente a cartões SIM que, combinados com *hardware*, permitam aceder a serviços de televisão por cabo.

Ainda a respeito desta segunda conduta típica, levanta-se a questão da compatibilização do art. 3.º, n.º 2, da Lei n.º 109/2009 com o disposto nos arts. 262.º e 267.º do CP, na medida em que o legislador, no art. 267.º, n.º 1, al. c), do CP, equipara, para efeitos dos crimes p. e p. pelos arts. 262.º a 266.º do CP (interessando-nos aqui apenas o crime de contrafação de moeda p. e p. pelo art. 262.º, n.º 1, do CP), os cartões de crédito[39] à moeda, sendo que alguns autores[40] consideram que o art. 3.º, n.º 2, da Lei n.º 109/2009 veio retirar qualquer aplicação

[37] Neste sentido, PEDRO VERDELHO, "A nova Lei do Cibercrime", *in* ScIvr, T. LVIII, p. 725.
[38]Assim, PEDRO VERDELHO, "A nova Lei do Cibercrime", *in* ScIvr, T. LVIII, p. 725.
[39] Mas não os de débito, como bem referem PINTO DE ALBUQUERQUE, Comentário do Código Penal, p. 672, ALMEIDA COSTA, "Art. 267º", *in* Comentário Conimbricense do Código Penal, II, pp. 811-812, e Acórdão da RL de 10/07/2012, *in www.dgsi.pt*.
[40] Casos de PEDRO VERDELHO, "Lei n.º 109/2009, de 15 de Setembro", *in* Comentário das Leis Penais Extravagantes, I, p. 507, e DIANA VIVEIROS DE SIMAS, O Cibercrime, p. 82.

prática à remissão operada pelo art. 267.º, n.º 1, al. c), do CP, em virtude de a Lei n.º 109/2009 exigir a verificação de pressupostos que o CP não exige, ao passo que a Jurisprudência[41] vem considerando que, pela diversidade dos bens jurídicos tutelados por cada uma das incriminações, a equiparação operada no art. 267.º, n.º 1, al. c), do CP continua em vigor, não tendo perdido a razão de ser por via da entrada em vigor do art. 3.º, n.º 2, da Lei n.º 109/2009.

Pela nossa parte, entendemos que a equiparação operada no art. 267.º, n.º 1, al. c), do CP continua em vigor, não tendo perdido a razão de ser por via da entrada em vigor do art. 3.º, n.º 2, da Lei n.º 109/2009. Por várias razões.

Em primeiro lugar, ao passo que o crime de falsidade informática tutela a segurança e a fiabilidade dos documentos eletrónicos no tráfico jurídico-probatório, o crime de contrafação de moeda tutela a intangibilidade do sistema monetário, incluindo a segurança e a credibilidade do tráfego monetário[42], pelo que, ocorrendo entre os crimes de falsidade informática e de moeda falsa, como veremos, uma situação de concurso efetivo (decorrente da diversidade de bens jurídicos tutelados), a equiparação do art. 267.º, n.º 1, al. c), do CP continua em vigor em matéria de crimes de moeda falsa.

E, em segundo lugar, se atentarmos nas penas, o crime de falsidade informática na modalidade prevista no n.º 2 do art. 3.º da Lei n.º 109/2009 é punível com pena entre 1 e 5 anos, elevando-se o limite mínimo a 2 anos e mantendo-se o limite máximo se o agente for funcionário, ao passo que, no caso do crime de contrafação de moeda p. e p. pelo art. 262.º, n.º 1, do CP, a pena aplicável é de 3 a 12 anos de prisão, pelo que, visando o legislador, com a introdução da Lei n.º 109/2009, alargar o espectro da punição (*v.g.* passando a punir a contrafação de cartões de débito através da manipulação dos dados neles registados ou incorporados) e não atenuá-lo, não faz sentido entender-se que

[41] Cfr. Acórdãos da RL de 30/06/2011 e 10/07/2012 e da RP de 21/11/2012 e 17/09/2014, *in www.dgsi.pt*.

[42] Cfr. PINTO DE ALBUQUERQUE, Comentário do Código Penal, p. 685, ALMEIDA COSTA, "Antes do art. 262º", *in* Comentário Conimbricense do Código Penal, II, pp. 749 e ss, LEAL HENRIQUES/SIMAS SANTOS, Código Penal Anotado, 2.º Vol., 3.ª Edição, p. 1152, e Acórdãos da RL de 30/06/2011 e 10/07/2012 e da RP de 21/11/2012 e 17/09/2014, *in www.dgsi.pt*.

dessa introdução possa resultar uma punição menos severa no caso de contrafação, mediante a manipulação de dados nele registados ou incorporados, de um cartão de crédito.

Quanto à terceira modalidade de conduta típica (art. 3.º, n.º 3, 1.ª parte), está em causa a utilização, por qualquer modo, do documento produzido em consequência da manipulação dos dados ou do seu tratamento nos termos que referimos quanto à primeira conduta típica.

No fundo, fazendo aqui um paralelismo com o art. 256.º, n.º 1, do CP, está em causa uma conduta análoga à prevista na sua al. e), pelo que esta conduta típica consistirá, não na manipulação dos dados informáticos ou do seu tratamento de que resultará a produção de um documento ou dados não genuínos, mas na utilização desse documento.

Tal como referimos quanto à primeira conduta típica, se o uso incidir sobre documento que tenha sido impresso ou sobre um registo em suporte digital não incorporado no computador que lhe deu origem, a conduta do agente deverá ser punida como crime de falsificação de documento p. e p. pelo art. 256.º do CP, uma vez que tais realidades são subsumíveis ao conceito de documento constante do art. 255.º, al. a), do CP[43]. Assim, sempre que o agente utilize um documento que tenha sido impresso ou um registo em suporte digital não incorporado no computador que lhe deu origem, cabendo tais realidades no conceito de documento constante do art. 255.º, al. a), do CP, cometerá o crime de falsificação de documento p. e p. pelo art. 256.º do CP; e cometerá o crime de falsidade informática se a utilização incidir sobre realidades "eletrónicas" não subsumíveis ao conceito de documento constante do art. 255.º, al. a), do CP.

[43] Nesse sentido, GARCIA MARQUES/LOURENÇO MARTINS, Direito da Informática, 2.ª Edição, p. 689, afirmam que a punição da conduta hoje incriminada pelo art. 3.º, n.º 3, da Lei n.º 109/2009 «*estará privilegiadamente dirigid[a] para o uso de documento emitido por computador e já em suporte escrito. Repare-se que neste caso surge o elemento intenção de causar prejuízo a outrem ou de obter um benefício ilegítimo, para si ou para terceiros", o que aproxima o tipo da lei penal comum. Ou seja, em vez de um crime de falsidade informática, estaremos próximos de um vulgar crime de falsificação*».

Não restando dúvidas de que a utilização de documento eletrónico falso (independentemente de a falsidade ser material ou ideológica) por pessoa diversa da pessoa que manipulou dados informáticos ou o seu tratamento é punível à luz do art. 3.º, n.º 3, da Lei n.º 109/2009, levanta-se a questão de saber se, quando quem manipula os dados ou o seu tratamento e utiliza o documento falso é mesma pessoa, é punida pela prática de ambas as condutas (falsificação e utilização) ou não (existindo uma situação de concurso aparente) e, neste caso, se deverá ser punido nos termos dos n.ºs 1 ou 2 (consoante o caso) ou nos termos do n.º 3, o que será analisado infra em sede de concurso.

No que concerne à quarta modalidade de conduta típica (art. 3.º, n.º 3, 2.ª parte), está em causa a utilização de um cartão ou dispositivo subsumíveis ao n.º 2 do art. 3.º da Lei n.º 109/2009, valendo aqui *mutatis mutandis* o que referimos quanto à terceira conduta típica.

E, por fim, relativamente à quinta modalidade de conduta típica (art. 3.º, n.º 4), o legislador pretendeu incluir aqui uma panóplia de dispositivos[44] (o que incluirá *software*) utilizáveis para aceder a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado para fins de introdução, modificação, apagamento ou supressão de dados informáticos ou interferência por qualquer outra forma no tratamento informático de dados.

A inclusão do n.º 4 no art. 3.º da Lei n.º 109/2009 foi uma opção (acertada) do legislador português, dado que a CCiber não impõe uma tal criminalização, uma vez que o art. 6.º só se refere às infrações previstas nos arts. 2.º a 5.º e a criminalização da falsidade informática consta do art. 7.º.

