FACULDADE DE DIREITO
Universidade de Lisboa

A PROBLEMÁTICA DO CONCURSO DE NORMAS NO ÂMBITO DA CRIMINALIDADE INFORMÁTICA - A FALSIDADE INFORMÁTICA - ART.º 3.º DA LEI 109/2009, DE 15 DE SETEMBRO, E OS ARTIGOS 267.º, E 262.º, AMBOS DO CÓDIGO PENAL.

Dissertação realizada no âmbito do Mestrado em Direito e Prática Jurídica, na especialidade em Direito Penal, sob orientação da Exma. Professora Doutora Inês Ferreira Leite.

Nuno Alexandre Craveiro Cabral

2019

À Vanda, Beatriz e Maria, pelas minhas ausências, e enorme paciência depositada neste meu projeto.

AGRADECIMENTOS

À minha mulher, pelo permanente apoio, encorajamento e motivação, por me fazer acreditar que este meu projeto era possível.

Às minhas duas filhas, pela enorme paciência demonstrada e por todas as minhas omissões.

À Professora Doutora Inês Ferreira Leite, que gentilmente se predispôs a orientar a presente dissertação, e pelos diversos esclarecimentos, chamadas de atenção, conselhos, bem ainda as correções que o presente trabalho justificou.

À Faculdade de Direito de Lisboa, por todo o conhecimento que me permitiu alcançar.

Ao meu colega e amigo José Amador que me incentivou a percorrer o caminho do Direito.

Ao meu colega e amigo Hernâni Pinto, por toda a ajuda, incentivo e revisão da presente dissertação.

Ao Dr. Pedro Verdelho, Procurador da República e Coordenador do Gabinete Cibercrime do Ministério Público, pela amabilidade em me receber, e por todos os esclarecimentos que me prestou que se demonstraram preciosos à elaboração deste projeto.

A todas as funcionárias da biblioteca da Procuradoria Geral Da República, que gentilmente me disponibilizaram todas as obras e artigos que solicitei, e as quais permitiram a feitura do presente trabalho.

RESUMO

A presente dissertação, realizada no âmbito do Mestrado em Direito e Prática Jurídica, na especialidade em Direito Penal, tem por objetivo a obtenção do grau de Mestre, tendo como destino a sua apresentação à Faculdade de Direito da Universidade de Lisboa.

Pretende-se com este estudo analisar toda a evolução da fraude com cartões bancários em Portugal, bem como a sua implicação ao nível das decisões dos nossos tribunais, desde a entrada em vigor do Dec. Lei n.º 48/95, de 15/03.

A celebração da Convenção de Budapeste, também conhecida por Convenção do Cibercrime em 23 de novembro de 2001, e a respetiva transposição para o ordenamento jurídico interno, através da Lei 109/2009 de 15 de setembro, colocou desafios à jurisprudência nacional, no confronto verificado entre comportamentos criminosos subsumíveis à norma constante do n.º 3.º da citada Lei, e os artigos 267.º e 262.º do nosso Código Penal.

No entanto, como se irá demonstrar ao longo da presente dissertação, a mencionada Lei do Cibercrime esvaziou de sentido a remissão operada pelo artigo 267.º do Código Penal, porquanto prevê, de forma inequívoca, a punição destes comportamentos, não se afigurando deste modo pertinente o recurso ao concurso de crimes, sob pena de violação do princípio do *ne bis in idem*.

PALAVRAS-CHAVE: Fraude com cartão bancário; Falsidade Informática; Clonagem de cartão bancário; Contrafação de Títulos Equiparados a Moeda; Captura de dados bancários inseridos em banda magnética; Concurso de Crimes.

ABSTRACT

The present dissertation carried out within the scope of the Master's Degree in Law and Legal Practice, specializing in Criminal Law, is carry out to obtain the Master's degree, with the purpose of presenting it to the Faculty of Law of the University of Lisbon.

The purpose of this study is to analyze all the evolution of bank card fraud in Portugal, as well as its implication in the decisions of our courts, since the entry into force of Dec. Law n. º 48/95 of 15/03.

The celebration of the Budapest Convention, also known as the Cybercrime Convention on November 23, of 2001, and its transposition into the internal legal order, through Law 109/2009 of September 15, stood challenges to national jurisprudence, in the confrontation verified between criminal behavior subsumed by the norm contained in article 3.º of the said Law, and articles 267.º and 262.º of our Penal Code.

However, as will be demonstrated throughout this dissertation, the above-mentioned Cybercrime Act has rendered meaningless the reference made by Article 267.º of the Criminal Code, since it provides unequivocal punishment for these behaviors and does not appear to be so infringement of the principle of *ne bis in idem*.

KEY-WORDS: Bank card fraud; Informatic Falsity; Bank cards replicating; Counterfeiting of Currency-equivalent Securities; Capturing bank data inserted in a magnetic stripe; Rules Contest.

INDÍCE

FORMA DE CITAR

A presente dissertação adota a norma APA.

1. A EVOLUÇÃO DOS CARTÕES DE PAGAMENTO NO SISTEMA BANCÁRIO PORTUGUÊS

O Cartão de crédito

A introdução do primeiro cartão de crédito no sistema bancário Português ocorreu nos finais dos anos cinquenta (Cordeiro, 2016, pp. 655-656) e, início da década de sessenta (Ferreira, 2011, p. 11), sob licença do "*Diners Club International"*. Só mais tarde, em março de 1970, é, finalmente, concebido o primeiro cartão de crédito bancário Português - o cartão "Sottomayor".

No entanto, somente no ano de 1974 através de uma associação fundada por diferentes bancos, é criado o cartão Unibanco (Ferreira, 2011, p. 11).

Este projeto beneficiou não só da permissão das entidades norte-americanas competentes, tanto no procedimento subjacente ao necessário licenciamento, mas igualmente, da anterior experiência nesta matéria oriunda dos Estados Unidos da América (Ferreira, 2011, p. 11). Conclui-se pelo exposto, que o primeiro cartão de crédito a operar em Portugal resultou não só da evolução económica, mas sobretudo por influência dos Estados Unidos da América (Ferreira, 2011, p. 11).

Hodiernamente a utilização de cartões de crédito[1] origina a celebração de um contrato entre o respetivo emitente desse cartão e o futuro titular, através do qual é acordado um limite máximo de crédito que uma vez utilizado parcialmente ou na sua totalidade, o titular se obriga a reembolsar, nas condições previamente acordadas (Guimarães, https://repositorio-aberto.up.pt, p. 319).

Essas condições compreendem as modalidades de pagamento integral ou parcial havendo, numa ou noutra situação, a possibilidade do pagamento de juros (Cordeiro, 2016, p. 655). Nessa relação, existe ainda um terceiro interveniente em regra um comerciante ou um fornecedor de serviços (Cordeiro, 2016, p. 659).

Em finais de 2003, segundo estimativas da altura, existiriam, cerca de quatro milhões de cartões de crédito a operarem em Portugal[2].

O funcionamento do cartão de crédito implica necessariamente a utilização cumulativa de outros instrumentos que permitem a validação da transação em causa.

---

1 BdP, Aviso, 11/2001, alínea b) do ponto 1.º

2 BdP, https://www.bportugal.pt/, 2004, p. 2

Inicialmente, a operação subjacente à utilização do cartão de crédito era autenticada mediante a utilização de uma máquina de impressão monográfica idêntica a um "ferro de engomar", na qual o cartão e um verbete previamente preenchido com o montante da despesa ou do levantamento, eram comprimidos por uma peça móvel dessa máquina transpondo para o verbete todas as inscrições em relevo constantes no cartão (Cordeiro, Direito bancário, 2016, p. 657).

Uma vez preenchido esse verbete, constituído por um original e duas cópias, era autenticado pela assinatura do titular do cartão que conservava para si uma das cópias, atestando assim a legitimidade da operação (Cordeiro, 2016, p. 657).

Quanto às demais duas cópias desse verbete, uma ficava na posse do comerciante e a outra era entregue pelo comerciante ao balcão do banco emissor do cartão de crédito, com vista ao ressarcimento da despesa efetuada pelo cliente.

Esse procedimento, porém, não envolvia quaisquer ligações ou comunicações eletrónicas ou sequer o recurso a redes informáticas, como se verifica atualmente.

O Cartão de garantia

O cartão de garantia por outro lado consistia num instrumento bancário que uma vez exibido por um cliente perante o comerciante, em acto simultâneo ao da entrega de um cheque para o respetivo pagamento de bens ou serviços, identificava por um lado o respetivo titular do cheque e por outro assegurava ao comerciante o pagamento por parte do banqueiro emissor desse cartão, de um determinado limite financeiro subjacente ao cheque entregue, independentemente da existência de provisão de saldo na conta bancária de onde iria ser descontado (Pereira, 1990, p. 5)[3].

Este cartão foi introduzido em Portugal em meados dos anos oitenta e, entretanto, retirado do mercado após o início da década de noventa, em razão da sua função de garantia ter sido paulatinamente integrada nos cartões de débito e de crédito (Aguiar, 1990, pp. 27-28).

Os cheques por outro lado após a constatação por parte dos banqueiros que os respetivos custos de exploração haviam atingido valores excessivos associados ainda à falta de confiança que naqueles era depositada (Aguiar, 1990, pp. 27-28), acabaram mais tarde por perder terreno para a cada vez maior utilização do cartão de débito.

[3] Neste mesmo sentido (Aguiar, 1990, p. 27), e, (Dias, et al., 1999, p. 811)

O Cartão de débito

O cartão de débito, por outro lado, foi introduzido no sistema bancário Português em fevereiro de 1985, inicialmente com a designação de "Cartão Multibanco" (Fernandes, 1998, p. 17). Foi possível concluir que até ao final do ano de 1997 já havia sido, entretanto, contabilizada a emissão de mais de oito milhões deste tipo de cartão (Rodrigues A., 1997, p. 1), e, em finais do ano de 2003, cerca de onze milhões[4].

O pagamento a débito de acordo com o Aviso do Banco de Portugal 11/2001[5] consiste na permissão outorgada ao respetivo titular desse cartão associado necessariamente a uma conta de pagamento, em regra uma conta à ordem aberta junto de uma instituição bancária, que lhe permite efetuar um conjunto alargado de serviços bancários de entre os quais o pagamento de diversos serviços em caixas automáticas ou perante comerciantes em que o valor pago é imediatamente descontado do saldo bancário disponível nessa conta bancária[6/7].

A emissão deste cartão está necessariamente subjacente a um contrato no qual figuram enquanto intervenientes apenas o banqueiro e o cliente.

A operação a débito compreende o pagamento de bens ou serviços em que montante envolvido é imediatamente subtraído ao saldo da conta bancária à qual o cartão de débito se encontra associado.

O Cartão bancário de pagamento

Presentemente no sistema bancário Português, existem três categorias de cartões bancários; o cartão de débito, o cartão de crédito, e o cartão pré-pago[8].

Por sua vez os cartões bancários dependendo da forma como podem ser utilizados dividem-se em dois tipos; - o cartão puro ou simples, que consiste naquele que desempenha, exclusivamente, uma das categorizações atrás referidas, ou seja, a função de débito, crédito ou pré-pago, ou, o cartão dual ou misto[9].

---

[4] BdP, https://www.bportugal.pt/, 2004, p. 2

[5] DR., 1Série B, n.º 269, de 20 de Novembro de 2001.

[6] BdP, Aviso, 11/2001, alínea b) do ponto 1.º.

[7] Informação igualmente constante em (BdP, https://www.bportugal.pt/, 2018.

[8] BdP, https://www.bportugal.pt/, 2004, p. 5

[9] Corroborando esta informação (BdP, https://www.bportugal.pt/, 2004, p. 2.

Esta última categoria de cartões bancários, por sua vez consiste na fusão das funções dos cartões de débito e de crédito pois permitem operações bancárias a débito na conta de depósito à ordem a que estão necessariamente associados nos exatos termos a que estão sujeitos os cartões de débito simples e, operações bancárias a crédito em termos em tudo semelhantes aos vulgares cartões de crédito[10].

O cartão pré-pago, por sua vez, consiste num cartão ao qual se encontra associado um montante pré-pago que quando utilizado implica um desconto com efeitos imediatos no valor do saldo disponível[11].

O cartão bancário encontra-se devidamente normalizado, através de um retângulo de plástico com as medidas de 86 por 54mm, e com 0,76mm de espessura[12], contendo ainda uma banda magnética na qual se encontram inseridos diversos elementos de segurança atinentes ao cartão, e ao código de segurança definido pelo titular (Cordeiro, 2016, p. 655).

Os cartões bancários são em regra emitidos por Instituições de Crédito ou, igualmente por outras entidades devidamente autorizadas para o efeito (Rodrigues A., 1997, p. 1)[13] permitindo o pagamento por duas vias, a débito, ou, a crédito (Cordeiro, 2016, p. 658).

Por outro lado, o pagamento com recurso a cartões bancários pode ser materializado com a utilização física do cartão em caixas automáticos ou, em terminais de pagamento automático, normalmente disponibilizados por comerciantes, ou ainda de forma não presencial com a inserção do número do cartão bancário para o pagamento de bens ou serviços em comerciantes com estabelecimentos comerciais na Internet, ou seja, afastando-se dessa forma a necessária interação física do cartão bancário com os demais sistemas de pagamento normalmente utilizados para validação da transação.

Essas duas formas de pagamento, são designadas, abreviadamente, pelos acrónimos de CP e CNP[14].

[10] BdP, https://www.bportugal.pt/, 2018.
[11] *Ibidem*
[12] Norma ISO 2894, registada em 01/12/1980.
[13] No mesmo sentido (Cordeiro, Direito bancário, 2016, p. 655) e (BdP, Aviso, 11/2001) - Alínea b) do ponto 2.º.
[14] Que deriva da tradução Inglesa de "Card Present" e "Card not Present".

2. A CONTRAFAÇÃO DE TÍTULOS EQUIPARADOS A MOEDA NO CÓDIGO PENAL PORTUGUÊS

O legislador quando introduziu o termo *contrafação* no nosso Código Penal teria em mente dois objetivos; por um lado atribuir um aumento da proteção penal à reprodução ilegítima de certos documentos tendo em conta os respetivos valores neles incorporados, quer se tratassem de valores probatórios ou patrimoniais, nomeadamente os documentos de identificação e os títulos de crédito e, por outro punir com maior severidade comportamentos que se subsumissem ao respetivo fabrico ilegítimo, quer os relativos a eventuais atos preparatórios.

Relativamente aos títulos de crédito equiparados a moeda, mencionados na alínea c) do n. º 1, do art. º 267.º do Código Penal – cartões de garantia ou de crédito estava em causa na alteração introduzida pelo Dec. Lei n.º 48/95, de 15/03 (Dias, et al., 1999, p. 807), a antecipação da tutela penal na punição de comportamentos suscetíveis de produzir *"...A fabricação ex. novo da base material do documento...*" (Albuquerque P. P., 2015, p. 932)[15], que no caso em apreço se reconduziria à *"... mera incriminação da falsificação do cartão enquanto peça de plástico com informação gráfica impressa..."* (Albuquerque & Verdelho, 2010, p. 507).

Nessa época[16], ou seja, em momento anterior à entrada em vigor do referido Dec. Lei n.º 48/95, de 15/03 os fenómenos criminais subjacentes à utilização deste tipo de documentos tinham por base a contrafação de cartões plásticos em tudo idênticos aos cartões de garantia que quando exibidos perante um comerciante em simultâneo com a entrega de um cheque, geralmente sem provisão bancária, iludiam os comerciantes levando-os por esse meio a aceitarem esses cheques bancários na espectativa de que os montantes aí inscritos seriam sempre garantidos pelos banqueiros responsáveis pela emissão de tais cartões.

Com os cartões de crédito sucediam-se comportamentos semelhantes na medida em que os autores deste tipo de ilícitos na posse de um cartão de crédito contrafeito, entregavam-no ao comerciante, que, para a necessária validação da transação utilizava a já mencionada máquina de impressão monográfica tipo *"ferro de engomar"* na qual esse cartão contrafeito produzia subsequentemente num verbete previamente preenchido com o montante da despesa, ou, do levantamento, através da compressão por uma peça móvel

---

15 Nesse mesmo sentido, (Leal-Henriques & Simas Santos, 2000, p. 1100).

16 Não necessariamente aquando da entrada em vigor do Dec. Lei n.º 48/95, de 15/03, mas, sobretudo, há data em que foram debatidas as alterações ao Código Penal de 1982, que tiveram lugar com a entrada em vigor do mencionado Dec. Lei.

dessa máquina, todas as inscrições em relevo impressas no cartão. Em seguida, o autor assinava esse verbete, forjando a assinatura do legítimo titular do cartão, cujo contrafeito pretendia substituir (Rodrigues B. M., Março de 1999, p. 3)[17].

No entanto, a contínua e rápida evolução dos sistemas de pagamento bancário a que fomos assistindo, associado ao elevado interesse do aumento do número de caixas automáticas[18] que num curto espaço de tempo foram sendo instaladas por todo o país (Cadete, p. 6), acentuou o decrescimento da diminuta utilização que já então se fazia do cheque culminando na prática com a descontinuação do cartão de garantia do mercado.

As diversas vantagens entretanto conferidas aos titulares de cartões bancários, de crédito ou de débito pouco tempo após a entrada em vigor das alterações ao Código Penal de 1995, alteraram toda a fisionomia do sistema bancário de então.

De uma forma cada vez mais rápida, inúmeras inovações e avanços tecnológicos, iam-se implementando em todo sistema bancário mundial, e em particular na Europa, com maior enfoque na cada vez maior segurança associada às transações bancárias.

Os próprios cartões bancários, foram alvo de diversas inovações, mormente, a introdução no próprio fabrico do plástico, de diversos elementos adicionais de segurança.

A esse propósito, a banda magnética e respetivos elementos bancários aí gravados, bem ainda os diversos certificados inseridos no fabrico originário do plástico, acrescido do incremento da tecnologia EMV, ou seja, a introdução de um "Chip" no próprio cartão, o qual consiste num circuito integrado contendo inúmeros dados bancários que em conjunto, conferem maior segurança nas transações uma vez que sempre que um cartão com este tipo de tecnologia é utilizado para essa transação em concreto é gerado um código específico que a valida no sistema bancário, permitindo o respetivo pagamento (Antunes & Rodrigues, 2018, p. 110).

No moderno fabrico do plástico para os cartões bancários são utilizadas técnicas que permitem desde logo a incorporação de um microprocessador e um chip de memória.

Mais recentemente, foi introduzida a tecnologia NFC, ou, *"contactless"*, permitindo-se por este meio o pagamento de serviços com a simples aproximação do cartão ao respetivo terminal de pagamento não havendo consequentemente a necessidade da sua passagem num terminal de pagamento automático nem tão-pouco a inserção do respetivo código secreto.

---

[17] Onde responde à seguinte questão: *"O que é a contrafação de cartões de crédito? Consiste em alterar os elementos identificativos de um cartão de plástico que se encontra na posse do infrator, para que este se assemelhe com um outro cartão emitido legitimamente por uma entidade bancária ou de crédito..."*

[18] Abreviadamente designadas por ATM – "*Automated Teller Machine"*.

Os pagamentos efetuados junto dos comerciantes passaram a concretizar-se através de ligações informáticas aos servidores dos bancos, com recurso à utilização de terminais automáticos de pagamento eletrónico, que estes colocavam à disposição dos seus clientes[19].

Os benefícios eram evidentes para ambas as partes. Possibilitavam-se pagamentos de avultados montantes diretamente em estabelecimentos comerciais que dispunham de terminais de pagamento eletrónico (Cadete, p. 7), incentivando-se por um lado o aumento do consumismo mas por outro, o incremento de uma maior e melhor segurança nas transações uma vez que os comerciantes evitavam dessa forma não só a presença de grandes quantias em numerário nos respetivos estabelecimentos, diminuindo desse modo igualmente a sua vulnerabilidade a furtos por parte de funcionários ou de roubos levados a cabo por terceiros (Cadete, p. 8).

Aos titulares de cartões bancários, foi ainda concedida a possibilidade de não terem que transportar consigo avultadas somas de dinheiro (Cadete, p. 8).

Por outro lado, importará considerar que outras razões estariam subjacentes ao facto de apenas aos cartões de garantia e de crédito o Legislador lhes ter concedido tal dimensão, acolhimento e proteção legal, como as que vieram a merecer em sede da previsão estatuída na norma do art.º 267.º do Código Penal?

E porque motivo, não teve o cartão de débito, introduzido no sistema bancário nacional em 1985, igual proteção legal se tal como o cartão de garantia ou de crédito permitia o acesso a fundos titulados por terceiros?

A resposta à questão formulada, pode ser encontrada recorrendo a um mero raciocínio lógico.

Apenas os cartões de garantia e de crédito, permitiam, através de contrafações do respetivo plástico produzir o engano nas relações jurídicas.

