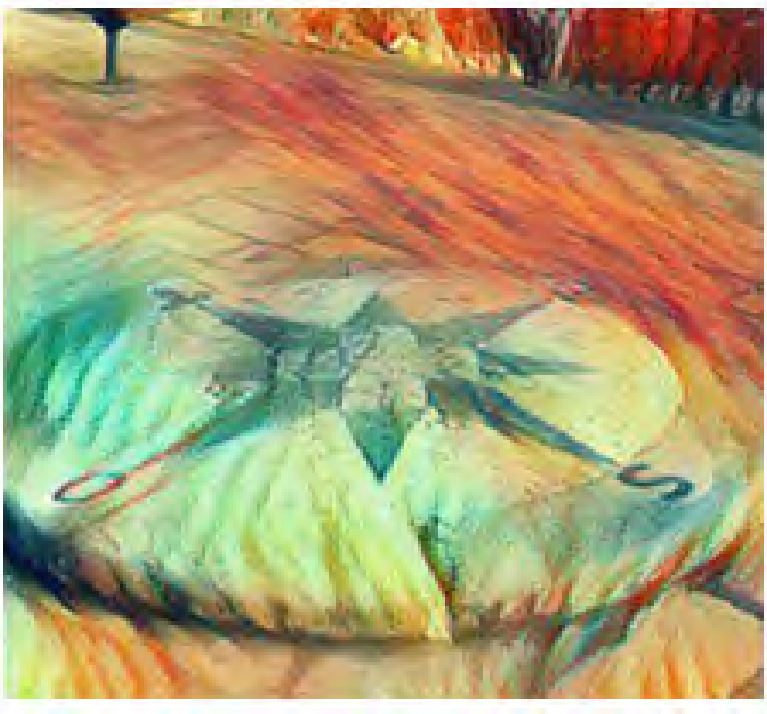
COLEÇÃO FORMAÇÃO — MINISTÉRIO PÚBLICO

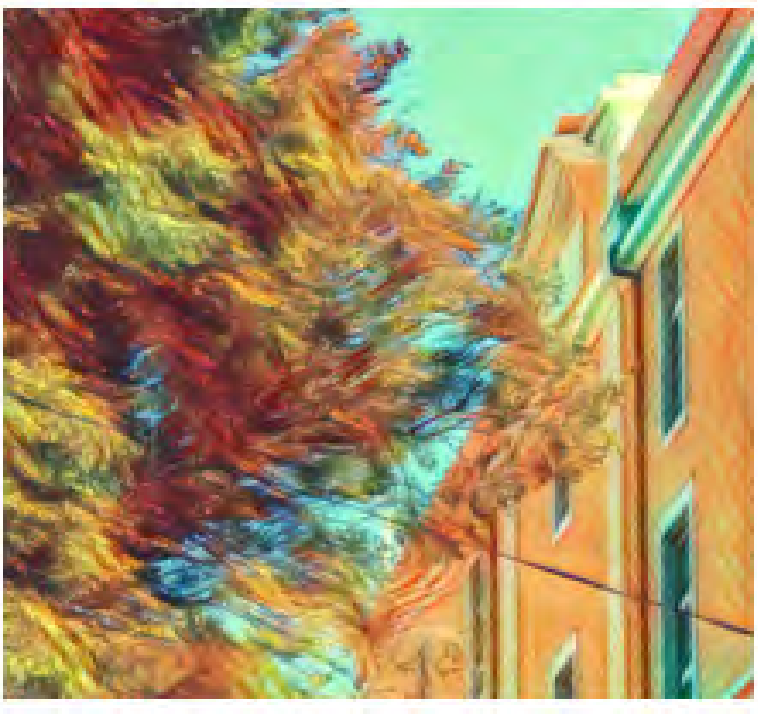
O CRIME DE ABUSO DE CARTÃO DE GARANTIA E CRÉDITO E O CRIME DE BURLA INFORMÁTICA

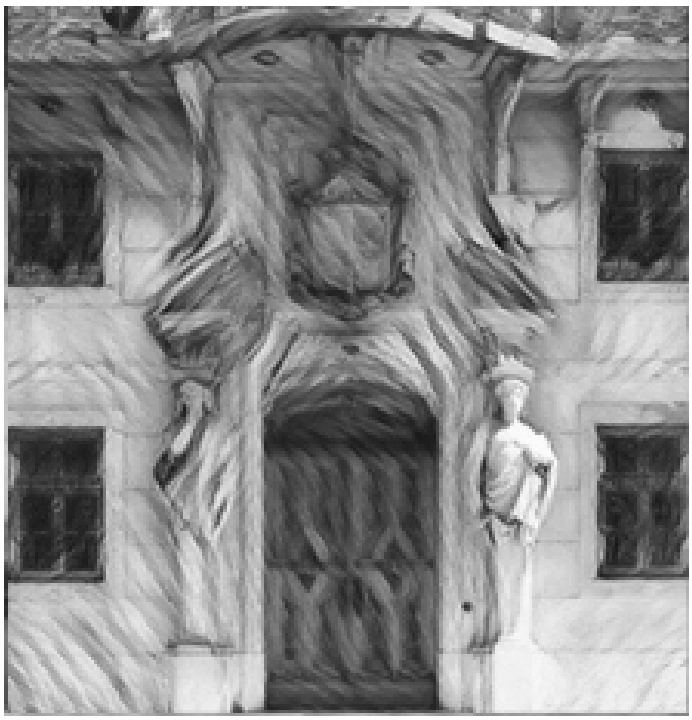
TRABALHOS DO 2.º CICLO DO 32.º CURSO

MAIO 2019

CENTRO DE ESTUDOS JUDICIÁRIOS







Diretor do CEJ: João Manuel da Silva Miguel, *Juiz Conselheiro*

Diretores Adjuntos:
Paulo Alexandre Pereira Guerra, *Juiz Desembargador*
Luís Manuel Cunha Silva Pereira, *Procurador-Geral Adjunto*

Coordenador do Departamento de Formação:
Edgar Taborda Lopes, *Juiz Desembargador*

Coordenadora do Departamento de Relações Internacionais:
Helena Leitão, *Procuradora da República*

Grafismo: Ana Caçapo, *CEJ*

Fotos da capa: Edifício da Procuradoria Geral da República,Rosa dos ventos na PGR, Rosa dos ventos e pormenor da fachada do CEJ.

Apresentação

Dando continuidade à publicação da série de *e-books* da colecção Formação – Ministério Público "Trabalhos Temáticos de Direito e Processo Penal", o Centro de Estudos Judiciários tem o grato prazer de proceder à divulgação dos volumes que compreendem os trabalhos temáticos realizados pelos auditores de justiça do 2.º ciclo, do 32.º Curso de Formação.

Como introdução a estes volumes remete-se, em grande medida, para as considerações efectuadas no momento da publicação dos seus antecessores.