Porém, tendo sido essa a opção do nosso legislador, não se percebe o porquê de ter restringido a punição desta conduta ao caso dos dispositivos que permitam aceder a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado para fins de introdução, modificação,

[44] De acordo com BENJAMIM SILVA RODRIGUES, Da Prova Penal, IV, p. 135, a expressão "dispositivo" deverá ser lida de forma pragmática, podendo consistir num mero programa de recuperação de *passwords*.

apagamento ou supressão de dados informáticos ou interferência por qualquer outra forma no tratamento informático de dados e não tenha punido, pura e simplesmente, os atos de importar, distribuir, vender ou detiver para fins comerciais qualquer dispositivo que permita "introduzir, modificar, apagar ou suprimir dados informáticos ou por qualquer outra forma interferir num tratamento informático de dados" em situações subsumíveis ao n.º 1 (que sempre incluiria as situações contempladas no n.º 2) do art. 3.º da Lei n.º 109/2009[45].

Entrando diretamente na redação do art. 3.º, n.º 4, da Lei n.º 109/2009, desde logo deparamos com um elemento estranho na descrição do tipo, que é a exigência de que esse dispositivo tenha sido utilizado para introdução, modificação, apagamento ou supressão de dados informáticos ou interferência por qualquer outra forma no tratamento informático de dados. A este respeito, PEDRO DIAS VENÂNCIO[46] afirma que, desse elemento típico parece resultar que o crime só se consuma se o dispositivo vier a ser usado para uma das ações previstas no n.º 2 do art. 3.º da Lei n.º 109/2009, o que, a suceder, «*contraria toda a lógica da previsão da CCiber que consagra um verdadeiro crime de perigo, em que o mesmo consuma-se sem a efectiva utilização do dispositivo, punindo-se não só a sua produção e distribuição como a mera detenção. É absolutamente ilógico, face à ratio legis subjacente a esta previsão, que a penalização da "importação, distribuição, venda ou detenção" dos referidos dispositivos fique, ela própria, dependente da efectiva utilização dos dispositivos para as "acções previstas no n.º 2". Cremos que seria intenção do legislador que fossem puníveis as condutas de detenção ou distribuição de dispositivos que fossem destinados a essas utilizações, mas sempre independente dessa sua efectiva utilização final, que é já punida nos termos do n.º 2 do mesmo artigo. Parece-nos, por isso, existir aqui um lapso de escrita do legislador que, no entanto, face ao seu elemento literal, nos deixa pouca margem para interpretações divergentes. Entendemos, por isso, que urge rectificar a previsão legal do n.º 4 deste artigo 3.º (...)*».

[45] Manifestando a mesma estranheza, PEDRO DIAS VENÂNCIO, Lei do Cibercrime, p. 40.
[46] PEDRO DIAS VENÂNCIO, Lei do Cibercrime, p. 40.

E, a ser assim, o legislador nacional teria andado muito mal ao exigir que o dispositivo "importado, distribuído, vendido ou detido para fins comerciais" e que permita o acesso a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado viesse a ser efetivamente utilizado para introdução, modificação, apagamento ou supressão de dados informáticos ou interferência por qualquer outra forma no tratamento informático de dados, o que o art. 6.º da CCiber não exige. Com efeito, não se perceberia o porquê de o legislador ter optado por uma antecipação da tutela penal através da criminalização dos atos de importar, distribuir, vender ou deter para fins comerciais dispositivos que permitam o acesso a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado e, depois, exigisse que tenha havido utilização dos mesmos para aceder a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado, pois tal contraria a *ratio* antecipatória da criminalização de tais condutas.

E convém ter presente de que o legislador goza da presunção do art. 9.º, n.º 3, do CC, razão pela qual, ao fixarmos o sentido e alcance deste art. 3.º, n.º 4, da Lei n.º 109/2009, teremos que presumir que, apesar de não ter exprimido o seu pensamento em termos adequados, o legislador consagrou a solução mais acertada, ou seja, que penalizou a importação, distribuição, venda ou detenção, para fins comerciais, de dispositivos que permitam o acesso a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado, independentemente de virem a ser utilizados para aceder a um sistema, meio de pagamento ou serviço com tais características, sendo certo que dizer "*sobre o qual tenha sido praticada qualquer das ações previstas no n.º 2*" não é a mesma coisa que dizer, por exemplo, "*desde que esse dispositivo venha a ser utilizado para praticar qualquer das ações previstas no n.º 2*" e, se fosse intenção do legislador exigir que haja utilização desse dispositivo para aceder a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado, teria certamente optado por uma redação como a que referimos ou idêntica, da qual, ao contrário do que sucede com a redação utilizada, resultaria inequivocamente a

exigência da utilização do dispositivo para aceder a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado.

Daí que, na nossa opinião, a leitura mais correta deste n.º 4 seja no sentido de serem punidos os atos de importar, distribuir, vender ou deter para fins comerciais dispositivos que permitam o acesso a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado sem se exigir que tenham sido ou venham a ser efetivamente utilizados para aceder a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado[47].

Relativamente aos dispositivos incluídos no art. 3.º, n.º 4, da Lei n.º 109/2009, PEDRO VERDELHO/ROGÉRIO BRAVO/MANUEL LOPES ROCHA[48] entendem, com razão, que o art. 6.º da CCiber, só inclui os dispositivos concebidos exclusiva ou especificamente para a prática de infrações, não cabendo nesse preceito os dispositivos de utilização dupla (*i.e.* os que, não sendo exclusiva ou especificamente concebidos para a prática de infrações, poderão ser utilizados para essa finalidade, sendo que, de acordo com o Relatório Explicativo da Convenção sobre o Cibercrime, essa foi uma discussão que surgiu no âmbito da elaboração da CCiber, tendo os relatores optado por limitar o art. 6.º da CCiber aos dispositivos concebidos exclusiva ou especificamente para a prática de infrações.

No entanto, entendemos que tal não significa que a Lei portuguesa não possa ter ido mais longe do que a CCiber, sendo que a redação do art. 3.º, n.º 4, da Lei n.º 109/2009 não é coincidente com a do art. 6.º, n.º 1, al. a), i), da CCiber, porquanto, neste preceito fala-se em "*dispositivo (…) concebido ou adaptado antes de mais para permitir a prática de uma das infrações (…)*"[49] e o legislador

[47] Como fazem, embora sem se referirem a esta problemática, PEDRO VERDELHO, "Lei n.º 109/2009, de 15 de Setembro", *in* Comentário das Leis Penais Extravagantes, I, p. 507, e BENJAMIM SILVA RODRIGUES, Da Prova Penal, IV, p. 136.

[48] PEDRO VERDELHO/ROGÉRIO BRAVO/MANUEL LOPES ROCHA, Leis do Cibercrime, I, p. 35.

[49] Sendo que, de acordo com o que resulta do Relatório Explicativo da Convenção sobre o Cibercrime, a "adaptação" terá de levar a que o dispositivo, por via dessa adaptação, apenas possa

português não opera qualquer distinção entre "dispositivos concebidos exclusiva ou especificamente para permitir o acesso a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado" e "dispositivos que, não tendo sido concebidos exclusiva ou especificamente para permitir o acesso a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado, ainda assim possa ser utilizados também para essa finalidade".

E, atenta a *ratio* do art. 3.º, n.º 4, da Lei n.º 109/2009, não se perceberia o porquê de uma tal distinção, dado que ambos os tipos de dispositivos acabam por permitir o acesso a sistemas ou meios de pagamento, a sistemas de comunicações ou a serviços de acesso condicionado, gerando desse modo um especial perigo para o bem jurídico tutelado pela incriminação que justifica uma tal antecipação da tutela penal.

Ademais, se, no art. 276.º do CP, o legislador apenas incrimina a importação, o fabrico, a guarda, a compra, a venda, a cedência ou a aquisição a qualquer título, o transporte, a distribuição e a detenção de "*instrumento ou aparelhagem <u>especificamente</u> destinados à montagem de escuta telefónica ou à violação de correspondência ou de telecomunicações*", caso pretendesse restringir o art. 3.º, n.º 4, da Lei n.º 109/2009 dispositivos concebidos exclusiva ou especificamente para permitir o acesso a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado, tê-lo-ia feito, adotando uma formulação análoga à que adotou no art. 276.º do CP.

Já, no caso do art. 104.º da Lei n.º 5/2004, de 10 de fevereiro, se atentarmos na definição de "dispositivo ilícito" constante da al. a) do n.º 2 desse preceito, o legislador inclui nesse conceito, quer os equipamentos ou programas informáticos concebidos para permitir o acesso a um serviço protegido, sob forma inteligível, sem autorização do prestador do serviço quer os que foram adaptados para esse fim; ou seja, numa disposição "paralela", o legislador optou

ser usado para a prática de crimes, excluindo-se a utilizabilidade dupla após essa adaptação) e, na lei portuguesa, fala-se em "*dispositivo que permita o acesso a sistema (...).*

por incluir dispositivos que não foram concebidos para esse fim, mas que foram adaptados para tal, não exigindo que tais dispositivos, por via da adaptação, apenas possam ser usados para aceder a um serviço protegido, sob forma inteligível, sem autorização do prestador do serviço, mas apenas que tenham sido alvo de adaptação.