O primeiro, mediante a mera apresentação em simultâneo com um cheque.

O segundo, através da forma de pagamento subjacente à já mencionada máquina de impressão monográfica tipo "ferro de engomar".

Contrariamente, se a intenção do Legislador, na proteção legal concedida aos referidos meios de pagamento, mencionados na alínea c) do n.º 1, do art.º 267.º do Código Penal, fosse no sentido que sobre estes incidissem uma eventual antecipação da tutela penal relativa à possibilidade de terceiros, ilicitamente apropriarem-se de quantias patrimoniais a estes associados ainda que tal contrafação se estendesse igualmente, aos

[19] Os terminais de pagamento eletrónico são designados de "*POS"* - designação decorrente da tradução da língua inglesa de um terminal de pagamento eletrónico; "*Point of Sale ou Point of Service".*

dados bancários inseridos nas respetivas bandas magnéticas, porque motivo, e enigmaticamente, se havia "esquecido" do cartão de débito[20]?

Por outro lado, se assim fosse, esse entendimento não faria sentido, tendo em conta a circunstância de ao cartão de garantia estar subtraída essa função, ou seja, a mesma bastava-se com a simples apresentação ao comerciante em simultâneo com o cheque que o mesmo pretendia garantir o respetivo pagamento.

Dito de uma outra forma, inexistia a necessidade de tal cartão interagir de todo, com qualquer equipamento.

Além do mais, no ano de 1995, era ainda desconhecida a atual e necessária tecnologia que mais tarde permitiu todo este modo de atuação criminoso de manipulação dos dados bancários inseridos nas bandas magnéticas dos cartões bancários.

Por último, chama-se a atenção para o facto de ainda no ano de 2003, tanto na Doutrina, como na Jurisprudência Portuguesa, subsistiam dúvidas, e por conseguinte a discussão, se a manipulação dos dados bancários gravados nas bandas magnéticas dos cartões de crédito, e a subsequente utilização ilegítima, se subsumia ao tipo legal previsto no artigo 225.º do Código Penal – O abuso de Garantia ou de Crédito, ou até a eventual existência de um concurso entre aquele tipo legal e o de Falsidade Informática prevista no artigo 4.º, da revogada Lei da Criminalidade Informática – 109/91, de 17 de Agosto (Verdelho, 2003, pp. 362-363).

3. A LEI DO CIBERCRIME

A Lei n.º 109/2009, de 15 de setembro, entrou em vigor no ordenamento jurídico nacional em 15 de setembro de 2009, tendo recebido, entretanto a denominação de Lei do Cibercrime. Esta nova Lei, procedeu à revogação da Lei n. º 109/91 de 17 de agosto - Lei da Criminalidade Informática. A génese da Lei do Cibercrime assenta na ratificação por Portugal da Convenção de Budapeste datada de 23/11/2001 – A Convenção sobre Cibercrime, e a subsequente transposição para o ordenamento jurídico interno (Nunes, 2018).

Segundo o sumário da referida Lei do Cibercrime, a respetiva aprovação legislativa interna, permitiu a transposição "*...para a ordem jurídica interna da Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de fevereiro, relativa a ataques contra sistemas de informação, e adaptando o direito interno à Convenção sobre Cibercrime do Conselho*

[20] Não olvidando que o saldo bancário de uma conta à ordem, pode, na maior parte das vezes, conter valores muito superiores aos dos plafonds concedidos a muitos dos cartões de crédito emitidos.

da Europa...". O legislador europeu a partir desta altura parece ter despertado da aparente apatia legislativa, comum em toda a Europa em face de alguns fenómenos criminais fortemente enraizados, e outros, emergentes. A Convenção de Budapeste, demonstrou igualmente, de forma inequívoca, que os países aderentes, não terão ficado indiferentes aos enormes e rápidos avanços tecnológicos, operados ao nível das Novas Tecnologias de Informação e Comunicação.

A possibilidade concreta de já nessa altura, através da internet, por via *"online"*, ser possível o envio de enormes volumes de dados, sob as mais variadas formas, máxime de voz, texto, música e imagens - estática e móveis[21], se ter tornado uma realidade, demonstrava ainda que de uma forma algo temerosa, as enormes potencialidades destas Novas Tecnologias de Informação e Comunicação. A acrescer a todas estas novas valências verificava-se igualmente a particularidade de inexistirem quaisquer obstáculos ou dificuldades acrescidas no respetivo acesso. Muito pelo contrário, o acesso à quase ilimitada informação contida nos sistemas informáticos encontrava-se completamente acessível. No entanto, a rápida transmissão e partilha desse conhecimento, acrescida da ausência de quaisquer fronteiras físicas ou digitais colocou por outro lado, os Estados perante uma enorme pressão.

As Novas Tecnologias de Informação e Comunicação, colocaram em evidência, de certa forma, não só as vulnerabilidades dos Estados em lidarem com todos estes novos fenómenos associados mas, acima de tudo, impuseram-lhes a necessidade de se defenderem de uma nova panóplia de novos comportamentos alguns suscetíveis de censura penal tendo em conta a mais do que evidente demonstração da possível danosidade que os mesmos seriam suscetíveis de causar, em diferentes planos, nomeadamente, a nível pessoal, social e patrimonial.

Além do mais, a Lei da Criminalidade Informática, publicada em 1991, demonstrava, há já algum tempo, uma certa incapacidade em acompanhar as muitas modificações produzidas ao nível da criminalidade informática moderna explicável maioritariamente pela capacidade tendencialmente dinâmica e extremamente criativa de novas formas de criminalidade (Verdelho, Gouveia, & Santos, Enciclopédia de direito e segurança, 2015, p. 255)

Os estados que ratificaram a Convenção de Budapeste são através desse instrumento de Direito Internacional Público, exortados a adotar mecanismos legais ao nível do seu direito interno suscetíveis de por um lado acompanhar os diversos avanços

[21] **Cibercrime, s.d., p**onto 2, acedido em16 de setembro de 2018.

tecnológicos entretanto verificados, e por outro, obstar a que os mesmos possam ser utilizados de forma incorreta, lesando interesses legalmente protegidos (Cibercrime, s.d.)[22].

A Lei do Cibercrime deverá assim, ser entendida como um novo instrumento legal, adequado à punição de todos os comportamentos, *"em que o elemento digital surge como parte integrador do tipo legal, ou mesmo como seu objeto de proteção"* (Venâncio, 2011, p. 17).

As Novas Tecnologias de Informação e Comunicação, trouxeram, sem dúvida, inúmeras vantagens à vida em sociedade, mormente a facilidade e rapidez na obtenção ou remessa de informação, na eliminação de diversos constrangimentos que se verificavam nas comunicações à distância designadamente, os elevados preços praticados antes da possibilidade em efetuarem-se chamadas de voz através da Internet[23] a proliferação de novos conteúdos e oportunidades de negócio, a criação de novos empregos, e muito mais.

No entanto, juntamente com estas inovações tecnológicas (Verdelho, 2009, p. 715), advieram igualmente novos fenómenos criminais.

Alguns em resultado do elevado interesse e uma quase ou total dedicação depositada pelos respetivos autores nos propósitos delinquentes específicos deste segmento criminal, extraordinariamente diferenciado.

Naturalmente, verificaram-se distintos aprimoramentos em certos tipos legais de crimes já previstos na revogada Lei da Criminalidade Informática e outros mais recentes, que já na vigência da referida Lei 109/91, de 17 de agosto exigiam por parte da jurisprudência um enorme esforço de acompanhamento no sentido de impedir a verificação de eventuais situações passíveis de se reconduzirem a vazios legais.

A exemplo do que se referiu, durante todos estes últimos anos, foi o que sucedeu, relativamente aos autores de comportamentos criminosos, que após entrarem na posse dos dados bancários, inseridos nas bandas magnéticas de cartões de crédito as replicavam em bandas magnéticas de outros cartões de crédito emitidos por entidades competentes para o efeito e, portanto, legítimos, efetuando em seguida pagamentos com os mesmos.

A Novas Tecnologias de Informação e Comunicação, permitiram, no entanto, o surgimento de verdadeiras Organizações Criminosas as quais por sua vez admitiram o ingresso nas suas fileiras de autênticos "especialistas" do crime.

---

[22] Ponto 9, Acesso em: 23 de setembro de 2018.

[23] Também denominadas por VOIP, derivado do inglês *Voice over IP*, que significa a utilização da internet para o envio de dados de voz.

O denominado "Crime-as-a-Service"[24], consiste numa moderna classificação de especiais competências ao nível das Novas Tecnologias de Informação e Comunicação, que designam a especialização de um conjunto, muito específico de indivíduos, que mediante um preço, produzem desde programas maliciosos, para serem utilizados em ataques informáticos a empresas, bancos, ou, ao fabrico de dispositivos aptos à cópia dos dados bancários inseridos nas bandas magnéticas de todos os cartões bancários de pagamento.

Este novo modelo de criminalidade, o "*CaaS*", fornece e permite o fácil acesso a ferramentas e serviços transversais a todo o espectro da cibercriminalidade permitindo por esse meio que tais serviços possam ser colocados à disposição dos agentes com níveis de conhecimentos criminais muito baixos ou intermédios, escalando para outros eventualmente com conhecimentos de topo.

O *"CaaS*" permite igualmente, o acesso a um tipo de ferramentas que podem ser utilizadas por outros atores deste palco criminal, mormente os mais radicais, como *"Hacktivistas"* (Antunes & Rodrigues, 2018, p. 116)[25] ou inclusivamente, terroristas.

Esta nova prestação de serviços, permite aos atuais cibercriminosos, ainda que os respetivos níveis de conhecimentos criminais se situem em patamares primários, possam realizar ataques sobredimensionados e de uma escala desproporcional à sua capacidade técnica.

A utilização destes meios tecnológicos na prática destes crimes encontram-se amplamente referenciados, de forma bastante detalhada, nos relatórios da Europol: SOCTA (Serious and Organized Crime Threat Assessment) e IOCTA (Internet Organized Crime Threat Assessment)[26].

Esses relatórios anuais dão conta que todos os anos, são lançados ciberataques de âmbito e escala sem precedentes, chamando ainda a atenção dos Estados para ameaças anteriormente subestimadas, designadamente fraudes operadas na área das telecomunicações, as quais colocam em evidência a necessidade de uma maior adaptação e desenvolvimento constantes a levar a cabo pelas autoridades dos respetivos países[27].

---

[24] Vulgarmente designado pelo acrónimo de CaaS.

[25] Derivação do termo hacking com o termo ativismo, o qual designa um conjunto de comportamentos, normalmente ilícitas, com o propósito de promoção de certa ideologia.

[26] O relatório SOCTA está disponível em https://www.europol.europa.eu/activities-services/main-reports/serious-and-organised-crime-threat-assessment e o IOCTA em https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018. No Relatório SERIOUS AND ORGANISED CRIME THREAT ASSESSMENT (SOCTA), European Union Organised Crime Report, ano de 2017, p. 29.

[27] *Ibidem*

Pouco depois do virar de século[28], este tipo de condutas e respetivas organizações criminosas que a suportam, já eram devidamente acompanhadas pela EUROPOL[29].

Fóruns e mercados criminosos dentro da *"Deep Web"*[30] ou a *"Darknet"* (Antunes & Rodrigues, 2018, p. 220)[31] continuam a ser um ambiente crucial para os estes cibercriminosos comunicarem, sendo por isso, uma componente chave para o *"CaaS"*.

Todos estes fatores permitiram integrar novos membros em certos grupos criminosos os quais puderam assim adicionar um conjunto de novos ingredientes, aos antigos e mais recentes crimes exequíveis através destas novas tecnologias e designadamente, acrescentaram maiores dificuldades na deteção em tempo útil da ocorrência da prática desses crimes, e por outro, a localização e detenção dos respetivos autores.

Nesta nova realidade, salientam-se as distintas caraterísticas das demais temáticas criminais, designadamente a possibilidade de anonimização dessas atuações e a faculdade concedida a quem pratica um certo crime, de poder-se encontrar localizado em qualquer parte do globo.

A existência de crimes cometidos por intermédio de um computador ou até por um sistema informático não os reconduzem forçosamente a uma possível categoria especial distinta do ponto de vista dogmático dos demais crimes, apenas porque foram praticados por essa via (Verdelho, 2003, p. 349).

---

[28] Cf. Relatório da EUROPOL, SERIOUS AND ORGANISED CRIME THREAT ASSESSMENT (SOCTA), European Union Organised Crime Report, dezembro de 2004, Disponível em <https://www.europol.europa.eu/activities-services/main-reports/serious-and-organised-crime-threat-assessment#fndtn-tabs-0-bottom-2>, p. 8, acedido em 28 de dezembro de 2018.

[29] Europol é a agência da União Europeia (UE) responsável por garantir o cumprimento da lei. Sediada em Haia, Holanda, presta apoio aos 28 Estados-Membros da União no âmbito da luta contra as formas graves de criminalidade internacional e de terrorismo. Colabora igualmente com muitos países terceiros e organizações internacionais.

[30] Consiste numa zona da internet, fora das áreas pesquisáveis com os correntes motores de busca. Só é acessível com Browsers específicos como por exemplo o TOR, que de entre muitas valências, se destaca a completa anonimização aquando da navegação.

[31] Corresponde a uma parte da Deep Web, constituída por redes privadas, cujo objetivo, através da anonimização, consiste em se transacionarem diversos conteúdos, maioritariamente ilegais.

4. O "SKIMMING" E O "CARDING"

As expressões anglo-saxónicas denominadas por "Skimming" e "Carding", designam técnicas ilícitas ou, dito de uma outra maneira, constituem modos de atuação criminosos, que estão na génese da prática de alguns dos comportamentos suscetíveis de integrar o tipo legal previsto na Lei do Cibercrime, mormente o de Falsidade Informática, previsto no art.º 3.º.

O *"Skimming"*[32], compreende a atividade levada a cabo por agentes que intencionalmente, procedem à instalação de forma tendencialmente dissimulada em caixas automáticas ou, em terminais de pagamento eletrónico disponibilizados por comerciantes, de dispositivos de pequenas dimensões com a capacidade de procederem à cópia e posterior gravação dos dados inseridos nas bandas magnéticas dos cartões bancários (Guimarães, 2013, p. 587)[33] que aí são introduzidos (Antunes & Rodrigues, 2018, p. 109).

Por outro lado, o *"Carding"*, consistirá no comportamento delinquente, que tem lugar no momento subsequente à obtenção ilícita dos dados bancários inseridos nas bandas magnéticas dos cartões bancários que são alvo da referida técnica de *"Skimming"*.

Posteriormente, esses dados bancários capturados por esse meio são inseridos[34] em outros cartões bancários indiferentemente da respetiva instituição de crédito responsável pela sua emissão.

Na maioria das vezes, os titulares dos cartões bancários alvo deste esquema criminoso, apenas tomam conhecimento da fraude de que foram vítimas em momento posterior à data dos factos, ou seja, somente após consulta do respetivo saldo bancário associado ao cartão cujos elementos foram comprometidos[35] ou, quando a instituição de crédito emissora desse cartão, procede ao envio do respetivo extrato associado[36].

A técnica de "Skimming", na esmagadora maioria das vezes em que vem a ser detetada designadamente com a apreensão dos respetivos instrumentos utilizados, consiste na instalação dos mencionados dispositivos de captura dos dados inseridos nas bandas magnéticas dos cartões bancários completamente dissimulados em caixas automáticos ou nos mecanismos de abertura que permitem o acesso ao interior de

---

[32] Cf. Relatório da EUROPOL, SERIOUS AND ORGANISED CRIME THREAT ASSESSMENT (SOCTA), European Union Organised Crime Report, dezembro de 2004, Disponível em <https://www.europol.europa.eu/activities-services/main-reports/serious-and-organised-crime-threat-assessment#fndtn-tabs-0-bottom-2>, p. 13, acedido em 28 de dezembro de 2018

[33] Cartões de pagamento, ou seja, de crédito ou de débito.

[34] Mormente, através da regravação da respetiva banda magnética.

[35] Se, no caso concreto, estarem em causa cartões de débito.

[36] Quando se está na presença de cartões de crédito.

instalações bancárias (Antunes & Rodrigues, 2018, p. 111), juntamente, com microcâmaras, colocadas de forma estratégica a incidirem sobre o teclado de forma a permitirem a gravação da imagem gerada pela introdução do código secreto pelo legítimo titular do cartão[37/38].

Este tipo de atuações criminosas, implicam, necessariamente a criação de verdadeiras estruturas de criminalidade organizada com alcance transnacional.

Pouco depois do virar de século[39] este tipo de condutas e respetivas organizações criminosas que a suportam já eram devidamente acompanhadas pela EUROPOL.

Este tipo de criminalidade informática, já no ano de 2004, havia sido categorizada pela EUROPOL, enquanto crime organizado e os respetivos autores integrados em Grupos de Criminalidade Organizada [40].

Nessa altura, no âmbito deste tipo de criminalidade que incide sobre a fraude subjacente aos cartões bancários, foram, rapidamente identificados grupos criminosos, constituídos por indivíduos oriundos da China e Malásia, a atuarem em solo Americano.

Estes grupos criminosos, adquiriam no mercado negro mediante pagamento, os dados relativos a cartões bancários[41] ilegitimamente copiados, os quais, em momento posterior, seriam duplicados noutros cartões servindo-se desses para a posterior aquisição de diversos bens de luxo que, comercializados no mercado negro eram convertidos em avultadas quantias monetárias[42].

Foram igualmente identificados grupos de criminalidade organizada, cujas respetivas fileiras, eram alimentadas por indivíduos de nacionalidade Romena e Búlgara[43]. Estes agentes dedicar-se-iam à prática de inúmeros comportamentos subsumíveis a diversos

---

37 *Ibidem*, p. 113.

38 Cf. Relatório da EUROPOL, SERIOUS AND ORGANISED CRIME THREAT ASSESSMENT (SOCTA), European Union Organised Crime Report, 17 de novembro de 2005, Disponível em <https://www.europol.europa.eu/activities-services/main-reports/serious-and-organised-crime-threat-assessment#fndtn-tabs-0-bottom-2>, p. 19, acedido em 30 de dezembro de 2018.

39 Cf. Relatório da EUROPOL, SERIOUS AND ORGANISED CRIME THREAT ASSESSMENT (SOCTA), European Union Organised Crime Report, dezembro de 2004, Disponível em <https://www.europol.europa.eu/activities-services/main-reports/serious-and-organised-crime-threat-assessment#fndtn-tabs-0-bottom-2>, p. 8, acedido em 28 de dezembro de 2018.

40 Cf. Relatório da EUROPOL, SERIOUS AND ORGANISED CRIME THREAT ASSESSMENT (SOCTA), European Union Organised Crime Report, dezembro de 2004, Disponível em <https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment-2017>, p. 32, acedido em 29 de dezembro de 2018.

41 Cartões de crédito e débito.

42 Cf. Relatório da EUROPOL, SERIOUS AND ORGANISED CRIME THREAT ASSESSMENT (SOCTA), European Union Organised Crime Report, dezembro de 2004, Disponível em <https://www.europol.europa.eu/activities-services/main-reports/serious-and-organised-crime-threat-assessment#fndtn-tabs-0-bottom-2>, p. 8, acedido em 28 de dezembro de 2018.

43 Cf. Relatório da EUROPOL, SERIOUS AND ORGANISED CRIME THREAT ASSESSMENT (SOCTA), European Union Organised Crime Report, dezembro de 2004, Disponível em <https://www.europol.europa.eu/activities-services/main-reports/serious-and-organised-crime-threat-assessment#fndtn-tabs-0-bottom-2>, p. 9, acedido em 28 de dezembro de 2018.

tipos legais de crimes de entre os quais comportamentos relacionados com a fraude com cartões de débito[44/45].

O exponente crescimento deste tipo de criminalidade teve por base diversos fatores designadamente o crescimento tecnológico incrementado pelas Novas Tecnologias de Informação e Comunicação[46].

5. A FALSIDADE INFORMÁTICA NA LEI DO CIBERCRIME

A Lei do Cibercrime, como já atrás se havia referido alterou em muito toda a previsão normativa plasmada na revogada Lei da Criminalidade Informática, a Lei 109/91, de 17 de agosto, cujo *"ratio legis"* advém da Recomendação n.º R (89) 9 do Conselho da Europa, de 13/9, a qual se propunha nessa altura definir e punir, comportamentos que designou por crimes informáticos (Verdelho, 2009, p. 717).

A Lei do Cibercrime, para além de criar novos tipos de crime, dirigidos às novas formas de criminalidade, inexistentes no ano da publicação da Lei da Criminalidade Informática, ou seja, 1991, introduziu igualmente, no ordenamento jurídico nacional, normas processuais específicas desta área, destacadas do Código Processo Penal (*Ibidem*, p. 718).