Sem embargo, não será de mais salientar que as fases designadas por 2.º Ciclo e Estágio, que se desenrolam num contexto puramente judiciário e que correspondem a dois terços de toda a formação inicial organizada pelo Centro de Estudos Judiciários, constituem um tempo e um lugar onde se visa a qualificação de competências e práticas e o conferir de uma coerente sequência ao quadro de objectivos pedagógicos e avaliativos definidos como estruturantes para a preparação dos futuros magistrados do Ministério Público.

Neste contexto, a par da formação pessoal (*o saber e o saber-ser*) é fundamental continuar a desenvolver nessas fases formativas a dimensão institucional, traduzida na aquisição e aperfeiçoamento de competências, cultura, ética e deontologia judiciárias (o *saber-fazer* e o *saber-estar*).

Os *e-books* que agora se publicam recolhem o conjunto dos trabalhos elaborados pelos auditores de justiça do Ministério Público em formação no 2.º ciclo para a denominada *semana temática*, enquanto componentes de um modelo de avaliação que pretendeu privilegiar fins formativos.

A centralização da actividade onde foram publicamente apresentados, a dinamização que nela imprimiram os seus promotores, e o bom acolhimento que a iniciativa teve por parte dos formandos, permitiu confirmar o seu significado e impacto efectivo na execução de uma estratégia pedagógica coerente.

A apresentação dos trabalhos temáticos serviu de teste à validação das competências práticas que foram sendo adquiridas na comarca junto dos formadores, ao mesmo tempo que se avaliaram competências de adequação e de aproveitamento quanto a todos os auditores, uma vez que a aludida apresentação ocorreu na mesma oportunidade, perante os mesmos avaliadores e perante os pares, que assim também beneficiaram de efectiva formação.