Daí que, por aplicação do princípio *ubi lex non distinguit nec nos distinguere debemus*, consideremos que o art. 3.º, n.º 4, da Lei n.º 109/2009 pune a importação, distribuição, venda ou detenção para fins comerciais de dispositivos que permitam o acesso a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado, independentemente de se tratar de dispositivos concebidos exclusiva ou especificamente para permitir o acesso a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado ou de dispositivos que, não tendo sido concebidos exclusiva ou especificamente para permitir o acesso a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado, ainda assim possa ser utilizados também para essa finalidade.

No entanto, se no caso dos "dispositivos concebidos exclusiva ou especificamente para permitir o acesso a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado", bastará a prova da importação, distribuição, venda ou detenção de tais dispositivos para fins comerciais, no caso dos "dispositivos que, não tendo sido concebidos exclusiva ou especificamente para permitir o acesso a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado, ainda assim possa ser utilizados também para essa finalidade", haverá que provar igualmente que os dispositivos importados, distribuídos, vendidos ou detidos pelo agente para fins comerciais se destinam a ser utilizados para aceder a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado (o que, reconhecemos, na prática, poderá ser quase impossível de demonstrar, embora não possa servir como fundamento para limitar o âmbito da punição do art. 3.º, n.º 4, da Lei n.º 109/2009 do modo que temos vindo a criticar).

De acordo com o art. 3.º, n.º 4, da Lei n.º 109/2009, a conduta do agente pode revestir uma das seguintes formas: (1) importar, (2) distribuir, (3) vender ou (4) deter para fins comerciais (o que exclui a detenção para uso pessoal). No entanto, tal como sucede, por exemplo com o crime de tráfico de estupefacientes, p. e p. pelo art. 21.º do DL n.º 15/93, de 22 de janeiro, teria sido preferível a opção por um elenco de condutas mais alargado ou então utilizar a fórmula constante do art. 6.º da CCiber[50] ou reproduzir a formulação utilizada no art. 276.º do CP[51] ou adotar uma solução análoga à adotada no art. 104.º da Lei n.º 5/2004, de 10 de fevereiro[52].

No entanto, cumpre referir que, de acordo com o n.º 3 do art. 104.º da Lei n.º 5/2004, apenas a conduta prevista na al. a) do n.º 1 constitui crime, sendo que a conduta prevista na al. d) constitui contraordenação grave (cfr. art. 113.º, n.º 2, al. ll)) e as condutas previstas nas als. b) e c) constituem contraordenação muito grave (cfr. art. 113.º, n.º 3, al. zz)).

---

[50] «*Quem produzir, vender, adquirir para efeitos de utilização, importar, distribuir disponibilizar de qualquer outra forma ou deter, para fins comerciais, dispositivo que permita o acesso a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado*».

[51] «*Quem importar, fabricar, guardar, comprar, vender, ceder ou adquirir a qualquer título, transportar, distribuir ou detiver para fins comerciais, dispositivo que permita o acesso a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado.*».

[52] «*1 - São proibidas as seguintes atividades:*

a) Fabrico, importação, distribuição, venda, locação ou detenção, para fins comerciais, de dispositivos ilícitos;

b) Instalação, manutenção ou substituição, para fins comerciais, de dispositivos ilícitos;

c) Utilização de comunicações comerciais para a promoção de dispositivos ilícitos;

d) Aquisição, utilização, propriedade ou mera detenção, a qualquer título, de dispositivos ilícitos para fins privados do adquirente, do utilizador, do proprietário ou do detentor, bem como de terceiro.

2 - Para efeitos do disposto no número anterior, entende-se por:

a) «Dispositivo ilícito» um equipamento ou programa informático concebido ou adaptado com vista a permitir o acesso a um serviço protegido, sob forma inteligível, sem autorização do prestador do serviço;

b) «Dispositivo de acesso condicional» um equipamento ou programa informático concebido ou adaptado com vista a permitir o acesso, sob forma inteligível, a um serviço protegido;

c) *«Serviço protegido» qualquer serviço de programas televisivo, de rádio ou da sociedade da informação desde que prestado mediante remuneração e com base em acesso condicional ou o fornecimento de acesso condicional aos referidos serviços considerado como um serviço em si mesmo. (...)*».

O legislador também poderia não ter restringido a punição dos casos de detenção à detenção para fins comerciais, dado que, estando-se no âmbito de uma antecipação da tutela penal, a detenção, pelo agente, de tais dispositivos, sobretudo no caso de dispositivos concebidos exclusiva ou especificamente para permitir o acesso a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado, também se verifica o perigo para o bem jurídico que justifica a antecipação da tutela penal para as demais condutas descritas, *maxime* a detenção para fins comerciais. E, de resto, uma tal restrição aos "fins comerciais" nem sequer consta do art. 6.º da CCiber e, no art. 276.º do CP, no caso de dispositivos que permitam a montagem de escuta telefónica ou a violação de correspondência ou de telecomunicações, basta a detenção de tais dispositivos, não se exigindo que essa detenção seja para fins comerciais.

No entanto, no caso do crime de dispositivos ilícitos p. e p. pelo art. 104.º, n.º 1, al. a), da Lei n.º 5/2004, o legislador apenas pune, como crime, a detenção para fins comerciais, punindo a detenção para uso pessoal do detentor ou outros fins que não sejam de cariz comercial como contraordenação (cfr. art. 104.º, n.º 1, al. d), conjugado com o art. 113.º, n.º 2, al. jj), ambos da Lei n.º 5/2004), solução que se nos afigura mais curial do que a solução adotada em sede de Lei n.º 109/2009, dado que a detenção para fins "não comerciais" de dispositivos ilícitos (na aceção do art. 104.º, n.º 2, al. a), da Lei n.º 5/2004), que, tal como a detenção para fins comerciais, representa um perigo para as condições de concorrência sã e transparente no mercado dos serviços que se baseiem ou consistam num acesso condicional, que passa pela defesa dos interesses patrimoniais dos exploradores desses serviços e direitos de autor e conexos[53], ainda assim acaba por ser punida (embora não como crime)

De notar que entendemos que a expressão "para fins comerciais" apenas se refere à detenção e não às demais modalidades da conduta, caso contrário, por

[53] Que, como referem PEDRO VERDELHO, "Lei n.º 5/2004, de 10 de Fevereiro", *in* Comentário das Leis Penais Extravagantes, I, p. 466, e os Acórdãos da RL de 15/12/2009 e 22/03/2011, *in www.dgsi.pt*, é o bem jurídico protegido pelo crime e pela contraordenação de dispositivos ilícitos.

exemplo no caso da venda, apenas se puniria a "venda para revenda" ou situações análogas e não a venda direta ao consumidor final do dispositivo para uso pessoal deste.

Quanto ao que se deve entender por "importar", "distribuir", "vender" e "deter" recorrendo uma vez mais ao Dicionário Houaiss da Língua Portuguesa,

a) "importar" significa «*trazer de fora (esp. de fora do país, mas também de outro estado ou município)*»;
b) "distribuir" significa «*entregar uma parcela (de algo) a diversos receptores; repartir, dividir; doar (bens, donativos, presentes, etc.) a várias pessoas, entidades, etc; enviar para diferentes direcções; espalhar; dispor espacialmente; encarregar-se da distribuição comercial de (determinado produto ou serviço)*»;
c) "vender" significa «*transferir (bem ou mercadoria) para outrem em troca de dinheiro*»; e
d) "deter" significa «*conservar em seu poder; reter*».

Mas também encontramos, no plano jurídico, alguns conceitos que nos poderão guiar na nossa tarefa. Assim, quanto ao conceito de "distribuir", surge-nos, desde logo, no âmbito do Direito Comercial, a figura dos contratos de distribuição comercial, que, de acordo com PUPO CORREIA[54], consistem nos diversos tipos contratuais de que os produtores de bens económicos se servem para fazer chegar esses bens ao seu consumidor final.

Relativamente ao conceito de "vender", encontramos no art. 874.º do CC uma definição de contrato de compra e venda: «*o contrato pelo qual se transmite a propriedade de uma coisa, ou outro direito, mediante um preço.*».