De entre as muitas alterações introduzidas pela Lei do Cibercrime, iremos destacar as operadas ao nível da previsão do crime de Falsidade Informática, o qual, na revogada Lei da Criminalidade Informática, constava no artigo 4.º [47].

A Lei do Cibercrime, não só modificou substancialmente toda a estrutura deste ilícito criminal como o inscreveu enquanto primeiro ilícito desta nova Lei, alterando-o igualmente em termos de numeração, passando a Falsidade Informática atualmente a constar como o respetivo artigo 3.º.

---

44 *Ibidem*, pp. 8-10.

45 Salienta-se que ao logo deste Relatório SOCTA, não é feita qualquer distinção entre a fraude cometida com recurso aos dados de cartões de crédito ou de débito, ou seja, os intentos criminosos subjacentes à prática destes crimes é exatamente o mesmo.

46 Cf. Relatório da EUROPOL, SERIOUS AND ORGANISED CRIME THREAT ASSESSMENT (SOCTA), European Union Organised Crime Report, ano de 2006, Disponível em <https://www.europol.europa.eu/activities-services/main-reports/serious-and-organised-crime-threat-assessment#fndtn-tabs-0-bottom-2>, p. 18, acedido em 30 de dezembro de 2018.

47 **Artigo 4.º**

Falsidade informática

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 dados, quando esses dados ou programas sejam susceptíveis 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 objecto dos actos referidos no número anterior, actuando 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.

Estas alterações, surgem como uma adaptação reativa do legislador, às novas tendências e atuações ilícitas, que há data da publicação da Lei da Criminalidade Informática, 1991, eram totalmente desconhecidas (Verdelho 2009, p. 724).

O artigo 3.º da Lei do Cibercrime, passou assim a ter uma nova redação, completamente inovadora e, sobretudo atual, que passou a prever a punição de um conjunto de antigos e novos comportamentos criminosos[48].

Dessas modificações, salientamos as introduzidas no atual n.º 2, do mencionado art.º 3.º da Lei do Cibercrime.

Aí, o legislador previu comportamentos criminosos que salvo melhor opinião, se subsumem aos já referidos modos de atuação denominados por *"Skimming"* e que posteriormente resultam num outro, o *"Carding"*

Repare-se que por outro lado, o legislador faz questão em tipificar esses comportamentos sem, no entanto, introduzir na norma qualquer distinção entre cartões de débito e cartões de crédito, referindo-se a esses meios de pagamento como "*cartão bancário de pagamento..."* pretendendo, e em nosso entender, de forma cristalina, fazer a inclusão neste preceito legal, necessariamente, dos cartões de crédito (*Ibidem, p. 724*).

Por outro lado, fazendo-se apelo às regras de interpretação em direito, a Lei do Cibercrime é clara, referindo-se a cartões bancários de pagamento, de modo abrangente.

Por outro lado, parece-nos óbvia a "*ratio legis"* da Lei do Cibercrime neste ponto em particular, pois de entre todos os Estados Membros que ratificaram a Convenção de Budapeste, e que posteriormente a transpuseram para os respetivos ordenamentos jurídicos, Portugal, foi o único que tipificou esta previsão normativa[49].

---

[48] **Artigo 3.º**

Falsidade informática

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 acções 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, actuando 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 objecto dos actos referidos no n.º 1 ou cartão ou outro dispositivo no qual se encontrem registados ou incorporados os dados objecto dos actos referidos no número anterior, é punido com as penas previstas num e noutro número, respectivamente.

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 acções 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.

[49] De acordo com esclarecimento obtidos em sede de entrevista individual mantida com o Dr. Pedro Verdelho, Procurador da República e Diretor do Gabinete Cibercrime do Ministério Público, o qual fez parte do plantel de juristas que criaram a Lei do Cibercrime.

Não obstante tanto o "Carding" como "Skimming" serem igualmente puníveis nas respetivas legislações penais dos demais Estados Membros que ratificaram a Convenção de Budapeste, o certo é que tais normas não foram inscritas nas respetivas Leis do Cibercrime.

Esse facto em nossa modesta perspetiva vem assim reforçar de forma inequívoca que a redação conferida ao artigo 3.º da Lei do Cibercrime, foi intencionalmente pensada de forma a incluir todos os cartões bancários de pagamento onde necessariamente se incluem os cartões de crédito[50].

O Legislador, prudentemente, e antes da feitura da Lei do Cibercrime, diligenciou por auscultar inúmeros especialistas da área de investigação e respetivo combate ao Cibercrime[51], vindo por esse meio a Lei do Cibercrime a beneficiar de preciosos contributos. Não existindo por esse motivo no nosso espírito qualquer dúvida quanto à razão de ser da previsão do n.º 2, muito menos o sentido e alcance da expressão "*Quando as acções descritas no número anterior incidirem sobre os dados registados ou incorporados em cartão bancário de pagamento...*"

Após atenta análise da hermenêutica subjacente à feitura da Lei do Cibercrime, tudo indica que o Legislador teve em conta as mesmas preocupações já presentes nas suas fontes originárias nomeadamente, a Convenção de Budapeste.

Salienta-se o enorme cuidado depositado em toda a exposição de conceitos que não obstante essa descrição encerrar um elevado rigor jurídico houve igualmente a preocupação de que os mesmos se traduzissem em noções, tecnologicamente neutrais, permitindo-se a sua sobrevivência e respetiva adaptação, a novas evoluções tecnológicas que necessariamente nos serão trazidas futuramente (Verdelho, Gouveia, & Santos, 2015, p. 256).

A exemplo do que se referiu, veja-se o caso do conceito de sistema informático previsto na Lei do Cibercrime, inspirado na Convenção de Budapeste que recorde-se foi ratificada por Portugal em 23/11/2001 e que por maioria de razão pensado em data anterior a 2001, conseguiu ao longo de todos esses anos e até aos dias de hoje manter uma atualidade notável uma vez que na atual Lei do Cibercrime essa noção inclui, sem qualquer dúvida os modernos *tablets* ou *smartphones* que há altura a sua idealização e respetiva conceção, não eram sequer imagináveis (Ibidem).

Do exposto, e tendo em conta todos os cuidados demonstrados pelo Legislador de 2009, mormente no rigor dos termos utilizados, na antecipação da possibilidade de

[50] Nesse sentido, igualmente (Verdelho, Gouveia, & Santos, 2015, p. 257) e (Verdelho, 2009, p. 724).

[51] Nomeadamente, o atual Diretor do Gabinete Cibercrime do Ministério Público, Procurador da República, Dr. Pedro Verdelho.

tais termos intencionalmente neutros poderem manter-se atuais durante muitos anos em face da evolução tecnológica e da constante diversificação criativa das técnicas levadas a cabo pelos autores nestas áreas de crime, permite-nos concluir com toda a segurança que o tipo legal previsto no artigo 3.º da Lei do Cibercrime, a Falsidade Informática, tem em vista a punição dos comportamentos subsumíveis ao modo de atuação criminoso denominado por *"Carding"* e o *"Skimming"*.

Pelo que se expôs, defendemos, que a norma enunciada no número 2 do tipo legal de Falsidade Informática, prevê a punição de todos os comportamentos que provoquem a interferência e subsequente captura dos elementos inseridos nas bandas magnéticas de todos os cartões bancários atualmente em vigor no sistema bancário português noção que nos é avançada pelo supervisor bancário nacional[52], na qual estão compreendidos os cartões de débito e de crédito.

Tem razão por esse motivo Pedro Verdelho (Albuquerque & Verdelho, 2010, p. 506), nas suas considerações à anotação do artigo relativo à Falsidade Informática constante na Lei do Cibercrime nomeadamente quando refere que a norma descrita no respetivo n.º 2, prevê a incriminação da Falsidade Informática que incida sobre os dados inseridos nas bandas magnéticas de cartões bancários indiferentemente destes se tratarem de cartões de crédito ou de débito.

Este Ilustre Magistrado vai mais longe considerando que a norma em apreço, esgota, não só a necessidade, como o próprio sentido, da remissão prevista na alínea c), do n.º 1 do artigo 267.º, do Código Penal, pensamento, aliás, com o qual concordamos na íntegra[53], pelas razões que a seguir se descrevem;

Tal como já tivemos ocasião de referir ao longo da presente dissertação, é nossa convicção que na mente do legislador, na redação dada ao Dec. Lei n.º 48/95, de 15 de março, que introduziu as alterações ao artigo 267.º do Código Penal equiparando a moeda o cartão de crédito e o cartão de garantia, o propósito era a punição do fabrico integral do plástico e respetivos elementos em relevo de ambos os cartões em vigor no longínquo ano de 1995.

O uso dessas contrafações, provocava necessariamente o engano nas relações jurídicas e causada danos patrimoniais e como de forma recorrente se tem lido na fundamentação de alguns recentes acórdãos, onde estas questões se têm vindo a

52 De acordo com a publicação disponível no sítio https://www.bportugal.pt/, 2018

53 Nesse sentido, igualmente, (Simas, 2014, p. 82).

colocar[54], a afetação do bem jurídico protegido pelo crime de contrafação de moeda, a qual se reconduz à "*intangibilidade do sistema monetário, incluindo a segurança e credibilidade do tráfego monetário*. *Tratando-se o cartão de crédito de moeda, tutelando aquele tipo legal a fiabilidade e confiança na circulação da moeda na versão moderna do chamado dinheiro de plástico"*[55].

Por outras palavras, a fundamentação atualmente defendida pelos Tribunais superiores, ao sustentarem a tese de que comportamentos, que impliquem a captura ilícita dos dados inseridos em bandas magnéticas dos cartões de crédito, constituem a prática do crime de Contrafação de Títulos Equiparados a Moeda, com base na remissão operada pela alínea c) do n.º 1, do artigo 267.º para o artigo 262.º, ambos do Código Penal, com o devido respeito, só fazia sentido, até à entrada em vigor da Lei do Cibercrime.

Importa salientar que, quando a mencionada norma constante na alínea c) do n.º 1, do artigo 267.º do Código Penal, foi introduzida[56], o respetivo período antecedente à discussão dessas alterações mormente a realidade do sistema bancário de então, quando comparado com o atual, era completamente diferente.

Desde logo na tecnologia e mecanismos de segurança, entretanto implementados, ao longo de todos estes anos, na produção do próprio cartão de crédito.

Naquela altura, em inícios dos anos noventa, a credibilidade conferida à utilização do cartão de crédito ou de garantia no comércio, bastava-se com os elementos em relevo nos respetivos cartões, e a própria aparência desses cartões.

Dessa forma, contrafações que mantivessem um grau mínimo de semelhança com legítimos cartões de crédito ou de garantia, seriam suficientes para produzir o engano nas relações jurídicas.

O primeiro, recorde-se, interagia com um mecanismo manual, designado por máquina de impressão monográfica idêntica a um "ferro de engomar", e o segundo, mediante a mera exibição ao comerciante, juntamente com o cheque com o qual se propunha garantir provisão.

Ambos partilhavam, no entanto, o facto de não carecerem de qualquer interação com quaisquer dispositivos ou sistema eletrónicos, que atualmente, se encontram

---

[54] Designadamente, e título de exemplo, o acórdão do Tribunal da Relação de Lisboa de 30-06-2011, processo nº: 189/09.3JASTB.L1-5.

[55] *Ibidem*

[56] Recorde-se que tal terá sucedido pelas alterações introduzidas pelo Dec. Lei n.º 48/95, de 15 de Março.

perfeitamente implementados em todo o sistema bancário, bem como no comércio[57/58].

No entanto, desde essa data - 1995, até à entrada em vigor da Lei do Cibercrime - 2009, o cartão de garantia foi, entretanto, retirado do sistema bancário.

Por outro lado, o cartão de crédito passou a incorporar diversos elementos de segurança, os quais não só vieram reforçar como tornaram completamente inútil, do ponto de vista criminoso, a respetiva contrafação.

Referimo-nos à introdução da banda magnética, no fabrico do plástico dos cartões de crédito.

Nessa banda magnética, as instituições de crédito responsáveis pela emissão dos respetivos cartões, passaram a introduzir um conjunto de elementos bancários, permitindo por esse meio, a inequívoca individualização do respetivo cartão.

Com esta nova tecnologia de segurança introduzida nos cartões de crédito, garantiu-se dessa forma a total autenticidade subjacente a todas as transações em que esses cartões fossem utilizados uma vez que se impôs que a banda magnética para a respetiva validação da transação interagisse com os dispositivos eletrónicos de pagamento ou levantamento que passaram a estar disponíveis no mercado[59].

Assim, qualquer contrafação direcionada especificamente ao plástico do cartão de crédito, ainda que nele se apusesse uma banda magnética, por forma a conferir-se uma maior credibilidade à respetiva aparência de legitimidade, colidia, inevitavelmente, com a barreira tecnológica que decorria da ausência dos dados previamente inseridos na banda magnética, pela entidade emissora desse cartão.

No entanto, já no final no primeiro trimestre do ano de 1999 (Rodrigues B. M., março de 1999), se havia dado conta que o ordenamento jurídico nacional era pioneiro nesta matéria, contrariamente ao que sucedia em outros países da Europa, nos quais, a contrafação de cartões de crédito não era sequer punível por inexistência de Lei prévia.

Por outro lado em balanço entretanto realizado tomou-se consciência de que não obstante todo o investimento nomeadamente nos avanços tecnológicos levados a cabo

---

57 Nomeadamente, com a disponibilização aos clientes de POS.

58 Nesse mesmo sentido, A. M. Almeida Costa na anotação ao art. 267.º em (Dias, et al., 1999, p. 812), que para distinguir os cartões de crédito e garantia enquanto títulos de crédito dos demais cartões, refere o seguinte: *"Fora do âmbito de previsão da norma encontram-se os chamados cartões de debito, categoria que inclui, por exemplo, o vulgar "cartão multibanco". Estes funcionam on line, sem a intermediação de um terceiro no processo de pagamento (v. g., de uma instituição de crédito), envolvendo as operações de compra com eles efectuadas a subtração imediata dos montantes na conta bancaria do titular. Por isso, as suas falsificações e subsequente utilização consubstanciam, respetivamente, a preparação e a execução de um atentado directo ao património do titular do cartão de debito, reconduzível ao tipo legal do furto (art.º 202.º ss.)."*

59 Designadamente as ATM`s e POS

pela indústria ligada ao fabrico e segurança dos cartões bancários, o certo é que já se haviam sinalizado grupos criminosos a atuarem em alguns países europeus desde o ano de 1998, os quais detinham ligações a outros grupos criminosos oriundos de diversos países asiáticos (Rodrigues B. M., Março de 1999)[60], os quais lhes forneciam alguns dos instrumentos[61] da nova face do crime de contrafação de cartões de crédito e de débito, as quais se reconduziam, já nessa altura, às técnicas ilícitas hodiernamente denominadas por *"Carding"* e *"Skimming"* (Rodrigues B. M., Março de 1999).

Terá sido logo após esta constatação, ou seja, final do primeiro trimestre do ano de 1999, que estes modos de atuação criminosos, denominados por *"Carding"* e *"Skimming"*, terão finalmente chegado a solo nacional.

Porém, salienta-se que nesta data - 1999, e desde já há algum tempo a segurança entretanto implementada no fabrico dos cartões de crédito[62] tal como já havia sucedido com os cartões de débito, determinou que todas as transações em que os cartões de crédito fossem utilizados, teriam forçosamente de interagir com dispositivos ligados *"on line"* ao sistema bancário os quais validavam essas transações ou, por outro lado, impediam-nas, caso se tratassem de fraude.

Mas, uma vez mais, os agentes, engenhosamente, urdiram uma nova forma de contornarem estes mecanismos de segurança implementados nos cartões bancários, que haviam introduzido durante algum tempo, alguma confiança no mercado e no tráfego jurídico.

Com a introdução em solo nacional de todas estas novas técnicas ilícitas, os criminosos, maioritariamente estrangeiros, conceberam o que futuramente se concretizou, em termos criminais, num enorme flagelo, de difícil combate, que gerou gigantescos impactos negativos ao nível da banca nacional, bem como entre particulares. Circunstância aliás, que perdura até aos dias de hoje.

Por isso, compreende-se o alcance da anotação ao artigo 267.º por A. M. Almeida Costa (Dias, et al., 1999, pp. 812-815), que, já no ano de 1999, tentando acompanhar esta nova forma de criminalidade subjacente à manipulação ilícita do dinheiro de plástico, reconduziu a punição destes comportamentos, mas somente quando incidissem sobre os dados bancários inseridos nas bandas magnéticas de cartões de crédito, ao tipo legal constante do artigo 265.º do Código Penal, ou seja, a passagem de moeda falsa.

---

[60] Nomeadamente, Malásia, Ilha Formosa e China.

[61] Entre outros, elementos relativos a contas bancários ou a cartões, equipamentos informáticos e mecânicos para contrafação dos cartões (fabrico integral do plástico), software específico, cartões plásticos com banda magnética regraváveis, tiras com hologramas contrafeitas.

[62] Mormente a introdução da banda magnética e respetivos elementos bancários atinentes ao cartão.

Se tal esforço não tivesse sido desenvolvido, tanto por parte da doutrina, como pela jurisprudência, e tal desiderato não tivesse sido atingido, não teria sido possível lançar-se mão de uma solução legal que impedisse o impensável, ou seja, que tais comportamentos criminosos, pelo menos até à publicação da Lei do Cibercrime (setembro de 2009), não se reconduzissem a um qualquer tipo legal, com vista à respetiva sanção penal. Tal como já sucedia com alguns países Europeus, que em momento anterior à chegada a solo nacional deste fenómeno criminal, se debatiam com esse vazio legal, quando se tratava de punir os respetivos autores (Rodrigues B. M., março de 1999).

Porém, com a publicação da Lei do Cibercrime, e com a norma prevista o seu artigo 3.º, é clara a intenção do legislador, em pretender punir estes comportamentos subsumíveis, ao modo de atuação denominado por *"Carding"* ou por *"Skimming"*[63].

A Lei é clara, repare-se que o n.º 2 do artigo 3.º estatui que; "*Quando as acções descritas no número anterior incidirem sobre os dados registados ou incorporados em cartão bancário de pagamento...",* ou seja, o legislador quis, claramente, incluir neste preceito, todas as ações ilícitas que incidam sobre os dados incorporados nos cartões de débito ou crédito, ou seja, o *"Skimming"*.

Por outro lado, na norma reproduzida no n.º 1 do artigo 3.º, prevê que; "*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*...": Neste preceito, o legislador, claramente, pretende punir o *"Carding"*.

No entanto, e se dúvidas subsistissem, invocando-se por hipótese o facto dos documentos referidos na previsão da norma, se reconduzissem a simples documentos digitais, e não, a documentos corpóreos, existentes, portanto, no mundo físico, excluindo-se por essa via o cartão bancário, basta que o intérprete do Direito, recorra às elementares regras de interpretação de normas, em concreto, a interpretação sistemática do artigo na base da presente discussão.

No número 3, deste artigo, o legislador concretiza o seguinte; "*Quem, actuando 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 objecto dos*

[63] Que como já acima se referiu, irá depender se os criminosos apenas recolhem os dados inseridos nas bandas magnéticas dos cartões bancários, com recurso a um dispositivo denominado por skimmer. Perante essa hipótese, tratar-se-á de "Skimming". Se, por outro lado, usam esses dados de cartões bancários, para produzirem outros cartões, ainda que esses cartões hajam sido emitidos por entidades competentes, mas nas respetivas bandas magnéticas os autores irão replicar os dados bancários ilegitimamente obtidos, aí estaremos perante o "Carding".

actos referidos no n.º 1 ou cartão ou outro dispositivo no qual se encontrem registados ou incorporados os dados objecto dos actos referidos no número anterior...".

Em nossa modesta opinião, e perante o que se expôs, não subsistem quaisquer incertezas de que o crime de Falsidade Informática, constante da atual Lei do Cibercrime, contém a previsão e respetiva estatuição de diversos comportamentos criminosos, de entre os quais, se salientam aqueles modos de atuação, aos quais a Europol, em termos de taxonomia criminal, os designou por "*Carding"* e "*Skimming"*.

Importará, neste momento, salientar que hodiernamente, a utilização fraudulenta de um qualquer cartão bancário, em que o mesmo, seja fisicamente interveniente na transação em causa[64], apenas poderá ocorrer por uma das seguinte três formas a seguir se descrevem.

1.ª) Mediante a posse ilegítima do cartão alvo de fraude, designadamente pelo facto de sobre o seu legítimo titular, terem sido exercidas práticas criminosas, as quais implicassem a perda da posse do respetivo cartão, falamos, por hipótese, em crimes de furto ou roubo, ou, até uma eventual situação de achamento desse cartão bancário, por um terceiro, que, por falta do dever de cuidado do titular, havia manuscrito no verso o respetivo código.