Tratou-se, pois, de uma excelente oportunidade para apreciar competências relativas a todos os parâmetros avaliativos, tanto no que se refere ao estrito aproveitamento como, também, à adequação.

Pelo trabalho escrito foi possível avaliar, entre outros, o conhecimento das fontes, a destreza do recurso às tecnologias de informação e comunicação, a eficácia da gestão da informação, a gestão do tempo, o domínio dos conceitos gerais, o nível de conhecimentos técnico-jurídicos, a capacidade de argumentação escrita e oral, a capacidade de síntese ou o nível de abertura às soluções plausíveis. Por seu turno, a apresentação oral permitiu fazer um juízo sobre aspectos da oralidade e do saber-estar, sociabilidade e adaptabilidade (trabalho de equipa), permitindo igualmente a apreciação da destreza de cada auditor no que respeita à capacidade de investigação, à capacidade de organização e método, à cultura jurídica, à capacidade de ponderação e, sobretudo, à atitude na formação, que tem de ser (ainda que difícil e exigente) uma atitude de autonomia e responsabilidade.

A tónica na preparação e supervisão dos trabalhos pelos coordenadores regionais assentou sobretudo nos aspectos da prática e da gestão do inquérito ou da gestão processual, que são tão mais importantes quanto impõem aos auditores uma transição entre a teoria e a prática, evitando-se trabalhos com intuito e conteúdo exclusivamente académico.

É inegável que alguns temas têm dificuldades associadas, mesmo na circunscrição de um objecto passível de tratar em espaço e tempo limitados. Essa foi também uma oportunidade de testar a capacidade de gestão da informação e mesmo da destreza na identificação e formulação das questões essenciais, o nível de abertura às soluções plausíveis, a autonomia e personalização e o sentido prático e objectividade. A opção do

auditor, face ao tempo e espaço limitados de que dispõe, envolverá sempre riscos e a circunscrição do objecto do trabalho revelará a inteligência, o sentido prático, o grau de empenhamento individual e respectivo nível de iniciativa, de capacidade de indagação e de capacidade de gestão da informação.

Estes trabalhos não pretendem que, através deles, o futuro magistrado cultive a polémica, a retórica ou o academismo do direito sem experiência e sem aplicação. Trata-se de uma oportunidade para teorizar a prática, em consonância com a fase de formação de 2.º ciclo, fazendo com que a *praxis* se abra à pluralidade de contextos sociais, económicos, comunicacionais, político-legislativos, em atenção concomitante aos sentimentos e opiniões sociais que fazem apelo às ideias de Justiça, reclamando dos princípios e normas a capacidade de se adaptarem a esses contextos e às suas mutações.

Uma breve nota final descritiva da forma como se operacionalizou a elaboração destes trabalhos:

Na sequência de prévias reuniões dos coordenadores com o Director Adjunto, foram seleccionadas as temáticas que viriam a constituir o objecto dos trabalhos escritos.

Seguidamente foram difundidas aos auditores as seguintes orientações:

a) Um tema para cada grupo de 4 auditores de justiça (sem possibilidade de repetição).
b) Cada trabalho temático escrito seria individual, sujeito a avaliação.
c) A escolha do tema e a constituição de cada grupo de auditores por tema decorreu de forma consensual entre os auditores de justiça.
d) Foi fixada uma data limite para o envio do trabalho escrito e do suporte da respectiva apresentação aos coordenadores regionais.
e) O trabalho escrito teve o limite de 30 páginas A4.
f) A apresentação oral teve lugar no Centro de Estudos Judiciários, em Lisboa, em Junho de 2018.
g) Nas apresentações orais foram utilizados meios de apoio, designadamente, o recurso a *data-show* (suporte «*powerpoint*» ou «*Prezi*»).

h) Os auditores de justiça que trabalharam o mesmo tema, sempre na prossecução do conceito de trabalho em equipa, foram encarregados de se articularem entre si, empreendendo as diligências necessárias por forma a investirem, na oportunidade devida, numa apresentação oral que resultasse coordenada, lógica e sequencial, sem repetição de conteúdos e portanto operada num contexto de partilha de saber e de estudo e com observância do limite temporal fixado.

i) A comparência foi obrigatória para todos os auditores de justiça (incluindo nos dias que não estiveram reservados à respectiva intervenção).