E, relativamente ao crime de substâncias explosivas ou análogas e armas, p. e p. pelo art. 275.º do CP na versão anterior à introduzida pela Lei n.º 59/2007, de 4 de setembro, de acordo com PAULA RIBEIRO DE FARIA[55]:

[54] PUPO CORREIA, Direito Comercial, 9.ª Edição, pp. 485-486.
[55] PAULA RIBEIRO DE FARIA, "Art. 275º", *in* Comentário Conimbricense do Código Penal, II, pp. 895 e ss, que, em "Art. 276º", *in* Comentário Conimbricense do Código Penal, II, p. 907, remete a

a) No que tange à "importação", «*A importação terá necessariamente um âmbito mais restrito que a introdução no país, pressupondo uma actividade comercial, e excluindo o mero ingresso no território nacional sem carácter de permanência*»;
b) Quanto à "venda", «*A venda é o acto jurídico pelo qual um sujeito transmite a outro a propriedade de uma coisa, ou outro direito, mediante um preço, sendo irrelevante a forma como em concreto se processa o acto de venda*»;
c) No que concerne à "distribuição", «*Distribuição é o acto de natureza económica pelo qual alguém lança nos circuitos comerciais um determinado produto com o objectivo de o fazer chegar aos consumidores finais*»; e
d) No que diz respeito à "detenção", «*Detenção corresponde à posse precária (art. 1253º do CC). Procura-se aqui abranger a simples disponibilidade da arma*».

Deste modo, "importar", para efeitos da incriminação do art. 3.º, n.º 4, da Lei n.º 109/2009, significará adquirir, em país estrangeiro, um dispositivo que permita aceder a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado e, após a aquisição, introduzi-lo com caráter de permanência no território nacional.

Quanto ao conceito de "vender", tratar-se-á de ceder a um terceiro (seja em Portugal seja por via de exportação para um país estrangeiro), mediante o pagamento de uma contrapartida monetária, um dispositivo que permita aceder a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado.

Relativamente ao conceito de "distribuir", consistirá na disponibilização a terceiros, por forma diversa da venda e, independentemente, de o ser a título oneroso (*v.g.*: troca, dação em cumprimento, aluguer) ou gratuito (*v.g.* doação,

determinação dos conceitos idênticos utilizados pelo legislador no crime de Instrumentos de escuta telefónica para o que referiu em sede de anotação ao art. 275.º do CP.

empréstimo) ou a título definitivo (*v.g.* troca, doação) ou temporário (*v.g.* aluguer, empréstimo), de um dispositivo que permita aceder a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado.

Por fim, no que tange à "detenção para fins comerciais", estarão em causa as situações em que o agente tem na sua posse um dispositivo que permita aceder a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado com a finalidade de, cedendo-o a terceiros, obter lucro.

No entanto, como referimos, o elenco de condutas é demasiado restritivo, deixando de fora do âmbito da punição, desde logo, a conduta de produzir dispositivos que permitam aceder a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado, sendo que, por tal constituir uma clara ultrapassagem do sentido normal das palavras utilizadas pelo legislador, não se mostra possível subsumir uma tal conduta a alguma das condutas referidas pelo legislador, sob pena de violação da proibição constitucional e legal do recurso à analogia em sede de normas penais positivas (cfr. arts. 29.º, n.ºs 1 e 3, da CRP e 1.º, n.º 3, do CP).

Por isso mesmo, estamos perante uma situação que, na nossa opinião, reclama uma intervenção urgente do legislador. Com efeito, ainda que a produção de dispositivos que permitam aceder a sistema de comunicações ou a serviço de acesso condicionado seja punível nos termos do art. 104.º, n.º 1, al. a), da Lei n.º 5/2004 (dado que o conceito de "serviço protegido" constante do n.º 2, al. c), desse preceito, inclui claramente os sistemas de comunicações e os serviços de acesso condicionado), a pena aplicável é de prisão de 1 mês a 3 anos ou multa de 10 a 360 dias (cfr. art. 104.º, n.º 3, da Lei n.º 5/2004, conjugado com os arts. 41.º, n.º 1, e 47.º, n.º 1, do CP), a qual é bastante inferior à pena aplicável ao crime de falsidade informática p. e p. pelo art. 3.º, n.º 4, da Lei n.º 109/2009; mas, mais grave ainda, a produção de dispositivos que permitam aceder a sistema ou meio de pagamento estão fora da previsão do art. 104.º, n.º 1, al. a), da Lei n.º 5/2004 e, por isso, a sua produção não é punível (o que configura uma inaceitável lacuna de

punição, uma vez que possui, no mínimo, a mesma gravidade que as condutas descritas no art. 3.º, n.º 4, da Lei n.º 109/2009).

4.2. O tipo subjetivo. Os elementos subjetivos especiais do tipo.

O crime de falsidade informática apenas poderá ser cometido dolosamente, não sendo puníveis condutas meramente negligentes (cfr. art. 3.º da Lei n.º 109/2009, conjugado com o art. 13.º do CP), podendo a conduta do agente revestir qualquer das modalidades de dolo previstas no art. 14.º do CP (direto, necessário ou eventual).

No entanto, à exceção da conduta prevista no n.º 4, o legislador exige, para além do dolo relativamente aos elementos objetivos do tipo, a verificação de elementos subjetivos especiais.

Deste modo, no caso da conduta dos n.ºs 1 e 2, exige-se, para além do dolo relativamente aos elementos objetivos do tipo, que o agente manipule os dados informáticos e, em consequência disso, produza documentos ou dados não genuínos com a intenção de que sejam considerados ou utilizados para finalidades juridicamente relevantes e, desse modo, causar engano nas relações jurídicas.

Já, no caso da conduta do n.º 3, exige-se, para além do dolo relativamente aos elementos objetivos do tipo, que o agente utilize o documento com a intenção de causar um prejuízo a outrem ou de obter um benefício ilegítimo. Estamos, pois, no caso dos n.ºs 1 a 3, perante um crime de resultado cortado ou *Absichtsdelikt* (na designação germânica), sendo que os crimes de resultado cortado consistem nos crimes em que o tipo legal exige, para além do dolo do tipo, a intenção de produção de um resultado que não integra o tipo de ilícito[56].

Começando pela intenção de que os documentos ou dados não genuínos sejam considerados ou utilizados para finalidades juridicamente relevantes e, desse modo, causar engano nas relações jurídicas, apesar da redação da Lei (em

[56] Cfr. FIGUEIREDO DIAS, Direito Penal, Parte Geral, I, 2.ª Edição, pp. 380-381.

que as duas intenções do agente surgem separadas, acabando por se reconduzir uma delas – a de causar engano nas relações jurídicas – à conduta de manipulação dos dados ou do seu tratamento e a outra – a de que os documentos ou dados não genuínos sejam considerados ou utilizados para finalidades juridicamente relevantes – ao resultado dessa manipulação), consideramos que se trata de "duas intenções" que se podem resumir a apenas "uma intenção", que é a de que os documentos ou dados não genuínos sejam considerados ou utilizados para finalidades juridicamente relevantes, surgindo a intenção de causar engano nas relações jurídicas como consequência óbvia e forçosa, uma vez que a única consequência de os documentos ou dados não genuínos serem considerados ou utilizados para finalidades juridicamente relevantes é a causação de engano nas relações jurídicas.

Deste modo, a intenção de que os documentos ou dados não genuínos sejam considerados ou utilizados para finalidades juridicamente relevantes e, desse modo, causar engano nas relações jurídicas consiste em o agente, ao manipular os dados informáticos ou o seu tratamento, ter de atuar com a intenção de os documentos ou dados não genuínos que resultarão dessa manipulação virem a ser considerados ou utilizados para finalidades juridicamente relevantes e, desse modo, causar engano nas relações jurídicas (por assentarem em documentos ou dados falsos).

Quanto à intenção de causar um prejuízo a outrem ou de obter um benefício ilegítimo (no caso da utilização), consiste em o agente, ao utilizar os documentos, agir com intenção de, por via dessa utilização, causar um prejuízo, que pode ser patrimonial (*v.g.* levar à realização de um pagamento indevido) ou não patrimonial (*v.g.* prejudicar o bom nome) a outra pessoa (física ou jurídica) ou obter (para si ou para outra pessoa, física ou jurídica) um benefício a que não tem direito, podendo esse benefício ser patrimonial (*v.g.* receber uma quantia em dinheiro a que não tenha direito) ou não patrimonial (*v.g.* casar com uma pessoa com a qual não poderia casar por existência de um impedimento legal) ou consistir num ganho (*v.g.* receber uma quantia em dinheiro a que não tenha

direito) ou na evitação de uma perda (*v.g.* evitar que um determinado bem seja penhorado para pagamento de uma dívida pela qual o património do beneficiado pelo uso do documento teria de responder).