2.ª) A utilização de um cartão legítimo, emitido por uma entidade autorizada para esse efeito[65], em que na respetiva banda magnética, após regravação, os criminosos, inserem os elementos bancários obtidos mediante o modo de atuação de *"Skimming"*.

3.ª) O uso de cartão, integralmente contrafeito, com referências a uma entidade bancária existente ou não[66], em que na respetiva banda magnética, são inseridos os dados bancários ilegitimamente obtidos, recorrendo, igualmente ao modo de atuação de *"Skimming"*.

No entanto, o método utilizado por estas redes criminosas de atuação nesta área de crime tão particular, optam, na esmagadoramente das vezes, pelo exemplo mencionado em segundo lugar, em detrimento do referido em terceiro.

O motivo é óbvio. A diminuição de custos, subjacente à desnecessidade em se contrafazerem cartões, e toda a respetiva logística inerente, e a inutilidade do aumento do

64 Excluímos, por ora, de forma intencional, a discussão subjacente à utilização dos dados de cartões bancários, ou seja a fraude de CNP (card not present).

65 Salienta-se que esse cartão, nem carece de ser um cartão bancário, ou seja, com todos os elementos de segurança que o caracterizam, mas um mero cartão plástico, que contenha uma simples banda magnética.

66 A única situação em que tal ocorreu em Portugal, tratavam-se de cartões estrangeiros, cf. acórdão do STJ, de 12-09-2012, Processo 1008/11.6JFLSB-L1.S1, ponto 6 e sgs.

risco de deteção desses cartões enquanto fraudulentos, quando exibidos perante comerciantes, ou, outras entidades a quem sejam apresentados, bem ainda, a desnecessária exposição dos criminosos perante terceiros.

Salienta-se igualmente que, num cartão bancário, legitimamente emitido pela entidade financeira competente, nas mãos deste tipo de criminosos, pode ser utilizado por diversas vezes, tendo em conta que, na respetiva banda magnética, existe a possibilidade técnica, de nela poderem vir a ser regravados diferentes elementos bancários, ilicitamente obtidos de distintos cartões bancários, por diversas vezes.

A fraude designada por CNP, ou "*card not present"*, designa um novo modo de atuação criminoso, que se caracteriza pelo uso dos dados relativos a cartões bancários[67], de forma ilegítima, no comércio eletrónico.

No entanto, e de acordo com os alertas, divulgados em diferentes anos, nos relatórios IOCTA[68], o *"Skimming"* mantém-se um problema constante na maioria dos Estados-membros da União Europeia.

Porém, no ano de 2018, constatou-se que o *"Skimming"*, mantendo a tendência de anos anteriores, tem vindo a diminuir, em razão das medidas implementadas pelos bancos, nomeadamente o bloqueio geográfico, que impedem assim que um cartão titulado por um cidadão de um certo Estado-membro, possa ser utilizado no estrangeiro, sem que para tal haja sido concedido prévio consentimento por parte do respetivo titular, junto do respetivo banco emissor.

É ainda nesse Relatório, dado conta que os dados obtidos através de *"Skimming"* são frequentemente vendidos na *"Darknet"*, que após replicação em simples cartões com banda magnética, são utilizados para o levantamento de somas em numerário, em regiões onde a implementação do Europay, Mastercard e Visa[69] ou é muito reduzida ou, totalmente inexistente designadamente, os Estados Unidos da América seguidos dos países asiáticos, como a China, Hong Kong, Indonésia, Malásia, Filipinas, Tailândia, e alguns países sul-americanos, como a Colômbia, República Dominicana, México e Peru.

---

67 O cartão em causa pode ser de crédito, débito ou dual.

68 O relatório IOCTA está disponível em https://www.europol.europa.eu/activities-services/main-reports/serious-and-organised-crime-threat-assessment.

69 Que implementou nos respetivos cartões bancários o sistema de segurança EMV.

6. A JURISPRUDÊNCIA DOS TRIBUNAIS PORTUGUESES NA PUNIÇÃO DOS COMPORTAMENTOS SUBSUMÍVEIS À NORMA DO ART. 3.º, N.º 3 DA LEI 109/2009, DE 15 SETEMBRO.

Os Tribunais Portugueses, em regra, quando chamados a pronunciarem-se relativamente aos factos descritos na acusação do Ministério Público, em que nas respetivas investigações por estes tituladas, estão em causa comportamentos criminosos, que em abstrato, se reconduzirão ao tipo legal de Falsidade Informática, da atual Lei do Cibercrime, demonstram alguma desconformidade entre decisões anteriores, proferidas por outros Tribunais, nas quais, em situações em tudo idênticas, acabam em condenações por tipos legais distintos.

No entanto, e para o acompanhamento destes fenómenos criminais, subjacentes às Novas Tecnologias de Informação e Comunicação, por Despacho de 7 de dezembro de 2011, o Procurador-Geral da República, criou o Gabinete do Cibercrime, cujas competências, consistem em coordenar a atividade do Ministério Público na área da Cibercriminalidade.

Este Gabinete tem sede na Procuradoria-Geral da República, e está dependente, hierarquicamente, do Procurador Geral da República.

Tem enquanto atribuições a coordenação interna do Ministério Público na área da cibercriminalidade, a formação específica nesta área de toda a magistratura[70], e a formalização de protocolos, envolvendo os diversos fornecedores de serviços de telecomunicações com vista à criação de canais específicos de comunicação entre estes e os magistrados titulares das investigações.

O Gabinete Cibercrime assegura a respetiva presença em todo território nacional, por intermédio de pontos de contacto, os quais são assegurados pela presença de pelo menos um magistrado, por cada uma das Comarcas.

Desde a data da sua criação, o Gabinete Cibercrime[71], tem realizado um esforço gigantesco, por forma a levar a cabo todas as suas atribuições.

Para além da celebração de diversos protocolos, mormente com provedores de serviços de telecomunicações, nacionais e estrangeiros, o mencionado Gabinete, criou uma página na internet[72], a qual se divide entre acessos livres, com conteúdos de grande

[70] A qual tem lugar em formações prestadas no Centro de Estudos Judiciários.

[71] Que desde a sua criação, em 7 de Dezembro de 2011, tem enquanto respetivo Coordenador, o Procurador da República, Dr. Pedro Verdelho.

[72] Referimo-nos ao URL http://cibercrime.ministeriopublico.pt/.

utilidade nesta temática, e uma outra, expressamente reservada a magistrados, onde são disponibilizadas informações e formulários confidenciais.

Na informação disponibilizada em acesso livre salienta-se a importância das notas práticas[73].

Nestas notas práticas do Gabinete Cibercrime, são divulgadas diversas orientações, com enorme interesse e utilidade para magistrados do Ministério Público que tenham em mãos inquéritos que para a respetiva instrução, necessitem de obter informações junto de diferentes entidades fornecedoras de serviços de telecomunicações e para as quais, tenham que cumprir um conjunto de formalidades, nomeadamente quanto ao canal de contacto a utilizar, e respetiva forma de o concretizar.

Até à presente data, o Gabinete Cibercrime já fez publicar, doze notas práticas, a primeira no ano de 2012, e a última, no ano de 2017.

Para a presente dissertação, a importância das notas práticas com os números 5, 9 e, 11, são de grande relevância, uma vez que nessas publicações, o Gabinete Cibercrime do Ministério Público, faz referência à jurisprudência de tribunais superiores sobre crimes informáticos e crimes cometidos por via de sistemas informáticos, após a entrada em vigor no ordenamento jurídico Português da Lei do Cibercrime.

Em todas essas notas práticas, cumulativamente ou, isoladamente, relativamente ao tipo legal de Falsidade Informática, são referenciados diversos acórdãos de tribunais superiores relacionados com Falsidade Informática.

De todo o universo respeitante a esses acórdãos, somente quatro[74], tratam a questão da utilização indevida dos dados inseridos em bandas magnéticas de cartões bancários, ilegitimamente obtidos e, posteriormente, replicados noutros cartões, com os quais é consumada a fraude.

Em todos esses acórdãos, não se verifica uma jurisprudência uniforme, que nos permita compreender o alcance da fundamentação subjacente às respetivas decisões, pese embora os *modi operandi* em causa nos diferentes acórdãos sejam distintos, mas todos, impliquem comportamentos criminosos que se subsumem à norma inscrita no artigo 3.º da Lei do Cibercrime – A Falsidade Informática. No entanto, os respetivos autores dos factos nos diferentes acórdãos, acabam condenados em concurso real, com o mencionado crime de A Falsidade Informática, com Burla Informática, ou com Contrafação de Títulos Equiparados a Moeda.

---

[73] Disponíveis para consulta em http://cibercrime.ministeriopublico.pt/notas-praticas.

[74] Todos, consultáveis no endereço www.dgsi.pt

Assim, e para uma melhor compreensão do problema em debate, optou-se por uma análise de cada um desses quatro acórdãos, por ordem cronológica.

Referimo-nos ao Acórdão do Tribunal da Relação de Lisboa, relativo ao processo 189/09.3JASTB.L1-5, de 30/06/2011, ao Acórdão do Tribunal da Relação de Lisboa, referente ao processo 7876/10.1JFLSB.L1-5, de 10/07/2012, ao Acórdão do Tribunal da Relação do Porto, atinente ao processo 1001/11.9JAPRT.P1, de 21-11-2012, e, por último, ao Acórdão do Tribunal da Relação do Porto, respeitante ao processo 2013/13.3JAPRT.P1, de 17-09-2014.

Relativamente ao primeiro acórdão de um Tribunal Superior, cujo respetiva decisão recaiu sobre factos suscetíveis de integrar o tipo legal de Falsidade Informática, da Lei do Cibercrime, ou seja, após a entrada em vigor desta nova Lei, em concreto o Acórdão do Tribunal da Relação de Lisboa, relativo ao processo 189/09.3JASTB.L1-5, de 30/06/2011, foi apreciado o recurso interposto por dois cidadãos Búlgaros que, em Dezembro de 2009, deslocaram-se para Portugal, devidamente instruídos por terceiros não identificados, e munidos dos respetivos instrumentos para a prática do crime de Falsidade Informática.

Estes condenados trouxeram com eles, designadamente, um teclado numérico, e, *"skimmers"*.

A função deste teclado numérico serviu o propósito de capturar o código secreto dos diversos cartões que operaram nas diversas máquinas ATM que vieram a ser comprometidas com este tipo de dispositivos. Foi instalado, de forma ilegítima, por cima dos normais teclados numéricos existentes nessas máquinas ATM e assim, habilmente dissimulado, substituindo desta forma a instalação dissimulada de uma microcâmara que iria gravar a inserção dos códigos secretos dos utilizadores daquele caixa automático.

Quanto ao *"skimmer"*, foi colocado na ranhura específica para a inserção dos cartões bancários, capturando e gravando, os respetivos dados bancários aí inseridos.

Todos estes comportamentos, permitem a concretização do já mencionado modo de atuação de *"Skimming"*.

Salienta-se que, ambos os arguidos, após a ilegítima captura dos dados bancários gravados em diversos cartões bancários[75], muito provavelmente, tê-los-ão enviado por via de correio eletrónico, para terceiros, atento ao lapso temporal decorrido entre a data da respetiva captura, em solo nacional, e a respetiva utilização desses dados, devidamente corporizados noutro cartão, que permitiram o levantamento de quantias em numerário em

75 Cartões de débito e de crédito.

caixas automáticas situadas em Alarcon - Espanha e em Nairobi - Quénia, em dias, imediatamente subsequentes.

Aos arguidos, tanto em sede de primeira instância, como neste Acórdão da Relação, que acabou por manter a decisão de primeira instância, acabaram condenados, respetivamente, pela prática dos seguintes crimes e penas:

- Ao arguido n.º 1, como coautor, pela prática de um crime de Falsidade Informática, na forma consumada, como reincidente, prevista e punida pelo artigo 3.º, n.º 1 e 2, da Lei n.º 109/2009, de 15/09, e, artigo 76.º, do Código Penal, na pena de três anos e seis meses de prisão, como coautor, pela prática de um crime de Falsidade Informática, na forma tentada, como reincidente, previsto e punido pelo artigo 3.º, n.º 1 e 2, da Lei n.º 109/2009, de 15/09, e artigos 22.º, 23.º, 73.º e 76.º do Código Penal, na pena de um ano e seis meses de prisão, como autor, pela prática de um crime de Falsificação de Documento[76], como reincidente, previsto e punido pelo artigo 256.º, n. º1, alíneas b) e e), e, 3, e artigo 76.º do Código Penal, na pena de dois anos de prisão, tendo-lhe sido aplicada a pena única de nove anos de prisão, após aplicação do respetivo cúmulo jurídico das penas.

- Ao arguido n.º 2, como coautor, pela prática de um crime de Contrafação de Moeda, como reincidente, previsto e punido pelo artigo 262.º, n.º 1, e 76.º do Código Penal, na pena de cinco anos de prisão, como coautor, pela prática de um crime de Falsidade Informática, na forma consumada, como reincidente, previsto e punido pelo artigo 3.º, números 1 e 2, da Lei n.º 109/2009, de 15/09, e 76.º, do Código Penal, na pena de três anos de prisão, como coautor, pela prática de um crime de Falsidade Informática, na forma tentada, como reincidente, previsto e punido pelo artigo 3.º, números 1 e 2, da Lei n.º 109/2009, de 15/09, e artigos 22.º, 23.º, 73.º e 76.º, todos do Código Penal, na pena de um ano de prisão, o que perfez, após aplicação do respetivo cúmulo jurídico das penas, a pena única de seis anos e seis meses de prisão.

Em nossa modesta opinião, e apenas quanto aos factos relacionados com a fraude subjacente à ilegítima apropriação dos elementos bancários inseridos em cartões bancários de terceiros, os arguidos, deveriam, assim, ser condenados somente pela prática de comportamentos que integrariam, em abstrato, o crime de Falsidade Informática, com base na previsão normativa espelhada no artigo 3.º, números 1 e 2, da Lei n.º 109/2009,

[76] Este arguido era portador de documentos de identificação falsos, alegadamente, emitidos pelas autoridades Búlgaras.

de 15/09, concretamente, pelo facto desses factos se reconduzirem ao já referenciado modo de atuação de *"Skimming"*.

Salienta-se, que neste Acórdão, e em concreto, quanto aos factos provados, não subsistem quaisquer dúvidas que os dados bancários ilegitimamente obtidos, e em momento posterior, replicados noutros cartões, com os quais a fraude foi entretanto consumada, ou seja, o modo de atuação de *"Carding",* não haviam sido cometidos pelos arguidos.

Porém, o coletivo de Juízes, neste Acórdão, optou por punir os arguidos pela prática do crime de Contrafação de Moeda, previsto e punido pelo artigo 262.º, n.º 1.

Pensamos que nesta decisão, como noutras que lhe seguiram, em que esta temática foi apreciada, não é levado em conta a especificidade deste tipo de criminalidade, nomeadamente, ao facto do já mencionado *"CaaS"*.

Senão, tomemos como exemplo estes factos e a presente decisão, e coloquemos a seguinte hipótese; se os arguidos, após os factos que praticaram, e que vieram a ser provados, ou seja, terem sido os autores da obtenção ilegítima dos dados bancários de cartões titulados por terceiros, se, em seguida, ao invés de os enviarem para os eventuais comparticipantes, como se passou neste caso concreto, os colocassem à venda, através de listagens, disponibilizadas na *"Darknet"*?

Esses elementos bancários comercializados dessa forma, seriam, posteriormente, adquiridos de forma perfeitamente anonimizada, e de seguida, replicados em cartões bancários, com os quais se consumava a fraude.

Seria admissível, que após a detenção desses autores do *"Carding"*, ainda que tal viesse a ocorrer em território nacional, e, em momento posterior, a respetiva investigação criminal, viesse a identificar os arguidos do presente Acórdão, enquanto autores do respetivo "Skimming" subjacente, e estes acabassem igualmente punidos pela prática da Falsidade Informática, em concreto pela norma prevista no artigo 3.º, n.º 3?

Entendemos, que a resposta será claramente negativa.

Ainda que a investigação, conseguisse demonstrar que os arguidos julgados neste Acórdão, haviam sido os autores do *"Skimming",* e, obviamente, ainda não tivessem sido julgados por esses factos, aí sim, ser-lhes-ia imputável o crime de Falsidade Informática, mas pela previsão constante no artigo 3.º, n.º 2.

É esta a nova realidade criminal, que carateriza o atual mundo digital, e que o Legislador português, através da Lei do Cibercrime, tentou antecipar, tendo, de forma deliberada, como já oportunamente referimos, criado termos, intencionalmente neutros,

com o intuito de os manter atuais e dinâmicos, em face da rapidez com que as redes criminosas operam e alteram os seus modos de atuação.

Todavia, esse desiderato, implica um esforço adicional, quer por parte da doutrina, quer por parte da jurisprudência.

Em nossa humilde opinião, tal como sucede com as demais Leis em geral, impõe-se ao aplicador da Lei, que não só conheça a Lei do Cibercrime, como igualmente o respetivo alcance nomeadamente, ao nível dos possíveis fenómenos subjacentes.

Só um perfeito domínio e conhecimento profundo destes novos fenómenos criminais implícitos nesta nova realidade por parte das Magistraturas, permitirá a boa realização da justiça nomeadamente, pela correta aplicação da Lei do Cibercrime, subsumindo aos respetivos tipos legais que a integram, todos os comportamentos suscetíveis de se reconduzirem à designada criminalidade informática.

E nesta segunda decisão, designadamente a referente ao Acórdão do Tribunal da Relação de Lisboa, relativo ao processo 7876/10.1JFLSB.L1-5, de 10/07/2012, é um exemplo do que atrás referimos.

Dois arguidos, ambos nacionais da República do Gana, vieram a ser localizados, e posteriormente detidos, pelas autoridades portuguesas, pelo uso ilegítimo de cartões bancários.

Tendo por base os factos provados em sede de audiência de discussão e julgamento, os cartões bancários utilizados pelos arguidos, não obstante se tratarem de cartões bancários legítimos, ou seja, terem sido emitidos pelas entidades financeiras competentes, nas respetivas bandas magnéticas, haviam sido inseridos dados bancários referentes a outros cartões[77].

Concluída a investigação, o Ministério Público, acusa os dois arguidos da prática dos seguintes crimes:

- Um crime de Contrafação e Passagem de Título Equiparado a Moeda Falsa, na forma continuada e consumada, previsto e punido pelos artigos 30.º, 262.º, n.º 1 e 265.º, n.º 1, alínea a), aplicável *ex* vi do artigo 267.º, n.º 1, alínea c), todos do Código Penal e artigo 151.º, da Lei n.º 23/2007, de 04/07.
- Um crime de Burla Informática, na forma continuada e consumada, previsto e punido pelos artigos 30.º, 221.º, n.ºs 1 e 5, alínea b), por

77 Que se apurou serem titulados por cidadãos dos Estados Unidos da América.

referência ao artigo 202.º, alínea b), todos do Código Penal e art. 151.º, da Lei n.º 23/2007, de 04/07.

- Um crime de Falsificação de Documento, na forma continuada e consumada, p. e p. pelo art. 256.º, n.º 1, alínea c), por referência à alínea a) do artigo 255.º, ambos do Código Penal e artigo 151.º, da Lei n.º 23/2007, de 04/07.
- Sendo que ao arguido A, ainda, da prática em autoria material e na forma consumada, de um crime de Falsificação de Documento, previsto e punido pelo art. 256.º, n.º 1, alíneas a), e) a f) a n.º 3, do Código Penal, por referência aos artigos 10.º, e 181.º da Lei n.º 23/2007, de 04.07, Regulamento (CE) n.º 539/2001, do Conselho, de 15.03.2001 a art.º 151.º, da Lei n.º 23/2007, de 04/07[78].

Porém, em sede de audiência de discussão e julgamento, o respetivo coletivo, tendo por base os factos provados, e chamando à colação[79] a anotação ao artigo 3.º da Lei do Cibercrime, efetuada pelo Procurador da República, Dr. Pedro Verdelho (Albuquerque & Verdelho, 2010, pp. 505-509), procede à alteração da qualificação jurídica dos factos, feita pelo Ministério Público, (Lobo, 2015, p. 693), reconduzindo os comportamentos ilícitos dos arguidos, relacionados com o uso indevido dos cartões bancários que lhe vieram a ser apreendidos, à seguinte decisão:

- Absolver os arguidos do crime de Contrafação e Passagem de Título Equiparado a Moeda Falsa de que estavam acusados.
- Absolver igualmente os arguidos do indicado crime de Burla Informática, previsto e punido pelos artigos 30.º, n.º 2, 221.º, n.ºs 1 e 5, alínea b), por referência ao artigo 202.º, alínea b), todos do Código Penal.