Luís Manuel Cunha da Silva Pereira
Director-Adjunto do Centro de Estudos Judiciários
Jorge Manuel Vaz Monteiro Dias Duarte
Coordenador Regional Norte – Ministério Público
Ângela Maria B. M. da Mata Pinto Bronze
Coordenadora Regional Centro – Ministério Público
José Paulo Ribeiro de Albuquerque
Coordenador Regional Lisboa – Ministério Público
Olga Maria Caleira Coelho
Coordenadora Regional Sul – Ministério Público

Ficha Técnica

Nome:

O Crime de Abuso de cartão de garantia e crédito e o Crime de Burla Informática

Coleção:

Formação Ministério Público

Conceção e organização:

Luís Manuel Cunha da Silva Pereira (Director-Adjunto do Centro de Estudos Judiciários)
Jorge Manuel Vaz Monteiro Dias Duarte (Coordenador Regional Norte – Ministério Público)
Ângela Maria B. M. da Mata Pinto Bronze (Coordenadora Regional Centro – Ministério Público
José Paulo Ribeiro de Albuquerque (Coordenador Regional Lisboa – Ministério Público)
Olga Maria Caleira Coelho (Coordenadora Regional Sul – Ministério Público)

Intervenientes:

Catarina Gomes Pedra*****
Catarina Rodrigues*****
Dália Sotero Palma*****
Maria José Clara Sousa*****
Nuno Filipe de Sousa Gonçalves*****
Paulo Luís Rodrigues Mota*****
Rui Miguel Ferreira dos Santos Cruz*****
Rui Miguel Lima Alves*****

Revisão final:

Edgar Taborda Lopes – Juiz Desembargador, Coordenador do Departamento da Formação do CEJ
Ana Caçapo – Departamento da Formação do CEJ
Lucília do Carmo – Departamento da Formação do CEJ

* Auditores/as de Justiça do 32.º Curso de Formação de Magistrados – MP à data da apresentação dos trabalhos.

Notas:

Para a visualização correta dos e-books recomenda-se o seu descarregamento e a utilização do programa Adobe Acrobat Reader.

Foi respeitada a opção dos autores na utilização ou não do novo Acordo Ortográfico.

Os conteúdos e textos constantes desta obra, bem como as opiniões pessoais aqui expressas, são da exclusiva responsabilidade dos/as seus/suas Autores/as não vinculando nem necessariamente correspondendo à posição do Centro de Estudos Judiciários relativamente às temáticas abordadas.

A reprodução total ou parcial dos seus conteúdos e textos está autorizada sempre que seja devidamente citada a respetiva origem.

Forma de citação de um livro eletrónico (NP405-4):

AUTOR(ES) – **Título** [Em linha]. a ed. Edição. Local de edição: Editor, ano de edição.
[Consult. Data de consulta]. Disponível na internet: <URL:>. ISBN.

Exemplo:
Direito Bancário [Em linha]. Lisboa: Centro de Estudos Judiciários, 2015.
[Consult. 12 mar. 2015].
Disponível na
internet: <URL: http://www.cej.mj.pt/cej/recursos/ebooks/civil/Direito_Bancario.pdf.
ISBN 978-972-9122-98-9.

Registo das revisões efetuadas ao e-book

Identificação da versão	Data de atualização
1.ª edição – 17/05/2019	

O Crime de Abuso de cartão de garantia e crédito e o Crime de Burla Informática

Índice

CENTRO
DE ESTUDOS
JUDICIÁRIOS

1.

Crime de burla informática e nas comunicações. Enquadramento jurídico, prática e gestão processual

Catarina Gomes Pedra

CENTRO
DE ESTUDOS
JUDICIÁRIOS

1. CRIME DE BURLA INFORMÁTICA E NAS COMUNICAÇÕES. ENQUADRAMENTO JURÍDICO, PRÁTICA E GESTÃO PROCESSUAL

Catarina Gomes Pedra

Índice

I. Introdução

Num mundo em constante mutação, a evolução tecnológica e a crescente utilização dos computadores, bem como os riscos inerentes, tais como a manipulação fraudulenta dos computadores e programas informáticos, a introdução de dados inexatos no computador ou no sistema informático e o acesso e utilização indevidos de dados ou outras ingerências no tratamento de dados, leva(ra)m à constatação da incapacidade operativa dos tradicionais conceitos de crime para prevenir e reprimir a nova criminalidade, tornando premente – até pelo efeito dissuasor que se lhe reconhece – a necessidade de adequação do sistema jurídico-penal àquele desenvolvimento.