De todo o modo, na medida em que a consideração e/ou utilização dos documentos ou dados não genuínos para finalidades juridicamente relevantes e o consequente engano nas relações jurídicas e a causação de um prejuízo a outrem ou a obtenção de um benefício ilegítimo não integram o tipo objetivo, bastará que o agente atue com essa intenção, não tendo de ocorrer uma efetiva e concreta consideração e/ou utilização dos documentos ou dados não genuínos para finalidades juridicamente relevantes e o consequente engano nas relações jurídicas nem causação de um prejuízo a outrem ou obtenção de um benefício ilegítimo. De todo o modo, se tal suceder, trata-se de uma circunstância (agravante) que deverá ser considerada em sede de determinação da medida concreta da pena (cfr. art. 71.º, n.º 2, do CP).

5. O crime de falsidade informática qualificada.

No caso da conduta prevista no n.º 5 do art. 3.º da Lei n.º 109/2009, estamos perante uma circunstância modificativa agravante consistente na qualidade do agente, que terá de ser funcionário, tratando-se, por isso, nesta parte, de um crime específico impróprio.

Não contendo a Lei n.º 109/2009 um conceito de funcionário, haverá que recorrer ao conceito de funcionário previsto no CP, pelo que este art. 3.º, n.º 5, da Lei n.º 109/2009 deverá ser conjugado com o art. 386.º do CP. Contudo, essa conjugação apenas deverá ocorrer relativamente aos n.ºs 1 e 2 do art. 386.º do CP, dado que as pessoas referidas no n.º 3 apenas são consideradas funcionário para efeitos dos crimes p. e p. pelos arts. 372.º a 374.º do CP.

Deste modo, sempre que o agente do crime seja funcionário civil, agente administrativo, árbitro, jurado, perito, desempenhe (provisória ou temporariamente, mediante remuneração ou a título gratuito, voluntária ou obrigatoriamente) uma atividade compreendida na função pública administrativa

ou jurisdicional, exerça funções ou participe em organismos de utilidade pública ou seja gestor, titular dos órgãos de fiscalização ou trabalhador de empresas públicas, nacionalizadas, de capitais públicos ou com participação maioritária de capital público e ainda de empresas concessionárias de serviços públicos e praticar qualquer uma das condutas prevista nos n.ºs 1 a 4 do art. 3.º da Lei n.º 109/2009, comete o crime previsto no n.º 5 desta Lei.

Porém, não basta que o agente seja funcionário, sendo necessário que o crime seja cometido no exercício das suas funções.

No que tange ao tipo subjetivo, o agente também apenas poderá ser punido a título de dolo, podendo a sua conduta revestir qualquer das modalidades de dolo previstas no art. 14.º do CP (direto, necessário ou eventual). E, relativamente aos elementos subjetivos especiais do tipo, tudo dependerá da conduta concretamente assumida pelo agente, valendo aqui o que referimos quanto às condutas dos n.ºs 1 a 4, que se aplicará à conduta que tiver sido assumida pelo agente *in concreto*.

6. Exclusão da ilicitude. Exclusão da culpa. Exclusão da punibilidade.

Na medida em que, para que o agente seja punido pela prática deste crime, terá de praticar um facto típico, ilícito e culposo (e punível), para além do preenchimento dos elementos objetivos e subjetivos do tipo, não poderão verificar-se os pressupostos de qualquer causa de exclusão da ilicitude, da culpa e da punibilidade.

Contudo, uma vez que esta incriminação tutela um bem jurídico supraindividual, à semelhança do que sucede com o crime de falsificação de documento p. e p. pelo art. 256.º do CP, aplicam-se relativamente ao crime de falsidade informática as regras gerais das causas de justificação e de exclusão da culpa da Parte Geral do CP em tudo o que se refiram a tipos de crime que tutelem bens jurídicos que não sejam de cariz eminentemente pessoal.

7. Condições de procedibilidade.

Não é necessária a apresentação de queixa quanto a nenhuma das condutas incriminadas neste preceito, bastando que o MP tenha conhecimento do conhecimento da infração para, a abrigo dos ditames do princípio da oficialidade, instaurar o competente inquérito, nos termos dos arts. 241.º e 262.º, n.º 2, do CPP.

8. Autoria e participação.

Não existem especificidades a este nível, podendo qualquer das condutas previstas no art. 3.º da Lei n.º 109/2009 ser cometidas a título de autoria material, autoria mediata, coautoria, instigação ou cumplicidade (moral ou material) nos termos gerais dos arts. 26.º e 27.º do CP, sendo ainda aplicável o disposto no art. 28.º do CP quanto ao crime de falsidade informática na forma qualificada, p. e p. pelo n.º 5 do art. 3.º da Lei n.º 109/2009.

9. Punibilidade da tentativa.

Atentas as molduras penais previstas no art. 3.º da Lei n.º 109/2009 e o disposto no art. 23.º, n.º 1, do CP, a tentativa é sempre punível, aplicando-se o disposto nos arts. 24.º e 25.º do CP em matéria de desistência e no art. 22.º do CP quanto ao conceito de tentativa e de atos de execução.

10. Penas aplicáveis.

Relativamente às condutas previstas no n.º 1 e no n.º 3, 1.ª parte, a pena aplicável é de prisão até 5 anos (o que, nos termos do art. 41.º, n.º 1, do CP, significa que o limite mínimo é de 1 mês e o máximo de 5 anos) ou de multa entre 120 e 600 dias, sendo que a opção pela pena de prisão ou pela pena de multa deverá nortear-se pelo disposto no art. 70.º do CP, ou seja, só se deverá optar pela pena de prisão se a pena de multa não permitir prosseguir suficientemente as finalidades de prevenção especial e de prevenção geral no caso concreto.

No caso das condutas previstas no n.º 2, no n.º 3, 2.ª parte, e no n.º 4, a pena aplicável é apenas de prisão (sem prejuízo da aplicação de uma das penas substitutivas da pena de prisão previstas no CP) entre 1 e 5 anos, o que representa um agravamento da pena aplicável, que se ficará a dever a uma intenção do legislador no sentido de tutelar mais intensamente a manipulação deste tipo de dados ou do seu tratamento[57].

No caso do n.º 5, por força da qualidade do agente, a pena aplicável é apenas de prisão, devendo ser fixada entre 2 e 5 anos, resultando esse agravamento da qualidade do agente que, ao cometer o crime no exercício das suas funções, está a incumprir igualmente os deveres especiais que sobre si recaem em razão desse exercício.

Por fim, no que tange ao crime na forma tentada, nos termos do art. 23.º, n.º 2, conjugado com os arts. 41.º, n.º 1, 47.º, n.º 1, e 73.º, n.º 1, ambos do CP, a pena de prisão aplicável será entre 1 mês e 3 anos e 4 meses, ao passo que, no caso das condutas previstas no n.º 1 e no n.º 3, 1.ª parte, a pena de multa aplicável será entre 10 e 400 dias de multa.

De referir, por último, que estas molduras penais observam a imposição constante do art. 6.º, n.º 2, da Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de fevereiro, bem como, atualmente, do art. 9.º, n.º 3, da Diretiva n.º 2013/40/UE do Parlamento Europeu e do Conselho, de 12 de agosto de 2013.

11. Prazo prescricional.

De acordo com o disposto no art. 118.º, n.ºs 1, al. b), 3 e 4, do CP, o procedimento criminal relativamente a qualquer das condutas incluídas no art. 3.º da Lei n.º 109/2009 (incluindo na sua forma qualificada), salvo se se tratar de crime na forma tentada, prescreve no prazo de 10 anos, o qual se inicia nos termos gerais previstos no art. 119.º do CP, sendo tal prazo passível de suspensão e interrupção nos termos dos arts. 120.º e 121.º do CP.

[57] Cfr. DIANA VIVEIROS DE SIMAS, O Cibercrime, p. 82.

No caso de interrupção da prescrição e salvaguardado o tempo de suspensão, a prescrição tem obrigatoriamente lugar sempre que tenham decorrido 15 anos desde o início da contagem do prazo prescricional, ressalvado o prazo de suspensão.

No caso de condutas na forma tentada, de acordo com o disposto no art. 118.º, n.ºs 1, al. c), 3 e 4, do CP, o procedimento criminal relativamente a qualquer das condutas incluídas no art. 3.º da Lei n.º 109/2009 (incluindo na sua forma qualificada), prescreve no prazo de 5 anos, o qual se inicia nos termos gerais previstos no art. 119.º do CP, sendo tal prazo passível de suspensão e interrupção nos termos dos arts. 120.º e 121.º do CP.