Os arguidos vieram assim a ser condenados pelos seguintes crimes e penas:

- Ao arguido A, pela prática, na forma continuada e consumada, de um crime de Falsidade Informática previsto e punido pelo artigo 3.º, n.ºs 1, 2 e 3 da Lei 109/2009, de 15 de Setembro e art. 30.º, n.º 2, do Código Penal, na pena de dois anos e anos e nove meses de prisão, pela prática, na forma continuada e consumada, de um crime de Burla Informática previsto e punido pelo artigo 221.º,

78 Este arguido, exibia no seu passaporte, um visto de entrada em Portugal, que após sujeição à respetiva perícia, determinou que o mesmo se tratava de uma contrafação.

79 Conforme citação de página 13 do mencionado acórdão.

n.º 1 e 30.º, n.º 2 do Código Penal na pena de um ano e nove meses de prisão., pela prática, na forma continuada e consumada, de um crime de Falsificação previsto e punido pelo artigo 256.º, n.º 1, alínea c) do Código Penal, na pena de um ano e nove meses de prisão, pela prática, na forma continuada e consumada, de um crime de falsificação previsto e punido pelo artigo 256.º, n.º 1, a), e) e f) e n.º 3 do Código Penal, na pena de dois anos de prisão.

- Em cúmulo jurídico, condenar o arguido A, na pena única de cinco anos de prisão.

- Ao arguido B, pela prática, na forma continuada e consumada, de um crime de falsidade informática previsto e punido pelo artigo 3.º, n.ºs 2 e 3 da Lei 109/2009, de 15 de Setembro e art. 30.º, n.º 2 do Código Penal, na pena de dois anos de prisão, pela prática, na forma continuada e consumada, de um crime de burla informática previsto e punido pelo artigo 221.º, n.º 1 e 30.º, n.º 2 do Código Penal, na pena de um ano e três meses de prisão, pela prática, na forma continuada e consumada, de um crime de falsificação previsto e punida pelo art. 256.º, n.º 1, alínea c) do Código Penal, na pena de um ano e três meses de prisão.
- Em cúmulo jurídico condenar o arguido B, na pena única de três anos de prisão.

Contudo, tanto o arguido A, como o Ministério Público, inconformados com os fundamentos dessa decisão, interpuseram recurso para o Tribunal da Relação de Lisboa.

Com base na análise dos factos, que vieram a ser provados em sede de decisão de primeira instância, o Juízes Desembargadores, decidiram alterar a condenação de ambos os arguidos, concedendo assim, parcial procedência do recurso interposto pelo Ministério Público, e, julgando improcedente o recurso interposto pelo arguido A.

Aos arguidos, foram-lhes imputados a prática dos seguinte crimes e penas de prisão:

- O arguido A, em substituição do crime de Falsidade Informática em que havia sido condenado em primeira Instância, acabou condenado pela prática de um crime de Contrafação de Moeda previsto e punido pelo artigo 262.º, n.º1, e 267.º, n.º1, alínea c), do Código Penal, e na pena de quatro anos e três meses de prisão, condená-lo, igualmente, pela prática de um crime de crime de Burla Informática previsto e punido pelo artigo 221.º, n.ºs 1 e 5 alínea a), com referência ao artigo 202.º, alínea b), todos do Código Penal, em substituição do crime de Burla Informática, na forma continuada, previsto e punido pelos artigos 221.º, n.º 1, e 30.º, n.º 2, do Código Penal, em que o havia sido condenado em primeira Instância, na pena de um ano e nove meses de prisão.

- Na reformulação das penas parciais, acabou condenado na pena única de cinco anos e seis meses de prisão.

- O arguido B, e em substituição do crime de Falsidade Informática em que havia sido condenado em primeira Instância, acabou condenado pela prática de um crime de passagem de Moeda Falsa previsto e punido no artigo 265.º, n.º 1, alínea a), por referência ao artigo 267.º, n.º 1, alíneas. c), todos do Código Penal, na pena de 2 anos de prisão, e, igualmente, pela prática de um crime de Burla Informática previsto e punido pelo art. 221.º, n.ºs 1 e 5 alíneas a), com referência ao artigo 202.º, alíneas b), todos do Código Penal, em substituição do crime de Burla Informática, na forma continuada, previsto e punido pelos artigos 221.º, n.º1, e 30.º, n.º 2, do Código Penal, no qual havia sido condenado em primeira Instância, na pena de um ano e três meses de prisão que lhe havia sido aplicada por aquela última infração.

  Na reformulação das penas parciais em que ficou condenado, foi-lhe mantida a pena única de 3 três anos de prisão.

Terá sido o Ministério Público que, nos fundamentos do recurso interposto para o Tribunal da Relação, quem suscitou a questão sobre o alcance do tipo legal escolhido pelo Tribunal de primeira Instância para a condenação dos arguidos pela prática do *"Carding"*, ou seja, a Falsidade Informática.

Realça-se deste facto, a circunstância de que terá sido o coletivo de juízes que presidiu ao julgamento em primeira Instância quem efetuou uma correta e atualista interpretação da Lei, em concreto da Lei do Cibercrime e mais, demonstrou conhecer a anotação à respetiva Lei por parte de Pedro Verdelho[80] (Albuquerque & Verdelho, 2010, pp. 505-509).

Foi o Ministério Público quem pôs em crise essa apreciação e respetiva decisão judicial, a qual teve enquanto consequência, a alteração do tipo legal em que ambos os arguidos haviam sido condenados, de Falsidade Informática, para o crime de Contrafação de Moeda.

Por outro lado, a condenação aplicada aos arguidos em sede de concurso efetivo, de Contrafação de Moeda, e, Burla Informática, com base no argumento do prejuízo causado

80 Conforme descrição no respetivo Acórdão, constante a página12.

pelos autores, no valor € 19.453,47, em nossa modesta opinião, e com o devido respeito, não faz o menor sentido.

Não seria desde logo esse o propósito dos autores, quando usaram os cartões bancários com as respetivas bandas magnéticas manipuladas?

Não era a apropriação ilegítima do património de terceiros?

Parece-nos evidente a resposta a essas perguntas, pelo que não se alcança a fundamentação para tal decisão.

O Acórdão do Tribunal da Relação do Porto, alusivo ao processo 1001/11.9JAPRT.P1, de 21/11/2012, tem enquanto objeto, o facto de três indivíduos, todos de nacionalidade Romena, após se deslocarem para o nosso país, no período compreendido entre os dias 08 e 09 de Junho de 2011, acabaram detidos pelas autoridades, e sujeitos à medida de coação de prisão preventiva, por factos relacionados com a utilização ilegítima de cartões bancários, e não bancários, cujos respetivos elementos bancários inseridos nas bandas magnéticas desses cartões, haviam sido ilegalmente manipulados.

Na acusação sustentada pelo Ministério Público, eram imputados a todos estes arguidos por factos suscetíveis de integrarem em abstrato em coautoria material e concurso real, a prática dos seguintes crimes:

- um crime de Associação Criminosa, previsto e punido pelo artigo 299.º, n.º 1 e 2, do Código Penal, um Crime de Contrafação de Moeda na forma continuada previsto e punido pelos artigos 262.º, n.º 1 e 267.º, n.º 1, alínea c) e 30.º, n.º 2, do Código Penal, um Crime de Passagem de Moeda Falsa, na forma continuada, previsto e punido pelos artigos 265.º, n.º 1, alínea a) e 267.º, n.º 1, alínea c) e 30.º, n.º 2, do Código Penal, um crime de Falsidade Informática, na forma continuada, previsto e punido pelos artigos 3.º, números 1 e 3, da Lei 109/2009 de 15 de Setembro, e 30.º, n.º 2, do Código Penal.

Porém, em sede de audiência de discussão e julgamento, os arguidos acabam condenados pela prática dos seguintes crimes e penas:

- O arguido B, pela prática, em coautoria material e concurso real, de um crime de Contrafação de Moeda, na forma continuada, previsto e punido pelo artigo 262.º, n.º 1, 267.º, n.º 1, alínea c), e 30.º, n.º 2, todos, do Código Penal, na pena de quatro anos de prisão, um crime de Passagem de Moeda Falsa, na forma continuada, previsto e punido pelos artigos 265.º, n.º 1, alínea a), 267.º, n.º 1, alínea c), e 30.º, n.º 2, todos, do Código Penal, na pena de dois anos de prisão, um crime de Falsidade Informática,

na forma continuada, previsto e punido pelos artigos 3.º, números 1 e 3 da Lei 109/2009 de 15 de Setembro, na pena de dois anos de prisão.

Em cúmulo jurídico, acabou condenado na pena única de cinco anos e seis meses de prisão.

- O arguido E, pela prática, em coautoria material e concurso real, de um crime de Contrafação de Moeda, na forma continuada, previsto e punido pelo artigo 262.º, n.º 1, 267.º, n.º 1, alínea c), e 30.º, n.º 2, do Código Penal, na pena de prisão de quatro anos de prisão, a um crime de Passagem de Moeda Falsa, na forma continuada, previsto e punido pelos artigos 265.º, n.º 1, alínea a), 267º, n.º 1, alínea c), e 30.º, n.º 2, do Código Penal, na pena de 2 dois anos de prisão, um crime de Falsidade Informática, na forma continuada, previsto e punido pelos artigos 3.º, n.º 1 e 3 da Lei 109/2009 de 15 de setembro, na pena de dois anos de prisão.

  Em cúmulo jurídico, foi condenado na pena única de 5 cinco anos e seis meses de prisão.
- O arguido H, pela prática, em coautoria material e concurso real, de um crime de Contrafação de Moeda, na forma continuada, previsto e punido pelo artigo 262.º, n.º 1, 267.º, n.º 1, alínea c), e 30.º, n.º 2, do Código Penal, na pena de prisão de quatro anos, e um crime de Passagem de Moeda Falsa, na forma continuada, previsto e punido pelos artigos 265.º, n.º 1, a), 267.º, n.º 1, alínea c), e 30.º, n.º 2, do Código Penal, na pena de dois anos de prisão, e um de Falsidade Informática, na forma continuada, previsto e punido pelo artigo 3.º, números 1 e 3 da Lei 109/2009 de 15 de setembro, na pena de dois anos de prisão.

  Em cúmulo jurídico, o mesmo foi condenado na pena única de 5 cinco anos e 6 seis meses de prisão.

De acordo com os factos provados na decisão proferida pelo Tribunal de primeira Instância, os arguidos, tinham em sua posse, cartões bancários legítimos, emitidos em seus nomes, outros cartões não bancários, mas contendo bandas magnéticas, e um cartão, emitido em nome de um dos arguidos, que na sequência de perícia, se determinou ser contrafeito.

Em comum, todos estes cartões, encerravam nas respetivas bandas magnéticas, os dados referentes a outros cartões bancários, titulados por terceiros.

Inconformados com a mencionada Decisão, os arguidos interpuseram recurso para o Tribunal da Relação do Porto, com base nos seguintes fundamentos:

- A impugnação da matéria de facto, com base no exposto no artigo n.º 412.º, números 3 e 4 do Código de Processo Penal,

- A eventual consumpção entre o crime de Passagem de Moeda Falsa na forma continuada, prevista e punida pelos artigos números 265.º, n.º 1, alínea a) e 267.º, n.º 1, alínea c) do Código Penal, e o crime de Falsidade Informática, na forma continuada, previsto e punido pelos artigos 3.º, n.º 1 e 3, da Lei n.º 109/2009, de 15 de setembro,
- Concurso aparente, na vertente de subsidiariedade, entre o crime de Contrafação de Moeda e o de Passagem de Moeda Falsa.
- A medida das penas parcelares, e da pena em absoluto.

Dos factos provados, em Decisão de primeira Instância, e atendendo aos diversos instrumentos utilizados para a prática dos crimes imputados aos arguidos, que lhes vieram a ser apreendidos, designadamente, um computador portátil, com o qual haviam sido feitas pesquisas na internet, no sentido de localizar programas informáticos suscetíveis de facultar a falsificação de identidades, o uso de programas e aplicações específicos para a programação de cartões com banda magnética, um *"skimmer"* para regravação de elementos bancários, em bandas magnéticas de cartões com essa funcionalidade, as inúmeras testemunhas que haviam reconhecido os arguidos enquanto autores dos pagamentos fraudulentos denunciados, não subsistiam dúvidas que os arguidos haviam praticados comportamentos reconduzíveis ao modo de atuação já referido de *"Carding"*, o qual, e como já atrás se defendeu, integra a previsão da norma vertida no número 3, do artigo 3.º, da Lei do Cibercrime.

Porém, o Tribunal da Relação do Porto, manteve a condenação decidida pelo Tribunal de primeira Instância, em aplicar a cada um dos arguidos, a pena única de cinco anos e seis meses de prisão.

O fundamento de tal decisão, estribou-se na doutrina vertida por Almeida Costa (Dias, et al., 1999, p. 749), quanto à possibilidade de inexistir, relativamente aos factos em apreço, uma eventual consumpção, entre o crime de Passagem de Moeda Falsa na forma continuada, prevista e punida pelos artigos números 265.º, n.º 1, alínea a), e, 267.º, n.º1, alínea c) do Código Penal, e o crime de Falsidade Informática, na forma continuada, prevista e punia pelos artigos 3.º, números 1 e 3 da Lei n.º 109/2009, de 15 de setembro.

No entanto, salienta-se que essa fundamentação, reporta-se a um comentário ao Código Penal, publicada no longínquo ano de 1999, ou seja, dez anos antes da publicação da Lei do Cibercrime.

Os Venerandos Desembargadores do Tribunal da Relação do Porto invocam o seguinte raciocínio *"...O bem jurídico protegido nos crimes de moeda falsa tem sido colocado, entre nós, quer na "confiança ou fé pública na moeda "(cfr. Prof. Beleza dos Santos, in RLJ , 64,*

275/276 , 290/291 e 305/307) quer na "segurança e funcionalidade (operacionalidade) do tráfego monetário ou em ambos "(Cfr. Almeida Costa, in Comentário Conimbricense do Código de Processo Penal , II , 739) , falando-se também na "pureza ou autenticidade do sistema monetário" , ou mais explicitamente na " integridade ou intangibilidade do sistema monetário em si mesmo considerado (cfr. Comentário Conimbricense do Código Penal , II , 749) , no interesse público da genuinidade respetiva de que é garante e nele encabeça o banco emissor .

Trata-se de um crime material ou de resultado que se consuma quando a moeda falsa penetra na esfera de disponibilidade do destinatário, sendo um delito de execução livre ou não vinculada; a passagem de moeda falsa pode verificar-se por qualquer modo que, de uma perspetiva " ex ante " se mostre idóneo para produzir o evento da entrada das peças contrafeitas na esfera de disposição do destinatário, vide Ac. do STJ, 25092008, Processo nº 08P2487, relator ARMINDO MONTEIRO..."

Salienta-se, uma vez mais, que o recurso a este tipo de raciocínio, apenas fazia sentido para fundamentar comportamentos idênticos aos aqui julgados, mas que tivessem tido lugar em momento anterior à publicação da Lei do Cibercrime.

Como já se referiu ao longo da presente Dissertação, estes modos de atuação criminosos, totalmente inovadores, chegaram a Portugal, pouco depois das alterações introduzidas no Código Penal, mormente pela reforma de 1995, através do Decreto Lei 48/95 de 15 de março.

Nessa altura, tanto a doutrina com a jurisprudência, fizerem grandiosos esforços, nomeadamente recorrendo às regras de interpretação, particularmente na vertente atualista do preceito constante no artigo 267.º, número 1, alínea c), do Código Penal, por forma a reconduzir os comportamentos denominados por *"Skimming"* e *"Carding"* ao mencionado preceito. Caso contrário, correr-se-ia o risco de tais comportamentos não poderem ser tratados como crimes, por inexistência de Lei prévia.

Por outro lado, é incompreensível o que fundamenta o motivo pelo qual antes da entrada em vigor no ordenamento jurídico nacional da lei do Cibercrime, todos os comportamentos em tudo idênticos aos que compunham o objeto deste processo, eram reconduzidos à norma constante no artigo 267.º, número 1, alínea c), do Código Penal, e, após a entrada em vigor da Lei do Cibercrime, em 15 de Setembro de 2009, que regula exatamente este tipo de comportamentos, de forma inexplicável, estando-se perante factos que apenas se conseguem consumar lançando mão de actos de execução de comportamentos descritos no tipo legal de Falsidade Informática, os Tribunais, não obstante esta evidência, optam por punir os respetivos autores por ambos os tipos legais, em sede de concurso efetivo.

O Acórdão do Tribunal da Relação do Porto, alusivo ao processo 2013/13.3JAPRT.P1 datado de 17-09-2014, vem igualmente pôr em crise, a aplicação da Lei do Cibercrime, na punição de dois cidadãos de nacionalidade Búlgara, que entre os dias 22 e 26 de Setembro de 2013, colocaram diversos dispositivos eletrónicos, em várias caixas automáticas[81], que permitiu capturar os dados inseridos nas bandas magnéticas de inúmeros cartões bancários.

Cumulativamente com esses dispositivos, suscetíveis não só de capturar, como igualmente de copiar os dados bancários inseridos nas bandas magnéticas de cartões de débito e de crédito, os arguidos, instalaram pequenas câmaras, dissimuladas nas diversas caixas automáticas, com o propósito de capturarem as imagens produzidas pelos legítimos titulares desses cartões bancários, a inserirem os respetivos códigos secretos.

De acordo com os factos provados, foram apreendidos pelas autoridades, toda uma panóplia de objetos utilizados para a prática de comportamentos reconduzíveis ao já referido modo de atuação de *"Skimming"*, e que como já bem se viu, são puníveis pelo artigo 3.º, número 2, da Lei do Cibercrime.

É igualmente dado como provado que os autores, de forma não apurada, terão feito chegar os elementos bancários, que capturaram através do modo acima mencionado, a terceiros, que os replicaram em cartões bancários, e os utilizaram de forma fraudulenta, nos Estados Unidos da América.

No entanto, os arguidos são acusados pelo Ministério Público, imputando-lhes a prática, em coautoria, de um crime de Contrafação de Moeda, previsto e punido pelos artigos 262.º, n.º 1 e 267.º, n.º 1, alínea c), do Código Penal, e de um Crime de Falsidade Informática, previsto e punido pelo artigo 3.º, n.º 1 e 2, da Lei nº 109/2009, de 15 de setembro.

Em sede de Decisão de primeira Instância, ambos os arguidos, acabaram condenados pela a prática, em coautoria, de um crime de Contrafação de Moeda, previsto e punido pelos artigos 262.º, n.º 1 e 267.º, n.º 1, alínea c), do Código Penal e de um crime de Falsidade Informática, previsto e punido pelo artigo 3.º, n.º 1 e 2, da Lei n.º 109/2009, de 15 de setembro, na pena única de quatro anos de prisão.

Inconformados com esta Decisão, os arguidos interpuseram recursos para o Tribunal da Relação do Porto, com o fundamento do que atrás se expôs, ou seja, alegam que os factos provados, apenas permitem que os arguidos sejam condenados pela prática do

[81] Vulgarmente designadas por ATM.

crime de Falsidade Informática, previsto e punido pelo artigo 3.º, n.º 1 e 2, da Lei n.º 109/2009, de 15 de setembro, e não pelo crime de Contrafação de Moeda.

Porém, tal pretensão não tem acolhimento, tendo o Tribunal da Relação do Porto mantido a Decisão de primeira Instância.

A fundamentação para a aplicação aos arguidos da prática, em concurso efetivo, dos crimes Contrafação de Moeda, previsto e punido pelos artigos 262.º, n.º 1 e 267.º, n.º 1, alínea c), do Código Penal e de um crime de Falsidade Informática, previsto e punido pelo artigo 3.º, n.º 1 e 2, da Lei n.º 109/2009, de 15 de Setembro, é justificada, quanto ao crime de Contrafação de Moeda da seguinte forma *"...O cartão de crédito é equiparado a moeda e, sendo o bem jurídico protegido pela incriminação, no que toca à contrafação de moeda, a intangibilidade do sistema monetário, incluindo a segurança e credibilidade do tráfico monetário, a proteção da secção na qual aquela norma se integra, estende-se, para além do mais, ao cartão de crédito. Assim, a interferência na banda magnética do cartão de crédito consubstancia um crime de contrafação de título equiparado a moeda, mesmo quando o cartão de crédito verdadeiro e o cartão falso apresentem dissemelhanças externas, mas o cartão falso desencadeou o funcionamento do sistema informático através do terminal de POS..."*

Os juízes Desembargadores, convocam também a doutrina de Paulo Pinto de Albuquerque, no seu comentário do Código Penal, para fundamentarem esse raciocínio.

Porém, essa anotação (Albuquerque P. P., 2015, p. 954)[82] remete-nos para um Acórdão do Supremo Tribunal de Justiça, datado de 1998, ou seja, onze anos antes, da entrada em vigor no ordenamento jurídico nacional, da Lei do Cibercrime, em 15 de setembro de 2009.

Por outro lado, e de forma igualmente recorrente, os Desembargadores justificam a necessidade de ser aplicada a figura do concurso efetivo entre os crimes de Contrafação de Moeda e Falsidade informática, aos factos praticados pelos condenados neste Acórdão, com a seguinte fundamentação;

".... Relativamente ao crime de Falsidade Informática, prevista e punida pelo artigo 3.º, números 1 e 2, da Lei 109/2009 de 15 de Setembro, apelidada de Lei do Cibercrime, transpôs para a ordem jurídica portuguesa a Decisão Quadro n.º 2005/222/JAI, relativa a ataques contra sistemas de informação, adaptando o direito interno à Convenção sobre Cibercrime do Conselho da Europa.

O bem jurídico que este ilícito pretende acautelar é a integridade dos sistemas de informação, Acórdão do Tribunal da Relação de Lisboa, 30/06/2011, processo nº TRL189/09.3JASTB.L15, Relator FILOMENA LIMA, in www.dgsi.pt.

82 Nesse mesmo sentido, (Garcia & Rio, 2015, pp. 1093,), que remete a fundamentação do modo de atuação de "Skimming" e "Carding" se subsumirem ao crime de Contrafação de Moeda, para a doutrina vertida no Acórdão relativo ao Processo 7876/10.1JFLSB.L1-5.

Dados informáticos são qualquer representação de factos, informações ou conceitos sob uma forma suscetível de processamento num sistema informático, incluindo os programas aptos a fazerem um sistema informático executar uma função – alínea b), do artigo 2.º da Lei 109/2009. Aqui, o bem jurídico que se pretende defender é a integridade dos sistemas de informação, pretendendo-se impedir os actos praticados contra a confidencialidade, integridade e disponibilidade de sistemas informáticos, de redes e dados informáticos, bem como a utilização fraudulenta desses sistemas, redes e dados Preâmbulo da Convenção sobre Cibercrime do Conselho da Europa, in DR 1.ª Série A, 15092009..."

Como bem se percebe, a argumentação que de forma recorrente, é utilizada na fundamentação dos diversos Acórdãos de 2.ª Instância, para a condenação de autores, sobre os quais hajam sido provados factos relacionados com a Falsidade Informática da Lei 109/2009 de 15 de setembro, resulta, de forma sistemática, com a invocação de alguns dos objetivos que se pretendem alcançar com a ratificação da mencionada Convenção.

No entanto, a jurisprudência negligência não só a singularidade, como também o caráter altamente inovador, da Lei 109/2009 de 15 de setembro, pois tal como já tivemos oportunidade de mencionar ao logo da presente Dissertação, Portugal é o único país, de entre os demais Estados Membros que ratificaram a referida Convenção, que previu e estatuiu a respetiva punição, concretamente no seu artigo 3.º, todos estes tipos de comportamentos, designadamente o *"Skimming"* e *"Carding"*[83].

Por outro lado, importará salientar que de acordo com as atuais normas de direito internacional público, o Legislador nacional ao ratificar uma Convenção, obriga-se, somente, a adaptar ao respetivo Direito Interno, esses princípios.

Contudo, o Estado, mantém inalterada não só a sua soberania, mas também, e sobretudo, a respetiva discricionariedade para a tipificação de comportamentos que entenda suscetíveis de censura penal.

Daí, resulta o desimpedimento para exceder as normas assumidos nessa Convenção, nomeadamente, a possibilidade em introduzir novos critérios e outras previsões legais, inovadoras, mormente, a antevisão e respetiva inscrição de normas legais na transposição para o direito interno resultantes dessa convenção, de outros comportamentos, aos quais pretenda tipificar e sancionar como crimes.

Foi, exatamente o que sucedeu com a redação entretanto dada à Lei 109/2009, de 15 de setembro, pois apenas o Estado Português, na transposição para o Direito interno que conferiu à Convenção de Budapeste, pretendeu punir todos os comportamentos que

83 De acordo com informações decorrentes de entrevista pessoal mantida com Diretor do Gabinete Cibercrime do Ministério Público, Dr. Pedro Verdelho

implicassem a manipulação, o uso e até a venda dos dados registados em todos os cartões bancários, incluindo-se nestes, forçosamente, os cartões de crédito.

Daí, que em nossa perspetiva, não resultem quaisquer dúvidas que a adequada interpretação da factualidade subjacente à manipulação dos dados informáticos, inseridos nas bandas magnéticas dos diversos cartões bancários em vigor, se subsuma à norma do artigo 3.º da Lei do Cibercrime.

7. O CONCURSO DE NORMAS NA LEI PENAL PORTUGUESA

O Código Penal, no seu artigo 30.º, disciplina as regras sobre o concurso de crimes e sobre o crime continuado (Cavaleiro de Ferreira, 1987, p. 373).

Porém, da interpretação do mencionado artigo, não se alcança qualquer definição, para a nossa lei penal, do sentido a extrair daquilo em que consiste o concurso de crimes[84].

O legislador, indicou apenas enquanto critério mínimo, por forma a permitir uma distinção entre unidade e pluralidade de infrações, a utilização do advérbio *"efetivamente"*[85].

Toda a construção do instituto da unidade e pluralidade de crimes, e respetiva solução da teoria do concurso, é assim entregue à doutrina e jurisprudência[86].

A solução encontrada pela doutrina, e, entretanto, adotada pela jurisprudência, consiste na fundamentação sustentada no facto que existe concurso de crimes, quando estamos perante factos em que um ou mais agentes, com as suas condutas, não preenchem um único ou o mesmo tipo de crime, mas mais do que um tipo de crime, ou, o mesmo tipo de crime, mais do que uma vez (Simas Santos & Leal-Henriques, Noções de direito penal, 2016, p. 153).

Segundo Germano Marques da Silva (2015, p. 421), quando várias pessoas praticam um crime, estamos perante um concurso de agentes, quando uma só pessoa, pratica dois ou mais crimes, ocorre o que se denomina de concurso de crimes.

Ainda segundo o mencionado autor (Silva, 2015, p. 418), o concurso de crimes não se confunde com o concurso de normas – concurso aparente de crimes, já o concurso de normas, pressupõe a unidade do facto e a pluralidade de normas potencialmente aplicáveis, mas o facto constitui um só crime, por isso se diz que no concurso de normas existe apenas um concurso aparente de crimes[87].

---

84 Neste sentido (Simas Santos & Leal-Henriques, Código penal anotado, 2014, p. 437)

85 *Ibidem*.

86 Nesse sentido (Cavaleiro de Ferreira, 1987, p. 377).

87 Neste ponto, citando José Lobo Moutinho - Da unidade à pluralidade dos crimes no Direito Penal Português, 2005.

Dessa forma, e com o contributo de vários ilustres juristas, foi construído todo um edifício doutrinário, baseado no instituído no mencionado artigo 30.º do Código Penal, no sentido de apurar, dentro de tais pluralismos, se o, ou, os agentes, cometerem um, ou mais crimes, ou seja, mais do que um tipo de ilícito, ou, preencher o mesmo tipo legal, porém, mais que uma vez (Silva, 2015, p. 419).

Ou seja, toda a teoria subjacente ao concurso de crimes, tem enquanto desiderato, a clarificação da questão que se coloca perante a hipótese, em sede de direito penal, quando um só autor, com uma só ação, ou, com várias ações, todas voluntárias, viola diversos tipos legais várias vezes, de forma ilícita e culposa, podendo tais comportamentos, ocorrer em qualquer modalidade de autoria ou de comparticipação (Garcia & Rio, 2015, p. 229).

Há, nessa matéria, um entendimento generalizado que o número 1 do artigo 30.º do Código Penal, aborda a temática da pluralidade, ou o chamado concurso de crimes (Simas Santos & Leal-Henriques, Código penal anotado, 2014, p. 437) (Cavaleiro de Ferreira, 1987, p. 377).

Para Figueiredo Dias (Dias J. d., 2007, p. 1005), *"o concurso de crimes existe sempre que no mesmo processo penal, ou em processo penal posterior destinado ao conhecimento de um concurso superveniente, o comportamento global imputado ao agente – traduza-se ele numa unidade ou pluralidade de ações – preenche mais que um tipo legal de crime, previsto em mais do que uma norma concretamente aplicável, ou preenche várias vezes o mesmo tipo legal de crime previsto pela mesma norma concretamente aplicável"*.

Que a figura do concurso de crimes, unitária, por sua vez, se divide em duas categorias: a do concurso efetivo, puro ou próprio, no qual se verifica uma pluralidade de sentidos de ilícito do comportamento global do agente; e a do concurso aparente, impuro ou impróprio, em quem no comportamento global, se verifica uma absoluta dominância ou prevalência de um sentido de ilícito sobre outro ou sentidos de ilícitos concorrentes, mas assim dominados, subordinados, dependente ou acessórios (Dias J. d., 2007, p. 1005)[88].

Assim, a determinação da existência do chamado concurso ideal só é possível depois de previamente se estudarem e se levarem em conta as especiais relações de subordinação em que se encontram os preceitos, uns, relativamente aos outros quanto à sua aplicabilidade, uma vez que só elas permitem limitá-lo e opô-lo ao chamado concurso legal, aparente ou impuro (Correia, 1963, p. 20).

[88] Nesse mesmo sentido (Correia, 1963, p. 18), e, (Cavaleiro de Ferreira, 1987, p. 377).

Relativamente àquelas relações de subordinação entre distintos preceitos, diferentes autores costumam distingui-las enquanto especialidade, subsidiariedade, consunção e alternatividade, muito embora a doutrina não se unanime a este respeito (Correia, 1963, p. 20).

Porém, no prisma da valoração objetiva, ou da respetiva imputação subjetiva ao agente, não existe qualquer justificação para se tratar de forma diferenciada o concurso real e o ideal (Correia, 1963, pp. 16-17)[89].

Assim, quando um agente, pratica por diversas vezes o mesmo tipo legal, sendo aqui indiferente que os tenha concretizado por intermédio de uma ou mais ações criminosas, subsistem duas possibilidades, ou existe unidade do facto punível, ou seja, um único crime, ou, está-se perante um concurso de crimes (Correia, 1963, p. 17)[90].

A solução para a determinação se num dado evento criminoso estamos perante uma unidade ou pluralidade de crimes, reside no facto da possibilidade dos vários comportamentos dolosos praticados pelo autor ou autores, se poderem subsumir a um, ou mais, tipos legais de crimes (Garcia & Rio, 2015, p. 229)[91].

Ou seja, pese embora no plano naturalístico, o autor dos factos tenha realizado apenas uma atividade, poderão, no entanto, existir uma pluralidade de valores jurídicos negados, existindo forçosamente, outros tantos crimes que haverão de ser contados e imputados ao respetivo autor (Correia, 1963, p. 17).

Interessa, portanto, apreciar todas as resoluções do autor, com o intuito de avaliar o sentido das respetivas determinações volitivas, na realização de todo o seu projeto criminoso (Correia, 1963, p. 18).

A jurisprudência nacional, tem acolhido a doutrina de Eduardo Correia, na aceção de que a uma diversidade de juízos de censura, corresponde uma pluralidade de resoluções autónomas (Correia, 1963, p. 17)[92].

Ainda que o agente pratique um só acto, o mesmo pode traduzir-se na ofensa de diversos interesses jurídicos, ou repetidamente, o mesmo tipo legal violado (Correia, 1963, p. 17). Assim, sempre que se verifique que a atividade criminosa levada a cabo pelo agente se desdobra numa pluralidade de condutas, determinada ficaria a existência do concurso real, material ou concurso de infrações (Correia, 1963, p. 21).

89 Partilhando da mesma opinião (Garcia & Rio, 2015, p. 229)

90 *Ibidem*.

91 Citando o critério proposto por Eduardo Correia.

92 No mesmo sentido (Garcia & Rio, 2015, p. 230)

Por outro lado, se cada uma das ações reclama individualmente aplicação de uma só e a mesma disposição, ou seja, se o autor cometeu o mesmo crime mais que uma vez, teríamos o concurso real da mesma espécie, homogéneo ou reiteração[93]. Se, as diferentes ações preenchem múltiplos tipos de crimes, ou seja, se o agente cometeu uma pluralidade de infrações de diferente natureza, teríamos o concurso real de espécies diferentes ou heterogéneo (Correia, 1963, p. 21).

Perante a eventualidade de se estar perante uma pluralidade de crimes, é assim, hodiernamente, pacifica a distinção entre;

a) **Concurso de crimes aparente, impuro ou impróprio** – cujo comportamento ilícito do autor preenche, apenas de forma formal, diversos tipos legais de crime, que, porém, por via de interpretação jurídica, conclui-se que a globalidade da conduta levada a cabo pelo autor, é, de forma exclusiva, e completamente absorvida, por apenas um dos vários tipos legais de crimes violados, devendo por isso, os demais tipos legais violados, retroceder, não sendo assim aplicados. É uma questão portanto que pode ser elidida porque os sentidos singulares de ilicitude típica presentes no comportamento global se conexionam, se intercessionam ou parcialmente se cobrem de tal que, em definitivo, se deve concluir que aquele comportamento é dominado por um único sentido de desvalor jurídico-social; por um sentido de tal forma dominante, quando lido à luz dos significados socialmente relevantes (Dias J. d., 2007, pp. 1011-1015)[94].

Nesta situação, e em rigor, está em causa um concurso de normas, porquanto a aplicação de uma dessas normas, exclui a aplicação de outras normas eventualmente em conflito, tratando-se somente de uma questão de decisão da norma aplicável ao caso em concreto (Cavaleiro de Ferreira, 1987, p. 377), (Simas Santos & Leal-Henriques, Código penal anotado, 2014, p. 437).

No entanto, também pode ocorrer o facto desses diferentes tipos de crimes, encontrarem-se em diversas relações entre si, subdividindo-se respetivamente em:

- **Especialidade** – quando uma das normas penais aplicáveis, se destaca das demais, eventualmente aplicáveis, por abarcar todos os elementos essenciais, acrescentando pelo menos um elemento adicional, a partir de uma perspetiva especial.

93 *Ibidem.*

94 No mesmo sentido (Cavaleiro de Ferreira, 1987, pp. 376-377).

Aqui, o intérprete apenas se concentrará nos preceitos abstratamente aplicáveis, indiferentemente da natureza, privilegiante ou qualificante, do elemento típico especializador (Cavaleiro de Ferreira, 1987, p. 378), (Garcia & Rio, 2015, p. 233).

Existe sempre uma especialidade na relação entre o tipo fundamental e as suas variantes qualificadas ou privilegiadas, e nas relações do tipo complexo, com o seu ou os seus tipos simples [95].

Assim, e por força do princípio *lex speciallis derogat legi generali*, deve ser aplicado somente o tipo especializado (Simas Santos & Leal-Henriques, Código penal anotado, 2014, p. 437).

- **Subsidiariedade expressa ou formal** – é facilmente reconhecível, tendo-se em conta as relações que necessariamente se estabelecem entre certos preceitos, em que uns condicionam expressamente a sua eficácia à não aplicação de outro ou outros (Cavaleiro de Ferreira, 1987, pp. 378-379), (Garcia & Rio, 2015, p. 234).

Ou seja, em que certas normas, apenas se aplicam subsidiariamente, mormente, quando o facto em causa, não seja punido por outra norma, de forma mais gravosa (Simas Santos & Leal-Henriques, Código penal anotado, 2014, p. 438).

Assim, as duas normas incriminadoras não podem, no caso concreto, ser aplicadas conjuntamente, pois isso corresponderia à violação do *non bis in idem*, de natureza substantiva, equivaleria dessa forma, a uma dupla valoração da mesma realidade do facto (Cavaleiro de Ferreira, 1987, p. 379).

- **Consumpção** – Consiste na apreciação efetuada sobre certos comportamentos, nos quais, existe, simultaneamente, o preenchimento de um tipo legal mais grave, que inclui um outro, de menor gravidade (Cavaleiro de Ferreira, 1987, p. 380).

A especificidade do caso concreto[96], irá ditar qual a norma que se aplicará, se a de menor, ou, maior gravidade.

A relação de consunção ocorre quando um tipo legal de crime inclui a realização de um outro tipo menos grave, não por necessidade lógico conceptual, mas sim de um modo típico. Desse facto, resulta o entendimento que o legislador, ao estabelecer a pena mais grave, tenha já tomado em conta nesse crime, todo o conteúdo material da ilicitude e da culpabilidade do crime menos grave. Por isso, a norma que prevê o crime mais grave

95 Por hipótese, a situação do crime de Roubo em confronto com os crimes de Furto, Coação ou até o Sequestro.

96 A título de exemplo uma situação que envolva os crimes de Furto Qualificado, conforme art.º 204.º, n.º 1, al. f), e, a Violação de Domicílio, conforme artigo 190.º, ambos do Código Penal.

exclui a aplicação em concreto da norma que prevê o crime menos grave, de acordo com o princípio *lex consumens derogat legi consuntae*.

Geralmente, a relação de consunção, ocorre quando as normas se encontram numa relação de inclusão material, da qual resulta que o conteúdo de um facto ilícito típico inclui normalmente o de outro facto ilícito típico e a punição do primeiro esgota o desvalor da globalidade dos factos praticados (Albuquerque P. P., 2015, p. 216).

A consumpção produz, enquanto consequência, que a norma consumptiva, ou seja, a dominante, supera a norma consumida, que será a dominada (Correia, 1963, pp. 130-131).

Por outro lado, a consumpção pode tratar-se de uma consumpção pura ou impura.

A consumpção é pura, quando a norma mais grave se sobrepõe à norma que se apresenta em simultâneo com esta última, e é ainda menos grave.

A consumpção é impura, quando o facto crime de menor gravidade, faz recuar a punição do facto de maior gravidade, aplicando-se a pena menos grave à globalidade dos factos em apreciação.

- **Facto posterior não punível –** Consistem naqueles crimes cujo desiderato do autor é garantir ou aproveitar a impunidade de outros crimes, os quais não são punidos em sede de concurso efetivo com o crime de fim lucrativo, ou de apropriação, com exceção de virem a causar um novo dano ao ofendido, ou forem direcionados a atingir um outro bem jurídico[97].

b) **Concurso efetivo, verdadeiro ou puro** – quando os comportamentos de um ou mais autores, preenchem diversos tipos legais, não se verificando porém, a exclusão de nenhum dos tipos legais preenchidos por aplicação de qualquer uma das regras mencionadas para o concurso legal (Cavaleiro de Ferreira, 1987, p. 382). Quando entre as normas penais violadas pelo agente não se verificar uma relação de exclusão recíproca ou de concurso aparente, estaremos então perante uma situação de concurso efetivo, verdadeiro ou puro, em que os diversos tipos legais de crime abstratamente aplicáveis concorrem simultaneamente na sua aplicação em concreto. Antes, porém, confirma-se que as normas violadas pelo autor ou autores, surgem como concorrentes na aplicação concreta, sendo a punição concreta da

[97] Cf. (Simas Santos & Leal-Henriques, Código penal anotado, 2014, p. 439)

> globalidade dos factos praticados, efetuada segundo as regras fixadas pelos números 1 a 4 do artigo 77.º do Código Penal, ou seja, fixando uma pena por cada crime, e, posteriormente, a unificação dessas penas através da aplicação de uma pena única resultante do concurso (Simas Santos & Leal-Henriques, Código penal anotado, 2014, p. 439).

Doutrinariamente distinguem-se, embora se equiparem, duas formas de concurso efetivo ou verdadeiro: concurso ideal e concurso real (Cavaleiro de Ferreira, 1987, p. 383):

- **Concurso ideal** – ocorre quando com apenas uma só ação, o autor ou autores, violam diferentes normas penais, existindo neste caso um concurso ideal heterogéneo, ou, se infringem por diversas vezes o mesmo tipo legal, verificando-se nesta situação a presença de concurso ideal homogéneo.
- **Concurso real** – verificar-se-á quando o agente através de várias ações preenche vários tipos de crime - concurso real heterogéneo (por exemplo, o agente pratica um furto, depois um homicídio, e, posteriormente um dano), ou várias vezes o mesmo tipo legal de crime. No concurso real homogéneo (por exemplo, o agente pratica sucessivos furtos ou agride fisicamente várias pessoas). Verifica-se este tipo de concurso quando o autor ou autores, mediante a prática de diversas ações, violam distintos tipos legais, sendo que a nossa lei penal equipara as duas referidas formas de concurso efetivo (art.º 30º, n.º 1), determinando para ambas a aplicação de uma pena única (art.º 77.º, n.º 1). (Albuquerque P. P., 2015, p. 218).

Figueiredo Dias, porém, introduziu uma tese corretiva, a qual reconduz ao concurso efetivo de crimes, as circunstâncias em que os factos em causa, integrem diferentes tipos legais e necessariamente bens jurídicos distintos ou, integrando esses comportamentos tipos legais cujo respetivo bem jurídico protegido seja o mesmo, essas violações, hajam ocorrido em lugar, e situações histórica distintas (Garcia & Rio, 2015, p. 231).