No caso de interrupção da prescrição e salvaguardado o tempo de suspensão, a prescrição tem obrigatoriamente lugar sempre que tenham decorrido 7 anos e 6 meses desde o início da contagem do prazo prescricional, ressalvado o prazo de suspensão.

12. O concurso de crimes.

Uma primeira possibilidade de concurso ocorre entre as condutas subsumíveis aos n.ºs 1 e 3, 1.ª parte, ou entre as condutas subsumíveis aos n.ºs 2 e 3, 2.ª parte, do art. 3.º da Lei n.º 109/2009, *i. e.*, no caso em que o mesmo agente manipule dados informáticos e depois utilize os dados ou documento resultantes dessa manipulação. Em tais casos, consideramos que existe concurso aparente[58], devendo operar-se um paralelismo com o entendimento da Doutrina maioritária no que tange ao crime de falsificação de documento "clássico" (no sentido de que a conduta de falsificação do documento consome a conduta de uso do documento)[59].

[58] No mesmo sentido, BENJAMIM SILVA RODRIGUES, Da Prova Penal, IV, p. 135.

[59] Cfr. EDUARDO CORREIA, A Teoria do Concurso em Direito Penal, Reimpressão, p. 138, PINTO DE ALBUQUERQUE, Comentário do Código Penal, p. 675, LEAL HENRIQUES/SIMAS SANTOS, Código Penal Anotado, 2.º Vol., 3.ª Edição, p. 1102, e HELENA MONIZ, "Art. 256º", *in* Comentário Conimbricense do Código Penal, II, p. 684).

Com efeito, estando consumado o crime na modalidade de manipulação dos dados informáticos ou do seu tratamento (n.º 1 ou n.º 2, consoante os casos), não faz sentido desconsiderar essa consumação (que, como é óbvio, ocorre em momento anterior ao da utilização) para se punir o agente pela utilização (que consumiria a manipulação anteriormente ocorrida). No fundo, como refere EDUARDO CORREIA[60], «*a eficácia destas disposições* [as disposições que punem abstratamente um perigo de lesão ou uma lesão, como se ela efetivamente se tivesse consumado, independentemente da averiguação da existência de um perigo efetivo de lesão ou de uma lesão no caso concreto] *consome naturalmente a daquelas que visam punir a verificação efectiva e concreta desse perigo ou dessa lesão de bens jurídicos*».

De todo o modo, se, para além de manipular os dados informáticos e o seu tratamento e de, desse modo, produzir documentos ou dados não genuínos, o agente ainda fizer uso dos mesmos, cometerá o crime de falsidade informática na na modalidade de manipulação dos dados informáticos ou do seu tratamento (n.º 1 ou n.º 2, consoante os casos), funcionando a utilização como circunstância (agravante) que deverá ser considerada em sede de determinação da medida concreta da pena (cfr. art. 71.º, n.º 2, do CP).

Outra possibilidade de concurso ocorre entre o crime de falsidade informática e o crime de falsificação de documento p. e p. pelo art. 256.º do CP, porquanto, como referem GARCIA MARQUES/LOURENÇO MARTINS[61], em face do conceito de documento constante do art. 255.º, al. a), do CP, não são de excluir relações de consunção entre ambos os tipos legais.

Entre os crimes de falsidade informática (no que tange à conduta prevista no n.º 4 do art. 3.º da Lei n.º 109/2009) e de instrumentos de escuta telefónica (p. e p. pelo art. 276.º do CP) e começando a nossa análise pelos demais casos referidos no art. 276.º do CP que não a violação de telecomunicações, por força da diversidade de bens jurídicos tutelados e de, salvo no caso da violação de

[60] EDUARDO CORREIA, A Teoria do Concurso em Direito Penal, Reimpressão, p. 138.
[61] GARCIA MARQUES/LOURENÇO MARTINS, Direito da Informática, 2.ª Edição, p. 690.

telecomunicações[62], inexistir sobreposição de condutas[63], existe uma relação de concurso efetivo.

E, no caso em que estamos perante um dispositivo que permite aceder a um sistema de comunicações e, concomitantemente, devassar telecomunicações, dado que cada uma das incriminações tutela bens jurídicos completamente diversos (posto que a segurança e a fiabilidade dos documentos no tráfico jurídico-probatório nada tem a ver com a intimidade/privacidade nem com a inviolabilidade das comunicações privadas), estaremos perante um concurso efetivo de crimes, na modalidade de concurso ideal.

Porém, na medida em que o elenco de modalidades da conduta é mais abrangente no art. 276.º do CP do que no art. 3.º, n.º 4, da Lei n.º 109/2009, nos casos em que a modalidade da conduta concretamente adotada apenas esteja prevista no art. 276.º do CP, o agente apenas será punido pela prática deste crime. Do mesmo modo, no caso de dispositivos que, não sendo especificamente destinados a aceder a um sistema de comunicações e a devassar telecomunicações, ainda assim permitam esse acesso, atenta a restrição do art. 276.º apenas aos dispositivos que se destinem especificamente a esse fim, o agente apenas será punido pela prática do crime de falsidade informática p. e p. pelo art. 3.º, n.º 4, da Lei n.º 109/2009.

Entre os crimes de falsidade informática e de contrafação de moeda (mediante o fabrico de cartão de crédito falso) existe uma relação de concurso efetivo, atenta a diversidade de bens jurídicos tutelados por ambas as incriminações[64].

No que tange aos vários tipos de crime de burla e começando pelo crime de burla informática e nas comunicações, entre os crimes de falsidade informática e de burla informática e nas comunicações existe uma relação de

[62] Que podem ser devassadas mediante o uso de um dispositivo que permita o acesso a sistema de comunicações

[63] Pois os dispositivos mencionados no art. 276.º do CP, pelo menos à partida, nada têm a ver com os dispositivos mencionados no art. 3.º, n.º 4, da Lei n.º 109/2009.

[64] Cfr. Acórdãos da RL de 30/06/2011 e 10/07/2012 e da RP de 21/11/2012 e 17/09/2014, *in www.dgsi.pt*.

concurso efetivo, atenta a diversidade de bens jurídicos tutelados por ambas as incriminações, ainda que o crime de falsidade informática seja cometido enquanto crime-meio para o cometimento do crime de burla informática e nas comunicações[65].

Do mesmo modo, entre os crimes de falsidade informática e de burla existe uma relação de concurso efetivo, atenta a diversidade de bens jurídicos tutelados por ambas as incriminações, ainda que o crime de falsidade informática seja cometido enquanto crime-meio para o cometimento do crime de burla[66].

E também, por força da diversidade de bens jurídicos tutelados por ambas as incriminações, existe uma relação de concurso efetivo entre os crimes de falsidade informática e de burla tributária, ainda que o crime de falsidade informática seja cometido enquanto crime-meio para o cometimento do crime de burla tributária[67].

Entre os crimes de falsidade informática e de sabotagem informática, atenta a diversidade de bens jurídicos tutelados e apesar de, no crime de sabotagem informática, a ação de entravar, impedir, interromper ou perturbar gravemente o funcionamento de um sistema informático ser feita por via 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, existe uma relação de concurso efetivo[68].

Entre os crimes de falsidade informática e de dano relativo a programas ou outros dados informáticos (incriminações entre as quais existe uma coincidência parcial[69]), ainda que ambas as incriminações tutelem bens jurídicos diversos, nos

[65] No mesmo sentido, PAULO ALEXANDRE GONÇALVES TEIXEIRA, O fenómeno do *Phishing*, p. 23; contra JOÃO CARLOS BARBOSA DE MACEDO, "Algumas considerações acerca dos crimes informáticos em Portugal", *in* Direito Penal Hoje, p. 237 (nota 55).
[66] Cfr. PEDRO VERDELHO, "Lei n.º 109/2009, de 15 de Setembro", *in* Comentário das Leis Penais Extravagantes, I, p. 508, e Acórdãos da RP de 30/04/2008 e 26/05/2015, *in www.dgsi.pt*.
[67] Cfr. Acórdão da RC de 26/01/2011, *in www.dgsi.pt*.
[68] Contra, JOÃO CARLOS BARBOSA DE MACEDO, "Algumas considerações acerca dos crimes informáticos em Portugal", *in* Direito Penal Hoje, p. 237 (nota 55).
[69] Cfr. PEDRO VERDELHO, "A nova Lei do Cibercrime", *in* ScIvr, T. LVIII, p. 724.

casos em que a conduta de manipulação dos dados consista na modificação (que é similar a alteração), apagamento ou supressão de dados informáticos, existirá concurso aparente na medida em que essas condutas estão abrangidas por ambas as incriminações, sendo que, nos casos em que o agente atue com as finalidades referidas no art. 3.º, n.º 1, da Lei n.º 109/2009 e da manipulação resulte a produção de dados ou documentos não genuínos, será punido pelo crime de falsidade informática, sendo punido pelo crime de dano relativo a programas ou outros dados informáticos nos demais casos.