Esta doutrina encontra-se vertida no Acórdão do Supremo Tribunal de Justiça, de 31/03/2011, processo 361/10.3GBLLE[98], onde os respetivos Conselheiros apreciaram um recurso, interposto pelo arguido, por factos relacionados com a prática do crime de Homicídio, o qual havia sido consumado com o recurso a uma arma de fogo, em concreto, uma espingarda caçadeira, ao qual, e em sede de decisão proferida em Tribunal de primeira Instância, lhe foram aplicadas as seguintes penas;

98 Consultável em http://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/77de29905c952c5680257868004ee9e5?OpenDocument, acedido em 06/01/2019.

- Pela prática de um crime de Homicídio previsto e punido pelas disposições combinadas dos artigos 131.º e 86.º, n.º 3, da Lei n.º 5/2006, de 23 de fevereiro, na pena de 17 anos de prisão;
- Pela prática de um crime de Detenção Ilegal de Arma previsto e punido pelo artigo 86.º, n.º 1, alínea c), da Lei n.º 5/2006, na pena de 1 ano e 4 meses de prisão;
- Em cúmulo jurídico daquelas duas penas, na pena única de 17 anos e 10 meses de prisão.
- Foi ainda aplicada ao arguido a sanção acessória de interdição de detenção, uso e porte de armas pelo período de 17 anos.

No entanto, foi entendimento do Juízes Conselheiros, que a agravação conferida à prática do crime de Homicídio, mediante a utilização de uma arma proibida, não pode ser valorada, uma vez que para que tal eventual agravamento do crime de Homicídio se verifique, seria indiferente que o autor estivesse numa situação de legalidade ou ilegalidade relativamente à portabilidade da arma de fogo, ou seja, a agravação ocorreria sempre, ainda que autor dos factos tivesse devidamente autorizado e lhe tivesse sido emitida a respetiva licença de uso e porte de arma.

Os Conselheiros concluíram igualmente que, não obstante os actos praticados pelo autor, aferidos em termos globais, se subsumirem a dois tipos legais de crimes, a saber, Homicídio e Uso de Arma Proibida, que ainda assim, não se devia concluir estar-se na presença de um concurso efetivo de crimes, mas antes, de um concurso aparente.

O arguido, após revisão da decisão proferida pelo Tribunal de primeira Instância, acabou sentenciado pelos seguintes crimes e penas;

- Foi absolvido da acusação relativamente ao crime previsto e punido, pelo artigo 86.º, n.º 1, alínea c), da Lei nº 5/2006;
- Fixada em 14 (catorze) anos de prisão a pena do Crime Homicídio, previsto e punido, pelas disposições combinadas dos artigos 131.º do Código Penal e 86.º, n.º 3, da Lei n.º 5/2006;
- Fixada em 14 (catorze) anos a medida da pena acessória de interdição de Detenção, Uso e Porte de Armas.

Apreciada desta forma, a conduta do autor relativamente à utilização da arma de fogo utilizada enquanto meio para o cometimento do Homicídio, esgotou-se na prática deste último crime referido, fazendo assim sobrevir, em sede de apreciação global, o sentido da prática do crime de Homicídio como absolutamente dominante, e, por outro lado, subsidiária a utilização de uma arma de fogo proibida para a sua concretização.

O alcance pretendido pelo ilustre Professor com este raciocínio, é a demonstração da *"unidade de sentido social do acontecimento ilícito global"*, uma vez que o propósito do autor dos factos em apreciação no citado Acórdão, foi o de pôr termo à vida da vítima, tendo o uso da arma de fogo proibida utilizada sido não mais que o processo de que lançou mão para o concretizar.

Porém, e tal como já se havia referido, os Tribunais têm seguido a doutrina proposta por Eduardo Correia relativa à pluralidade de juízos de censura a qual se reconduz por sua vez, a uma multiplicidade de decisões independentes, relativas a resoluções que culminam na prática de crimes dolosos, e em decisões de onde deflectem as violações do dever de cuidado, quando estamos perante situações de negligência (Garcia & Rio, 2015, p. 231).

8. O CONCURSO DE CRIMES - UMA DIFERENTE PERSPECTIVA.

Os Tribunais portugueses, como já se referiu, para punirem os comportamentos que integram o tipo legal da Falsidade Informática prevista na nova Lei do Cibercrime, têm utilizado a figura do concurso de crimes, em concreto o concurso real, entre os crimes de Falsidade Informática, previsto e punido no artigo 3.º da Lei 109/2009, de 15 de setembro, e a Contrafação de Moeda, prevista e punida no artigo 262.º do Código Penal, por remissão da previsão constante na alínea c) do número 1, do artigo 267.º do Código Penal, o qual equipara a moeda, os cartões de crédito.

A fundamentação usada para justificar a aplicação destes tipos legais em sede de concurso real, e como já igualmente se oportunamente se referiu, tem sido, em regra o seguinte;

"*O cartão de crédito é equiparado a moeda e, sendo o bem jurídico protegido pela incriminação, no que toca à contrafação de moeda, a intangibilidade do sistema monetário, incluindo a segurança e credibilidade do tráfico monetário, a proteção da secção na qual aquela norma se integra, estende-se, para além do mais, ao cartão de crédito. Assim, a interferência na banda magnética do cartão de crédito consubstancia um crime de contrafação de título equiparado a moeda, mesmo quando o cartão de crédito verdadeiro e o cartão falso apresentem dissemelhanças externas, mas o cartão falso desencadeou o funcionamento do sistema informático através do terminal de POS..."*

"…. Relativamente ao crime de Falsidade Informática, prevista e punida pelo artigo 3.º, números 1 e 2, da Lei 109/2009 de 15 de Setembro, apelidada de Lei do Cibercrime, transpôs para a ordem jurídica portuguesa a Decisão Quadro n.º 2005/222/JAI, relativa a ataques contra sistemas de informação, adaptando o direito interno à Convenção sobre Cibercrime do Conselho da Europa.

O bem jurídico que este ilícito pretende acautelar é a integridade dos sistemas de informação, Acórdão do Tribunal da Relação de Lisboa, 30/06/2011, processo nº TRL189/09.3JASTB.L15, Relator FILOMENA LIMA, in www.dgsi.pt.

Dados informáticos são qualquer representação de factos, informações ou conceitos sob uma forma suscetível de processamento num sistema informático, incluindo os programas aptos a fazerem um sistema informático executar uma função – alínea b), do artigo 2.º da Lei 109/2009. Aqui, o bem jurídico que se pretende defender é a integridade dos sistemas de informação, pretendendo-se impedir os actos praticados contra a confidencialidade, integridade e disponibilidade de sistemas informáticos, de redes e dados informáticos, bem como a utilização fraudulenta desses sistemas, redes e dados Preâmbulo da Convenção sobre Cibercrime do Conselho da Europa, in DR 1.ª Série A, 15/09/2009..."

No entanto, o que nos parece ser evidente, é o facto de os Tribunais estarem a aplicar um tipo legal, especificamente criado para a punição deste tipo de comportamentos, exclusivo das Novas Tecnologias de Informação e Comunicação, cumulativamente com um outro em concreto, com o de Contrafação de Moeda, prevista e punida no artigo 262.º do Código Penal, por remissão da previsão constante na alínea c) do número 1, do artigo 267.º do Código Penal o qual, apenas fazia sentido aplicar até à entrada em vigor da Lei do Cibercrime, e como já se referiu, por esforço interpretativo da Doutrina e Jurisprudência de molde a impedirem que tais comportamentos não tivessem a devida tutela penal.

Por outro lado, a previsão do tipo legal constante no artigo 3.º da Lei do Cibercrime, não só prevê a totalidade destas novas formas de crime, como, por outro lado, exclui a totalidade do sentido da aplicação do mencionado artigo do Código Penal, a este tipo de fenómenos criminais, uma vez que para a respetiva consumação destas novas práticas de crime informático, não fará qualquer sentido, que os autores desperdicem recursos, totalmente desnecessários, quer na aquisição, quer no eventual fabrico de cartões bancários, integralmente contrafeitos.

Importa salientar que a particularidade deste tipo criminal[99] é de tal forma singular, que apenas pode ser concretizado com recurso a este tipo de tecnologia, ou seja, à captura, sub-reptícia dos dados inseridos nas bandas magnéticas dos atuais cartões bancários, indiferentemente da respetiva origem, ou seja, de tais elementos bancários terem sido extraídos de cartões de débito, de crédito, ou duais.

Como já anteriormente ao longo da presente dissertação se tem referido, o modo de atuação de *"Skimming"*, implica a apreensão, inteiramente aleatória, de um conjunto

99 Referimo-nos tanto ao "Carding" como ao "Skimming".

indeterminado de dados bancários, inseridos nas bandas magnéticas, de todos os cartões bancários que, num certo lapso temporal[100] sejam utilizados num caixa automático ou num terminal de pagamento automático, comprometido.

Durante esse período de tempo, e no decurso dessa atividade delituosa, os dispositivos colocados em máquinas automáticas dispensadoras de dinheiro, vão capturar os dados respeitantes a cartões de crédito como de débito, ou até cartões mistos ou duais.

Os autores destes factos, não irão assim, efetuar qualquer distinção quanto à origem dos dados bancários que ilegitimamente entram na posse, ou seja, se os mesmos provêm de cartões de crédito ou de débito.

Terá sido exatamente o propósito acertado do Legislador, quando na Lei do Cibercrime, ao inscrever na norma subjacente à Falsidade Informática, a expressão "... sobre os dados registados ou incorporados em cartão bancário de pagamento...".

Aliás, em nossa modesta opinião, não faria qualquer sentido destacar os dados *registados ou incorporados*, em cartões de crédito dos dados *registados ou incorporados* num cartão de débito, ou em cartões duais ou mistos.

Assim, e com base nesse raciocínio, poder-se-iam levantar inúmeras hipóteses concretas, cuja atual solução legal criada pelos nossos Tribunais, seriam, no mínimo, absurdas.

Imagine-se, as seguintes hipóteses:

- Num ATM, situado na região de Lisboa, durante o lapso temporal de três horas, dois criminosos, A e B, após a colocação com sucesso, de um dispositivo apto a capturar os dados *registados ou incorporados*, mas apenas de cartões de débito, viriam a obter os dados bancários relativos a cem desses cartões. Em momento subsequente, após o envio desses dados, por via eletrónica, para um qualquer país[101], no qual o respetivo sector bancário não tenha ainda implementado o sistema de segurança EMV[102], e aí, outros criminosos, replicando esses dados em cartões bancários, concretizam, com sucesso, entre pagamentos de serviços e compras, e levantamentos em numerário, um prejuízo na ordem dos €100.00,00 (cem mil euros).

100 Ou seja, enquanto o "skimmer", e restantes elementos que compõem estes dispositivos ilegítimos de captura de dados bancários se encontrarem ativos, quer por quem os colocou, por hipótese numa ATM, ainda não ter procedido à sua remoção, ou, a sua deteção ainda não ter sido participada às entidades competentes.

101 Apenas basta que para tal, se trate de um país situado fora do continente europeu.

102 A qual impõe que o cartão bancário ao entrar em contacto com um certo terminal ou caixa automático, têm que ser coincidentes; a leitura da banda magnética, a leitura do chip do respetivo cartão, e a inserção do código secreto. Caso estas três condições não se verifiquem, ou a operação é recusada, gerando, consequentemente um alerta no sistema, ou, caso se trate de um terminal ATM, o respetivo cartão é capturado.

- Agora, imagine-se, a mesma hipótese, envolvendo os criminosos C e D, mas os dados capturados por estes, estavam *registados ou incorporados*, apenas em cartões de crédito. Após o envio desses dados, pela mesma via eletrónica, para outro país, no qual a utilização de um cartão bancário com os dados replicados de um outro, se bastasse com a mera leitura da banda magnética, outros criminosos, replicando esses dados bancários em bandas magnéticas de cartões de crédito, concretizassem entre, pagamentos de serviços e compras, e levantamentos em numerário[103], um prejuízo na ordem dos €50.000,00 (cinquenta mil euros).

A questão que se colocaria, em face daquilo que têm sido as decisões dos nossos Tribunais superiores, seria qual, ou quais, os crimes e respetivas penas a que seriam condenados A, B, C e D?

Um facto teríamos seguramente como certo ou seja, que pese embora o prejuízo patrimonial causado pela dupla A e B ser o dobro do prejuízo que havia sido causado pela dupla de criminosos C e D, estes últimos ainda assim, seriam punidos em sede de concurso efetivo pelos crimes de Contrafação de Moeda, previsto e punido pelos artigos 262.º, n.º 1 e 267.º, n.º 1, alínea c), do Código Penal e de Falsidade Informática, previsto e punido pelo artigo 3.º, n.º 1 e 2, da Lei n.º 109/2009, de 15 de setembro e, muito provavelmente, a penas de prisão muito superiores àquelas que iriam ser aplicadas à dupla de criminosos A e B.

Nestes breves exemplos, perfeitamente enquadráveis na nossa atual realidade jurídico-criminal bastando que para tal os criminosos, após a captura dos dados registados ou incorporados nos cartões bancários, selecionassem o tipo de dados bancários que pretendiam replicar noutros cartões ou, os relativos a cartões de crédito ou, de débito.

Através destes exemplos, pretende-se igualmente demonstrar não só a injustiça que se coloca perante tais hipotéticas situações legais subjacentes mas, igualmente a desconformidade interpretativa que é atualmente produzida pelos nossos Tribunais nesta matéria a qual, contraria de forma inequívoca, a vontade do Legislador.

No entanto, todo este panorama que sustenta a atual doutrina dominante relativamente ao concurso de normas, foi completamente desconstruído, por Inês Ferreira Leite (Leite, 2016).

Com efeito, e contrariando a visão da doutrina dominante, relativamente à escolha das regras de cumulação que fundamentam o concurso de normas, as quais defendem que

103 Atendendo aos respetivos limites dos plafons dos cartões de crédito.

os respetivos critérios se encontram na norma e, no plano do caso julgado, os critérios estribam-se na identidade factual, aponta, desde logo, um problema comum ou seja, a impossibilidade de poder ser construído um conceito de facto jurídico, que por um lado não esteja vinculado à realidade ontológica, e por outro, que não decorra de forma exclusiva da própria norma (Leite, 2016, pp. 926-927).

Entende igualmente a mencionada autora, que fazendo o Legislador parte da vida em sociedade, e sendo a sua função, a regulação da respetiva realidade social, seria totalmente contraditório, que pudesse cumprir esse objetivo, de uma forma completamente alheada da sua vida em sociedade (Leite, 2016, p. 927).

Tendo por base esse raciocínio, é possível concluir que factos e normas, possuem elementos em comum ou, um *tertium genus* intermediário, que os faz corresponder a um "sentido social" de identificação, sem o qual, a interpretação dos factos, comportamentos e respetiva operação de subsunção à norma jurídica, ficariam irremediavelmente comprometidos (Leite, 2016, p. 929).

A autora vai mais longe, ao concluir que o Legislador, num terceiro plano, se encontra vinculado à compreensão das deduções que infere do agir humano, em termos sociais, designadamente, acerca dos valores negativos ou positivos dos comportamentos sociais, cumulativamente com os exclusivos modos de atuação criminosos (Leite, 2016, p. 938). Pese embora essa vinculação que recai sobre o Legislador, ser alvo de acérrimas criticas no âmbito do concurso de normas, esses reparos, no entanto, esbatem-se, quando se trata de admitir figuras como a adequação social ou, de modo semelhante, quanto a situações de aparência exterior de verificação da tipicidade, da exclusão da ilicitude ou, da culpa.

Dito de outra forma, a compreensão jurídica não decorre de uma simples leitura do tipo legal enquanto fenómeno descritivo e sim, como reflexivo de um tipo social (Leite, 2016, p. 939).

O tipo social proposto pela Ilustre autora, reconduz-se assim a um fenómeno de agregação de sentidos jurídicos e sociais, que resultará num processo de interpretação da realidade, e consequentemente, num mecanismo de interpretação da norma, a qual permite concluir que o mesmo existe, independentemente, e para além do tipo legal de crime (Leite, 2016, p. 943).

O tipo social, exprimirá assim a violação da norma em causa, e corresponderá a um padrão de comportamento socialmente comum de negação de vigência da norma. (Leite, 2016, p. 945). No entanto, o tipo social não prevalece sobre o tipo legal, nem o crime existe ou deixa de existir somente por impulso do tipo social (Leite, 2016, p. 998).

A solução encontrada, reside no facto de se conjugarem critérios sociais e normativos, daí que estes se suportem no conceito de facto normativo-social (Leite, 2016, p. 998). Nem a unidade do facto, ou respetiva punibilidade ou impunidade, são ditadas pela valorização social, por si só (Leite, 2016, p. 998).

Assim, a eventual exclusão de uma punição autónoma, por um certo tipo legal de crime, traduzir-se-á no resultado de diferentes momentos de análise jurídica, levados em conta quando confrontados com o sentido constitucional do *non bis in idem* (Leite, 2016, p. 998) - *"unicidade do facto, identificação da função normativo-social da norma de valoração e da norma sancionatória"* (Leite, 2016, p. 998).

A ilustre autora entende que em todos estes momentos atrás citados, as valorações sociais serão relevantes porém, restringem-se apenas a uma função, ainda que predominante, a de delimitação da unicidade do facto jurídico, necessariamente, com a mediação de critérios jurídicos (Leite, 2016, p. 322)

Nos demais momentos de análise, serão os critérios jurídicos que, notoriamente, predominam (Leite, 2016, p. 998).

Assim, para a mencionada autora, o crime não será ação, nem resultado, e muito menos, a mera lesão do interesse tutelado pela norma, mas tão somente, uma análise e correlação dos diversos elementos, fáticos e normativos, que, conjugados, constituem uma categoria normativo-social (Leite, 2016, pp. 1001-1002).

Por outro lado, o facto normativo-social, constituirá uma representação da realidade, cuja respetiva pretensão, exige o estabelecimento de uma relação de identidade representativa entre o facto natural e respetivo sentido normativo (Leite, 2016, pp. 1002-1003).

Assim, a procura de uma redução mínima do conceito de crime, não poderá ser encontrada em movimentos corporais, nem em *"unidade da vontade do agente"*, e, muito menos, no bem jurídico violado pela conduta (Leite, 2016, p. 1003).

A unidade mínima de facto jurídico com relevância penal, terá, necessariamente, que incorporar uma manifestação consciente da vontade por parte do autor, a qual pode ser dirigida à concretização da própria lesão, ou, à colocação em perigo de um bem jurídico, ou, de um interesse socialmente protegido, ou, à violação de um dever de cuidado que haja sido imposto para proteção de bens jurídicos aos quais se possam atribuir um desvalor suscetível de censura jurídico-penal (Leite, 2016, p. 1004).

A Ilustre autora, em síntese, dá enfase ao facto de que não se poder ter a pretensão de reduzir o conceito de crime a apenas uma das suas particularidades. No entanto, pode identificar-se num conjunto de factos, que, de forma agregada, manifestam a essência do

crime ou, recorrer a uma valoração global da conduta, em termos de uma perspetiva social e do tipo legal ou seja, visto de uma perspetiva normativa, com vista à identificação de uma unidade jurídica (Leite, 2016, pp. 1004-1005).

Porém, admite-se que a redução mínima do conceito de crime terá que incorporar todos os seus respetivos elementos fundamentais, ou seja, o desvalor da ação e um desvalor do resultado, em sentido normativo, que lhe seja atribuível (Leite, 2016, p. 1006).

Assim, o processo identificativo do crime em causa, inicia-se com a análise da realidade, correspondendo dessa forma, a um método tão interpretativo como aquele que possibilita ao jurista a circunscrição do âmbito de aplicação de normas penais. Em ambos os processos, o intérprete do direito lança mão de critérios fácticos e normativos. Nestes dois processos, a perceção social da vida e do Direito são determinantes (Leite, 2016, pp. 1007-1008).

Os elementos essenciais do crime, a saber, o desvalor da ação, o desvalor do resultado e relação da atribuição, serão apenas os princípios mínimos do facto jurídico-penal, uma vez que, se o desiderato é alcançar um conceito de unicidade do facto crime, para efeitos do *non bis in idem*[104], ter-se-á, necessariamente, que fazer juntar a todos esses elementos, outros, fornecidos pelo tipo social, de molde a que se obtenha a necessária união social de sentido, juridicamente valorada (Leite, 2016, pp. 1008-1009).

Desse modo, para que se deduza estar-se perante um concurso efetivo de crimes, espelhado no número 1, do artigo 30.º, e regulado pelo artigo 77.º, ambos do Código Penal, a verificação de vários tipos incriminadores, não se demonstra suficiente (Leite, 2016, p. 287).

Segundo a autora, mostra-se ainda necessário que, subjacente a cada um dos crimes em concurso, esteja, *efetivamente*, um crime autónomo, que sobre o mesmo possa, de forma igualmente autónoma, ser realizado um juízo de censura jurídico-penal (Leite, 2016, p. 287).

Dessa forma, será inadmissível o raciocínio que conclua pela existência de um concurso efetivo de crimes sempre que o mesmo autor pratique um só facto unitário, do ponto de vista normativo-social, em sentido estrito, na sua unidade mínima ou, o mesmo agente, pratique um só facto unitário, do ponto de vista normativo-social, em sentido amplo, quando, algum dos elementos nucleares do facto, nomeadamente, o desvalor da ação, o desvalor do resultado ou imputabilidade, sejam impeditivos da necessária

104 A proibição de dupla valoração, ínsita no número 5, do artigo 29.º da Constituição da República Portuguesa.

autonomização para que possam ser realizados dois, ou mais, juízos de censura jurídico-penal distintos, indispensáveis para a determinação, igualmente individual, das respetivas penas (Leite, 2016, p. 287).

O mesmo raciocínio se aplicará à eventual prática de uma pluralidade de factos, levada a cabo pelo mesmo autor, que sobre os quais a aplicação de um dos tipos incriminadores implique a ponderação de alguma das unidades nucleares essenciais a outro ou outros tipos incriminadores, resultando dessa forma uma dupla valoração proibida do mesmo facto, no seu sentido normativo-social (Leite, 2016, p. 287).

Com base neste argumento, com o qual nos identificamos e concordamos na íntegra, existe um conjunto imenso de situações que ficarão, desde logo, excluídas do regime legal do concurso efetivo, algumas por não se tratar de um verdadeiro concurso efetivo, e outras, por força do *non bis in idem* (Leite, 2016, p. 287).

É exatamente neste ponto em concreto, e que com o devido respeito, entendemos que a jurisprudência nacional, no que diz respeito à punição dos comportamentos subjacentes ao modo de atuação de *"Skimming"* e *"Carding"*, falha.

O tipo legal previsto no artigo 3.º da Lei do Cibercrime, ou seja, a Falsidade Informática, incorpora o sentido normativo-social, subjacente aos comportamentos dos modos de atuação criminosos acima mencionados.

A aplicação deste tipo legal aos modos de atuação criminosos de *"Skimming"* e *"Carding"*, esgota, portanto, a aplicação de qualquer outro tipo incriminador.

Dessa forma, entendemos inexistir qualquer fundamento para a aplicação de um concurso efetivo entre os tipos de crime de Falsidade Informática, artigo 3.º da Lei do Cibercrime, e de Contrafação de Moeda, artigo 262.º, por remissão constante na alínea c) do número 1, do artigo 267.º, ambos do Código Penal, quando estão em causa comportamentos criminosos, subsumíveis aos referidos modos de atuação de *"Skimming"* e *"Carding",* porquanto se está a efetuar uma dupla valoração proibida do mesmo facto, no seu sentido normativo-social.

9. CONSIDERAÇÕES FINAIS

Ao longo da presente dissertação deu-se conta que o cartão bancário em Portugal, ao longo de todos estes anos, em rigor desde o ano de 1995, e considerando as alterações introduzidas no Código Penal pelo Decreto Lei n.º 48/95, de 15/03, sofreu inúmeras inovações que não só o tornaram mais versátil, como incrementaram maior segurança em todas as transações em que este é interveniente.

As atuais diferenças entre o cartão de débito, crédito e dual, encontram-se esbatidas, porquanto até os cartões de débito, têm, bastas vezes, associados ao respetivo contrato, modalidades de pagamento diferido, permitindo por esse meio que o respetivo titular liquide o valor da transação em momento posterior, tal como sucede atualmente com os cartões de crédito.

Daí resulta que a Lei do Cibercrime não estabeleça qualquer distinção entre os diferentes cartões bancários, tratando-os por isso de igual forma.

As diversas incrementações que de forma recorrente foram sendo efetuadas, quer ao nível da segurança, quer em termos tecnológicos, pelas empresas com o encargo do fabrico do plástico de onde são produzidos os cartões bancários, retiraram utilidade ao tipo legal de Contrafação de Títulos Equiparados a Moeda, previsto na alínea c) do número 1 do artigo 267.º do Código Penal, designadamente, os cartões de garantia e de crédito.

Como já se referiu, o cartão de garantia já há muito que foi descontinuado do sistema bancário português, em razão do crescente interesse e maior segurança que foi sendo depositada no cartão de débito.

Por outro lado, a eventual contrafação de um cartão de crédito seria seguramente, impossível de ser concretizável, atendendo aos elementos de segurança inseridos no fabrico desses cartões, para além de que mesmo para os agentes, o investimento a ser depositado numa tal tarefa, seria incomportável, não só em termos logísticos, como do ponto de vista financeiro, que tal logística necessariamente envolveria.

Pese embora se compreenda o facto de tanto a doutrina como a jurisprudência após as alterações introduzidas no Código Penal pela entrada em vigor do Decreto Lei 48/95, de 15/03, terem reconduzido ao mencionado tipo legal a manipulação ilícita dos dados bancários inseridos nas bandas magnéticas dos cartões de crédito, tendo em conta os avanços tecnológicos que vieram a ter lugar no final da década de noventa, levadas a cabo por grupos criminosos, maioritariamente oriundos de países da Europa de leste o certo é,

e em rigor, que esse tipo de criminalidade não implicava a contrafação de cartões de crédito.

A atuação desses grupos criminosos, limitavam-se à colocação estratégica, e posterior utilização de dispositivos específicos, os quais lhes permitiam copiar, ilegitimamente, os dados bancários inseridos na banda magnética de um determinado cartão de crédito, e, posteriormente, replicá-los na banda magnética de um outro, legítimo, consumando a fraude através desse modo de atuação. Posteriormente, a captura dos dados bancários inseridos nas bandas magnéticas dos cartões bancários passou a ser indiscriminada[105] ou seja, os agentes optaram por fazer uma captura dos dados bancários de todos os cartões que fossem introduzidos nos terminais de pagamento automático ou de levantamento de numerário, que houvessem sido comprometidos por dispositivos aí ilegitimamente colocados.

Porém, entende-se que estes comportamentos criminosos, tendo em conta a respetiva danosidade causada, tanto ao nível patrimonial, como ao nível social, não podiam deixar de ser punidos pela lei penal.

No entanto, este tipo de comportamentos, não estavam tipificados na legislação penal nacional, tendo sido necessário, um esforço de interpretação, quer por parte da doutrina, e posteriormente pela jurisprudência, que permitiu que estas condutas não ficassem impunes.

Ou seja, o sistema bancário e respetiva segurança nas transações evoluiu, mas a norma ínsita na alínea c) do número 1 do artigo 267.º do Código Penal, cristalizou-se.

O mundo, tal como o conhecíamos em 1995 transformou-se, tendo em conta o incremento das inúmeras inovações tecnológicas, que constantemente foram sendo trazidas ao conhecimento geral de todos os cidadãos.

O legislador nacional, tentou contudo, adequar a nova realidade ao direito penal, aderindo a um instrumento de direito internacional público, nomeadamente, a Convenção de Budapeste.

Esta Convenção, tinha como desiderato, transpor para a ordem jurídica portuguesa a Decisão Quadro n.º 2005/222/JAI, relativa a ataques contra sistemas de informação, adaptando o direito interno à Convenção sobre Cibercrime do Conselho da Europa.

No entanto, e tal como já se referiu ao longo da presente dissertação, a Lei do Cibercrime transposta para o ordenamento jurídico nacional foi mais longe do que os demais estados-membros aderentes, pois foi a única que previu, no artigo 3.º,

105 A captura de dados bancários inseridos nas bandas magnéticas de todos os cartões bancários, de crédito, de débito ou duais.

relativamente ao crime de Falsidade Informática, a punição dos comportamentos denominados de *"Skimming"* e de *"Carding"*, de forma taxativa, indiferentemente do tipo de cartão bancário em causa, esvaziando assim, o sentido útil que se vinha retirando da interpretação constante na alínea c) do número 1, do artigo 267.º do Código Penal.

Razão pela qual não se alcança a fundamentação que é normalmente avançada pelos tribunais superiores, quando se pronunciam por factos subsumíveis a este tipo legal de crime.

A acrescer a esse facto a jurisprudência nacional, pese embora o tenha feito em apenas nos quatro acórdãos que foram já objeto de análise na presente dissertação, ao invés de aplicar este novo tipo legal aos mencionados comportamentos ilícitos ou seja, o previsto na Lei do Cibercrime, optou por puni-los em sede de concurso efetivo com o crime de Contrafação de Moeda, previsto no artigo 262.º, por remissão da previsão legal constante na alínea c) do número 1, do artigo 267.º, ambos do Código Penal.

Entendemos que as penas aplicadas com base nesta fundamentação, violam, de forma clara, o *non bis in idem*, uma vez que tal como já oportunamente referimos, está-se a efetuar uma dupla valoração proibida do mesmo facto, no seu sentido normativo-social.

A doutrina fundamenta a existência de um concurso efetivo entre os crimes de Contrafação de moeda, previsto no artigo 262.º, por remissão da previsão legal constante na alínea c) do número 1, do artigo 267.º, ambos do Código Penal e de Falsidade Informática, previsto no artigo 3.º, números 1 e 2 da Lei 109/2009, de 15 de setembro, com diversos argumentos, algo redundantes, senão vejamos;

Paulo Pinto de Albuquerque (Albuquerque P. P., 2015, p. 948)[106], entende existir concurso efetivo entre os mencionados crimes, remetendo essa fundamentação para o acórdão do Tribunal da Relação de Lisboa relativo ao processo 189/09.3JASTB.L1-5, já atrás analisado, bem ainda para um acórdão do Supremo Tribunal de Justiça, datado de 4.6.1998, ou seja, muito anterior à entrada em vigor no nosso ordenamento jurídico da Lei do Cibercrime, e, por maioria de razão, totalmente desenquadrado desta discussão, e por último, remete ainda para a doutrina vertida no acórdão do Tribunal da Relação de Lisboa, relativo ao processo 7876/10.1JFLSB.L1-5.

Ou seja, este autor, a toda esta problemática, nada acrescenta de novo, e muito menos algo verdadeiramente inovador.

Relativamente aos autores M. Miguez Garcia e J.M. Castela Rio, no seu Código Penal, parte Geral e Especial, com notas e comentários (Garcia & Rio, 2015, p. 1093)[107], mantêm

106 Anotação n.º 15.

107 Anotação n.º 6.

idêntico raciocínio, no que tange à existência de um concurso efetivo entre os crimes de Contrafação de Moeda, previsto no artigo 262.º, por remissão da previsão legal constante na alínea c) do número 1, do artigo 267.º, ambos do Código Penal e de Falsidade Informática, previsto no artigo 3.º, números 1 e 2 da Lei 109/2009, de 15 de setembro, remetendo, no entanto, a respetiva fundamentação, para a já mencionada doutrina subjacente ao acórdão do Tribunal da Relação de Lisboa relativo ao processo 7876/10.1JFLSB.L1-5, ou seja, uma vez mais, estes autores, igualmente, nada de novo acrescentam a esta temática, tornando toda a sua fundamentação, como a da restante doutrina, como aquela que acaba por ser acolhida pela jurisprudência, redundantes.

Por outro lado, este tipo de solução encontrada pela jurisprudência para punir estes comportamentos criminosos, tem subjacente um enorme problema operativo.

Como já se referiu ao longo da presente dissertação, os agentes destes tipos de crimes, são maioritariamente oriundos de países do leste Europeu, e do continente Africano, tendo ambos, em comum, o facto de se tratarem de estrangeiros em solo nacional.

Assim, se tais comportamentos fossem reconduzidos, tal como deveriam ser, ao tipo legal previsto no artigo 3.º da Lei do Cibercrime, o de Falsidade Informática, levantar-se-ia um impedimento legal, nomeadamente aquele que se prende com a imperiosa necessidade, devidamente fundamentada, de lhes vir a ser aplicada uma medida de coação privativa da liberdade, por força da previsão legal constante na alínea a) do número 2 do artigo 257.º, e, alínea a), do número 1, do artigo 202.º, ambos do Código de Processo Penal, ou seja, tendo em conta o facto de que o tipo legal de Falsidade Informática ter como limite da medida da pena os 5 anos de prisão, existe o impedimento legal, para que fora de flagrante delito, os agentes possam vir a ser detidos, para posterior sujeição a primeiro interrogatório judicial, e de lhes vir a ser aplicada uma medida de coação privativa da liberdade, impedindo que estes se coloquem em fuga, eximindo-se, dessa forma, à ação da justiça, com exceção de que no processo haja sido demonstrada a envolvência dos autores numa estrutura típica de uma associação criminosa, aplicando-se dessa forma os pressupostos constantes na alínea c), *in fine*, do n.º 1, do 202.º, do Código de Processo Penal.

No entanto, esse será um problema, que competirá ao legislador resolver, sem que para tal, se imponham ao arguido, um incomportável sacrifício dos seus direitos fundamentais, ínsitos na nossa Constituição da República Portuguesa, e densificados em sede do Código de Processo Penal.

Assim, sugere-se que *de jure constituindo*, sejam, no mais curto espaço de tempo possível, efetuadas as necessárias alterações à Lei do Cibercrime, que garantam por um

lado o termo à dúvida que ainda persiste, tanto na doutrina, como na jurisprudência, se o artigo 3.º da mencionada lei, contempla ou não todos os comportamentos ilegítimos exercidos sobre os cartões bancários, indiferentemente daqueles se tratarem de cartões de débito, de crédito, ou duais, e por outro, a respetiva moldura legal seja ou aumentada, para um número de anos de prisão superior aos atuais 5 anos de prisão, o que causa desnecessárias entropias aos operadores de justiça ou, o crime de Falsidade Informática ser incluído no catálogo de crimes previstos na alínea d), do n.º 1, do 202.º, do Código de Processo Penal, tal como foi o de Burla Informática.

Desta forma, evitava-se que os autores deste tipo de crimes, ao lhes serem aplicadas medidas de coação diversas da prisão preventiva, se colocassem em fuga, ausentando-se do nosso país, e eximindo-se dessa forma à respetiva punição pela aplicação da lei penal nacional.

Bibliografia

Silva, G. M. (2015). *Direito penal português, teoria do crime.* Lisboa: Universidade Católica Portuguesa.

Aguiar, A. L. (1990). *Dinheiro de Plástico: cartões de crédito, de débito e novos meios de pagamento.* Lisboa: Rei dos Livros.

Albuquerque, P. P. (2015). *Comentário do Código Penal, à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem.* Lisboa: Católica Editora.

Albuquerque, P., & Verdelho, P. (2010). *Comentário das leis penais extravagantes* (Vol. I). Lisboa: Universidade Católica Editora.

Antunes, M., & Rodrigues, B. (2018). *Introdução à Cibersegurança – A Internet, os aspetos legais e a análise digital forense.* FCA – Editora de Informática.

Antunes, M., & Rodrigues, B. (2018). *Introdução à Cibersegurança: A internet, os aspetos legais e a análise digital forense.* Lisboa: FCA - Editora de Informática.

BdP. (11/2001). Aviso.

BdP. (2004). Obtido em Novembro de 2018, de https://www.bportugal.pt/: http://www.bbs.pt/publicacoes/BancodePortugal/BP6-CartoesBancarios.pdf

BdP. (23 de Novembro de 2018). *https://www.bportugal.pt/*. Obtido de https://clientebancario.bportugal.pt

BdP. (23 de Novembro de 2018). *https://www.bportugal.pt/*. Obtido em Dezembro de 2018, de https://clientebancario.bportugal.pt/pt-pt/o-que-sao-e-tipos-de-cartoes

Cadete, E. M. (s.d.). *www.mlgts.pt.* Obtido em Novembro de 2018, de https://www.mlgts.pt/xms/files/v1/Publicacoes/Artigos/538.PDF

Cavaleiro de Ferreira, M. (1987). *Lições de direito penal* (Vol. I). Editorial Verbo.

Cibercrime, R. E. (s.d.). *https://www.coe.int*. Obtido em Novembro de 2018, de <https://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Documents/Convention%20and%20protocol/ETS_185_Portugese-ExpRep.pdf

Cordeiro, A. M. (2016). *Direito bancário.* Almedina.

Correia, E. H. (1963). *A teoria do concurso em direito criminal.* Livraria Almedina.

Dias, J. d. (1999). *Comentário Conimbricense do Código Penal, Parte Especial* (Vol. Tomo II). Coimbra: Coimbra Editora.

Dias, J. d. (2007). *Direito penal - parte geral - questões fundamentais - a doutrina geral do crime* (Vol. I). Coimbra editora.

Fernandes, J. M. (1998). *Tudo o que deve saber sobre Cartões Bancários.* Lisboa: Editora Estar.

Ferreira, A. C. (2011). *A Introdução dos cartões de crédito em portugal (1960 – 1975).* Lisboa: Edições Afrontamento.

Garcia, M. M., & Rio, C. J. (2015). *Código penal, parte geral e especial.* Coimbra: Almedina.

Guimarães, M. R. (2013). *A fraude no comércio eletrónico: o problema da repartição do risco por pagamentos fraudulentos.* Coimbra editora.

Guimarães, M. R. (s.d.). *https://repositorio-aberto.up.pt.* Obtido em Novembro de 2018, de https://repositorio-aberto.up.pt/bitstream/10216/23897/2/49708.pdf

Leal-Henriques, M. d., & Simas Santos, M. J. (2000). *Código penal anotado - 3.ª edição* (Vol. II). Lisboa, Portugal: Rei dos Livros.

Leite, I. F. (2016). *Ne (idem) bis inidem, proibição de dupla punição e de duplo julgamento: contributos para a racionalidade do poder punitivo público* (Vol. II). Lisboa: AAFDL.

Lobo, F. G. (2015). *Código de processo penal, anotado.* Coimbra: Almedina.

Nunes, D. R. (2018). *Os meios de obtenção de prova previstos na lei do cibercrime.* Coimbra: GESTLEGAL.

Pereira, C. F. (1990). *https://portal.oa.pt/.* Obtido em 2018, de https://portal.oa.pt/upl/%7B14b68ee3-ec16-4bc9-a321-6f522607363a%7D.pdf

Ramalho, D. S. (2017). *Métodos ocultos de investigação criminal em ambiente digital.* Coimbra: Almedina.

Rodrigues, A. (1997). Obtido em Novembro de 2018, de https://www.ine.pt/ngt_server/attachfileu.jsp?look_parentBoui=106912&att_display=n&att_download=y

Rodrigues, B. M. (Março de 1999). *Relatório sobre o fórum europeu de conhecimento sobre contrafação de cartões de crédito,.* RESERVADO, Polícia Judiciária, Londres.

Simas Santos, M., & Leal-Henriques, M. (2014). *Código penal anotado* (Vol. I). Parede: Rei dos Livros, letras e conceitos lda.

Simas Santos, M., & Leal-Henriques, M. (2016). *Noções de direito penal.* Rei dos Livros, letras e conceitos lda.

Simas, D. V. (2014). *O cibercrime.* Dissertação de Mestrado, Universidade Lusófona de Humanidades e Tecnologias., Direito, Lisboa.

Venâncio, P. D. (2011). *Lei do cibercrime - anotada e comentada.* Coimbra: Coimbra Editora.

Verdelho, P. (2003). *Direito da sociedade de informação* (Vol. IV). Editora Coimbra.

Verdelho, P. (2009). *A nova lei do cibercrime, in scientia ivridica, revista de direito comparado – português e brasileiro* (Vols. Tomo LVIII-Número 320). Portugal: Coimbra Editora.

Verdelho, P., Gouveia, J. B., & Santos, S. (2015). *Enciclopédia de direito e segurança.* Almedina.

Jurisprudência

Acórdão do Tribunal da Relação de Lisboa, proferido no âmbito do processo 189/09.3JASTB.L1-5, de 30/06/2011, consultável em: http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/fd8c21bdd02218c0802578d30030770e?OpenDocument

Acórdão do Tribunal da Relação de Lisboa, proferido no âmbito do processo 7876/10.1JFLSB.L1-5, de 10/07/2012, consultável em: http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/e6182f4e3c05f8b480257a68004d5a67?OpenDocument

Acórdão do Tribunal da Relação do Porto, proferido no âmbito do processo 1001/11.9JAPRT.P1, de 21-11-2012, consultável em: http://www.dgsi.pt/jtrp.nsf/c3fb530030ea1c61802568d9005cd5bb/f756eafb8a57bac380257ada003ae7f9?OpenDocument

Acórdão do Tribunal da Relação do Porto, proferido no âmbito do processo 2013/13.3JAPRT.P1, de 17-09-2014, consultável em: http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/5fd1df126b7ffe9880257d6600370f95?OpenDocument