Porém, nos casos em que o agente atue com as finalidades referidas no art. 3.º, n.º 1, da Lei n.º 109/2009 e da manipulação resulte a produção de dados ou documentos não genuínos, mas, ao mesmo tempo, acabe por, pelo menos com dolo eventual, afetar o funcionamento dos dados informáticos (em que, como veremos, se incluem os programas, atenta o conceito de dados informáticos do art. 2.º, al. b), da Lei n.º 109/2009), bem como nos casos em que, para além de a conduta consistir na modificação (que é similar a alteração), apagamento ou supressão de dados informáticos para as finalidades referidas no art. 3.º, n.º 1, da Lei n.º 109/2009, incluir igualmente alguma das demais condutas previstas no art. 4.º, n.º 1, da Lei n.º 109/2009, tutelando ambas as incriminações bens jurídicos diversos, existirá uma relação de concurso efetivo.

Entre os crimes de falsidade informática e de abuso de confiança existe uma relação de concurso efetivo, atenta a diversidade de bens jurídicos tutelados por ambas as incriminações[70].

Entre os crimes de falsidade informática e de abuso de cartão de garantia ou de crédito existe uma relação de concurso efetivo, atenta a diversidade de bens jurídicos tutelados por ambas as incriminações.

Quanto aos crimes de falsidade informática e de dispositivos ilícitos (p. e p. pelo art. 104.º, n.ºs 1, al. a), e 3, da Lei n.º 5/2004, de 10 de fevereiro), há que ter em conta que o art. 3.º, n.º 4, da Lei n.º 109/2009 passou a incluir todas as

[70] Cfr. PEDRO VERDELHO, "Lei n.º 109/2009, de 15 de Setembro", *in* Comentário das Leis Penais Extravagantes, I, p. 508, e Acórdão da RL de 09/01/2007, *in www.dgsi.pt*.

condutas subsumíveis ao art. 104.º, n.º 1, al. a), da Lei n.º 5/2004[71], pelo que consideramos que ocorreu uma revogação (tácita) do art. 104.º, n.º 1, al. a), da Lei n.º 5/2004 pelo art. art. 3.º, n.º 4, da Lei n.º 109/2009 (salvo no caso do fabrico); mas, ainda que assim não fosse, o disposto no art. 104.º, n.º 1, al. a), da Lei n.º 5/2004 dificilmente encontraria campo de aplicação em face do disposto no n.º 3 desse preceito, dado que, sempre que a conduta seja subsumível, quer à previsão deste preceito quer à previsão do art. 3.º, n.º 4, da Lei n.º 109/2009, existe uma relação de concurso aparente (por subsidiariedade explícita), sendo o agente punido pela prática do crime p. e p. pelo art. 3.º, n.º 4, da Lei n.º 109/2009, cuja pena aplicável é mais elevada.

No caso do crime de fabrico de dispositivos ilícitos, não sendo tal conduta punível nos termos do art. 3.º, n.º 4, da Lei n.º 109/2009, o agente será punido pelo crime de dispositivos ilícitos p. e p. pelo art. 104.º, n.ºs 1, al. a), e 3, da Lei n.º 5/2004, salvo se a conduta de fabrico de dispositivos ilícitos concretamente adotada pelo agente for subsumível ao art. 3.º, n.º 2, da Lei n.º 109/2009, dado que, atenta a moldura penal mais elevada no caso deste preceito, o agente será punido pelo crime de falsidade informática p. e p. pelo art. 3.º, n.º 2, da Lei n.º 109/2009 por força do disposto no art. 104.º, n.º 3, da Lei n.º 109/2009[72].

Entre o crime de falsidade informática e a contraordenação de dispositivos ilícitos (p. e p. pelo art. 104.º, n.º 1, als. b) a d), conjugado com o art. 113.º, n.º 2, al. ll), e 3, zz), ambos da Lei n.º 5/2004, de 10 de fevereiro, sendo grave no caso da al. d) e muito grave no caso das als. b) e c), sempre que a conduta possa ser subsumida ao art. 3.º, n.º 4, da Lei n.º 109/2009, o ilícito contraordenacional será consumido pelo ilícito penal, sendo o agente apenas punido pelo crime p. e p. pelo art. 3.º, n.º 4, da Lei n.º 109/2009. Diversamente, quando o agente pratique

[71] No mesmo sentido, PEDRO VERDELHO, "Lei n.º 109/2009, de 15 de Setembro", *in* Comentário das Leis Penais Extravagantes, I, p. 508, e também em "Lei n.º 5/2004, de 10 de Fevereiro", *in* Comentário das Leis Penais Extravagantes, I, pp. 468-469 e em "A nova Lei do Cibercrime", *in* ScIvr, T. LVIII, pp. 725-726.

[72] Neste sentido, considerando que o art. 3.º, n.º 2, da Lei n.º 109/2009 poderá ter mesmo revogado o art. 104.º, n.º 1, al. a), da Lei n.º 5/2004 na modalidade do "fabrico", PEDRO VERDELHO, "Lei n.º 5/2004, de 10 de Fevereiro", *in* Comentário das Leis Penais Extravagantes, I, p. 468.

factos, uns subsumíveis ao art. 3.º, n.º 4, da Lei n.º 109/2009 e outros (apenas) subsumíveis ao art. 104.º, n.º 1, als. b) a d), conjugado com o art. 113.º, ambos da Lei n.º 5/2004, será punido pela prática do crime p. e p. pelo art. 3.º, n.º 4, da Lei n.º 109/2009 e pela contraordenação p. e p. pelo art. 104.º, n.º 1, als. b) a d), conjugado com o art. 113.º, ambos da Lei n.º 5/2004.

Uma última situação de concurso que poderá ocorrer será entre o art. 3.º, n.º 4, da Lei n.º 109/2009 e o art. 128.º do RGIT[73]. Ora, na medida em que o art. 128.º, n.º 1, do RGIT não exige a efetiva utilização de tais programas informáticos, sempre que ocorra uma utilização efetiva desses programas e esteja preenchida a previsão legal do crime de falsidade informática p. e p. pelo art. 3.º da Lei n.º 109/2009, o agente será punido pela prática deste crime, como resulta do próprio art. 128.º, n.º 1, do RGIT, quando exclui a punição a título contraordenacional sempre que a conduta do agente também constitua crime[74].

No entanto, a situação acaba por se complicar na medida em que existe uma sobreposição entre as disposições do art. 128.º, n.º 1, do RGIT e do art. 3.º, n.º 4, da Lei n.º 109/2009, sendo que PEDRO DIAS VENÂNCIO[75] considera que tal sobreposição não será total, dado que o legislador apenas pune como crime as condutas associadas a dispositivos que permitam o acesso a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado e que tenha sido efetivamente utilizado para praticar alguma das ações previstas no n.º 2 e, desse modo, as demais condutas de "*criar, ceder ou transacionar programas informáticos, concebidos com o objetivo de impedir ou alterar o apuramento da situação tributária do contribuinte*", são punidas ao abrigo do art. 128.º, n.º 1, do RGIT como contraordenação.

Um outro argumento no sentido da inexistência de concurso efetivo e de, pelo contrário, existir um mero concurso aparente, prende-se com o facto de,

[73] Preceito cuja epígrafe é "Falsidade informática" e prevê uma contraordenação, dispondo o seu n.º 1 que «*Quem criar, ceder ou transacionar programas informáticos, concebidos com o objetivo de impedir ou alterar o apuramento da situação tributária do contribuinte, quando não deva ser punido como crime, é punido com coima variável entre €3750 e € 37 500.*».

[74] No mesmo sentido, PEDRO DIAS VENÂNCIO, Lei do Cibercrime, p. 41.

[75] PEDRO DIAS VENÂNCIO, Lei do Cibercrime, p. 41.

também no caso da contraordenação p. e p. pelo art. 128.º, n.º 1, do RGIT, o bem jurídico tutelado ser a segurança e a fiabilidade dos documentos no tráfico jurídico-probatório (com incidência das relações tributárias) – tal como sucede com o crime de falsidade informática –, estando em causa uma antecipação da punição contra a criação, cedência ou transação de programas informáticos dirigidos a permitir falsificações ou a induzir a administração tributária em erro[76].

[76] Cfr. BENJAMIM SILVA RODRIGUES, Da Prova Penal, IV, p. 130.

BIBLIOGRAFIA

Albuquerque, Paulo Pinto de – Comentário do Código Penal à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem, Universidade Católica Editora, Lisboa, 2008.

Ascensão, José de Oliveira – "Criminalidade informática", *in* Direito da Sociedade da Informação, Vol. II, pp. 203 e ss., Coimbra Editora, Coimbra, 2001.

Correia, Eduardo – A Teoria do Concurso em Direito Penal, 2.ª Reimpressão, Almedina, Coimbra, 1996.

Correia, Miguel Pupo – Direito Comercial, Direito da Empresa, 9.ª Edição, refundida e actualizada, Ediforum, Lisboa, 2005.

Costa, A. M. Almeida – "Art. 221º", *in* Comentário Conimbricense do Código Penal Parte Especial, Tomo II, Artigos 202º a 307º, pp. 328 e ss., Coimbra Editora, Coimbra, 1999.

Costa, A. M. Almeida – "Antes do art. 262º", *in* Comentário Conimbricense do Código Penal Parte Especial, Tomo II, Artigos 202º a 307º, pp. 736 e ss., Coimbra Editora, Coimbra, 1999.

Costa, A. M. Almeida – "Art. 267º", *in* Comentário Conimbricense do Código Penal Parte Especial, Tomo II, Artigos 202º a 307º, pp. 807 e ss., Coimbra Editora, Coimbra, 1999.

Costa, José Francisco de – "Algumas reflexões sobre o estatuto dogmático do chamado "Direito penal informático"", *in* Direito Penal da Comunicação, Alguns escritos, pp. 103 e ss, Coimbra Editora, Coimbra, 1998.

Costa, José Francisco de/ Moniz, Helena – "Algumas reflexões sobre a criminalidade informática em Portugal", *in* Boletim da Faculdade de Direito da Universidade de Coimbra, Vol. LXXIII (1997), pp. 297 e ss, Universidade de Coimbra, Coimbra, 1997.

Dias, Jorge de Figueiredo – Direito Penal, Parte Geral, Tomo I, 2.ª Edição, Coimbra Editora, Coimbra, 2007.

Faria, Paula Ribeiro de – "Art. 275º", *in* Comentário Conimbricense do Código Penal Parte Especial, Tomo II, Artigos 202º a 307º, pp. 889 e ss., Coimbra Editora, Coimbra, 1999.

Faria, Paula Ribeiro de – "Art. 276º", *in* Comentário Conimbricense do Código Penal Parte Especial, Tomo II, Artigos 202º a 307º, pp. 903 e ss., Coimbra Editora, Coimbra, 1999.

Leal Henriques, Manuel/Santos, Manuel Simas – Código Penal Anotado, 3.ª Edição, 2.º Vol., Parte Especial, Editora Rei dos Livros, Lisboa, 2000.

Macedo, João Carlos da Cruz Barbosa de – "Algumas considerações acerca dos crimes informáticos em Portugal", *in* Direito Penal Hoje, Novos desafios e novas respostas, pp. 221 e ss., Coimbra Editora, Coimbra, 2009.

Marques, Garcia/Martins, Lourenço – Direito da Informática, 2.ª Edição Refundida e Actualizada, Almedina, Coimbra, 2006.

Moniz, Helena – "Art. 256º", *in* Comentário Conimbricense do Código Penal Parte Especial, Tomo II, Artigos 202º a 307º, pp. 674 e ss, Coimbra Editora, Coimbra, 1999.

Pereira, Joel Timóteo Ramos – Compêndio Jurídico da Sociedade da Informação, Quid Juris, Lisboa, 2004.

Rocha, Manuel António Lopes – "A lei da criminalidade informática (Lei n.º 109/01 de 17 de Agosto). Génese e técnica legislativa", *in* Cadernos de Ciência de Legislação, n.º 8 (Outubro-Dezembro 1993), pp. 65 e ss, Instituto Nacional da Administração, Lisboa, 1993.

Rodrigues, Benjamim Silva – Da Prova Penal, T. IV, Da Prova Electrónico-Digital e da Criminalidade Informático-Digital (Contributo para a Fundamentação de um Modelo Dinâmico-Reversivo de Ciência Forense Digital em sede de Investigação da Cyber-Criminalidade Informático-Digital e à Luz do Novíssimo Regime da Lei do Cibercrime Portuguesa), Rei dos Livros, Lisboa, 2011.

Simas, Diana Viveiros de – O Cibercrime*, in* *http://recil.ulusofona.pt/bitstream/*

handle/10437/5815/Tese%20Cibercrime%20-%20Diana%20Simas.pdf?sequence=1 (consultado em 21/04/2016).

Teixeira, Paulo Alexandre Gonçalves – O fenómeno do *Phishing*, Enquadramento jurídico-penal, *in* *http://repositorio.ual.pt/bitstream/11144/301/1/O%20fen%C3%B3meno%20do%20Phishing%20%E2%80%93%20Enquadramento%20Jur%C3%ADdico-Penal%20%282013-02%29.pdf* (consultado em 21/04/2016).

Velozo, José António/Rocha, Manuel A. Cardoso Lopes – "Criminalidade informática: modos de execução", *in* Scientia Ivridica, T. XXXV (1986), pp. 173 e ss, Livraria Cruz, Braga, 1986.

Venâncio, Pedro Dias – "O Crime de Falsidade Informática", *in* JusNet 120/2010, *in http://jusjornal.wolterskluwer.pt* (consultado em 21/04/2016).

Venâncio, Pedro Dias – Investigação e meios de prova na criminalidade informática, *in* *www.verbojuridico.net/doutrina/tecnologia/meiosprovacriminalidadeinformática.pdf* (consultado em 21/04/2016).

Venâncio, Pedro Dias – Lei do Cibercrime Anotada e Comentada, Coimbra Editora, Coimbra, 2011.

Verdelho, Pedro – "A nova Lei do Cibercrime", *in* Scientia Ivridica, T. LVIII (2009), pp. 717 e ss, Universidade do Minho, Braga, 2009.

Verdelho, Pedro – "Lei n.º 5/2004, de 10 de Fevereiro", *in* Comentário das Leis Penais Extravagantes, I, pp 465 e ss, Universidade Católica Editora, Lisboa, 2010.

Verdelho, Pedro – "Lei n.º 109/2009, de 15 de Setembro", *in* Comentário das Leis Penais Extravagantes, I, pp 505 e ss, Universidade Católica Editora, Lisboa, 2010.

Verdelho, Pedro/Bravo, Rogério/Rocha, Manuel Lopes – Leis do Cibercrime, Vol. I, Centro Atlântico, Vila Nova de Famalicão, 2003.

JURISPRUDÊNCIA

SUPREMO TRIBUNAL DE JUSTIÇA

Acórdão de 20 de setembro de 2006 (Proc. 06P1942), *in www.dgsi.pt.*

Acórdão de 5 de novembro de 2008 (Proc. 08P2817), *in www.dgsi.pt.*

Acórdão de 18 de dezembro de 2013 (Proc. 6479/09.8TBBRG.G1.S1), *in www.dgsi.pt.*

TRIBUNAL DA RELAÇÃO DE COIMBRA

Acórdão de 26 de janeiro de 2011 (Proc. 370/06.7TACBR.C1), *in www.dgsi.pt.*

TRIBUNAL DA RELAÇÃO DE ÉVORA

Acórdão de 19 de maio de 2015 (Proc. 238/12.8PBPTG.E1), *in www.dgsi.pt.*

TRIBUNAL DA RELAÇÃO DE LISBOA

Acórdão de 9 de janeiro de 2007 (Proc. 5940/2006-5), *in www.dgsi.pt.*

Acórdão de 15 de dezembro de 2009 (Proc. 4251/07.7TDLSB.L1-5), *in www.dgsi.pt.*

Acórdão de 30 de junho de 2011 (Proc. 189/09.3JASTB.L1-5), *in www.dgsi.pt.*

Acórdão de 10 de julho de 2012 (Proc. 7876/10.1JFLSB.L1-5), *in www.dgsi.pt.*

TRIBUNAL DA RELAÇÃO DO PORTO

Acórdão de 30 de abril de 2008 (Proc. 0745386), *in www.dgsi.pt.*

Acórdão de 21 de novembro de 2012 (Proc. 1001/11.9JAPRT.P1), *in www.dgsi.pt.*

Acórdão de 24 de abril de 2013 (585/11.6PAOVR.P1), *in www.dgsi.pt.*

Acórdão de 17 de setembro de 2014 (Proc. 2013/13.3JAPRT.P1), *in www.dgsi.pt.*

Acórdão de 7 de outubro de 2014 (Proc. 747/12.9TJPRT.P1), *in www.dgsi.pt.*

Acórdão de 26 de maio de 2015 (Proc. 35/07.2JACBR.P1), *in www.dgsi.pt.*