No âmbito da referida adequação, e à semelhança do caminho trilhado em outros países da Europa Ocidental, o legislador nacional procedeu à construção de uma figura jurídico-penal que, inspirada no tipo legal da burla, procurou colmatar as lacunas de punibilidade resultantes da inadequação das figuras criminais de conteúdo patrimonial tradicionais para a punição de determinadas condutas fraudulentas que, prescindindo, embora, do erro ou engano de qualquer pessoa, se concretizam em formas de manipulação informática lesivas do património

e se apresentam marcadas, entre o mais, pelo automatismo, permanência e por um específico *modus operandi*.

Foi neste contexto, e na esteira da experiência germânica, que o crime de burla informática, que não encontrava previsão na versão originária do Código Penal (1982), foi introduzido no sistema jurídico-penal português em 1995, com a revisão operada pelo Decreto-Lei n.º 48/95, de 15 de março.

Posteriormente, e ainda com o ensejo de adaptar a legislação penal aos desafios colocados pela nova criminalidade, na Reforma do Código Penal de 1998 operada pela Lei n.º 65/98, de 2 de setembro, foi introduzido o crime de burla nas comunicações, colhendo este ilícito criminal previsão no n.º 2 do artigo 221.º, daquele diploma legal.

II. Objetivos

O presente trabalho – cuja pertinência se prende, desde logo, com o aumento generalizado da criminalidade informática – tem como escopo proceder a uma análise dogmática dos tipos legais de crime de burla informática e de burla nas comunicações, bem como a uma abordagem, de pendor mais prático, das dificuldades de prova que a investigação destes crimes evidencia, procedendo-se, neste particular, a uma análise dos meios de obtenção de prova e meios de prova que se revelam pertinentes à investigação da existência do crime e à determinação do(s) respetivo(s) agente(s) e à responsabilidade dele(s), e, bem assim, das formas de encerramento do inquérito legalmente previstas e que, em concreto, se revelam aplicáveis.

É, assim, nosso objetivo que este trabalho auxilie os Auditores de Justiça e Magistrados do Ministério Público na sua vida prática, contribuindo para a compreensão dos crimes de burla informática e nas comunicações, auxiliando na superação de algumas dificuldades – teóricas e práticas – que a sua aplicação suscita.

III. Resumo

O presente trabalho tem como objeto de estudo os crimes de burla informática e nas comunicações que colhem previsão no artigo 221.º, n.ºs 1 e 2, respetivamente, do Código Penal.

Uma vez que a análise destes tipos legais de crime se insere num tema mais amplo, que é o da *criminalidade informática*, começaremos por uma abordagem, de teor geral e histórico, mas necessariamente concisa, da influência da evolução tecnológica e dos meios informáticos no Direito Penal e dos desafios que a nova criminalidade coloca aos sistemas jurídico-penais.

Após uma análise das motivações que levaram o legislador nacional a introduzir no Código Penal, na Reforma operada em 1995, o crime de burla informática, passaremos ao estudo do

seu enquadramento jurídico-penal, refletindo sobre o bem jurídico (bens jurídicos?) protegido(s) pela incriminação, a natureza do crime, abordando depois os respetivos elementos típicos (objetivos e subjetivos).

Terminaremos a análise do crime de burla informática com a problemática da relação que intercede entre este tipo de crime e outros previstos no Código Penal e na Lei do Cibercrime; abordagem que assentará, essencialmente, nos contributos da doutrina nacional e na experiência que a jurisprudência dos tribunais superiores portugueses, a propósito, revela.

De seguida, e de forma semelhante, procederemos à análise dogmática do tipo legal de crime de burla nas comunicações, abordando as questões do bem jurídico protegido pela incriminação, a natureza do crime e respetivos elementos típicos (objetivos e subjetivos).

Para finalizar a análise dogmática dos tipos de crime em estudo, e por uma questão de facilidade expositiva, abordaremos os aspetos comuns a ambos os ilícitos (moldura penal, punibilidade da tentativa, natureza dos crimes, responsabilidade das pessoas coletivas e aplicabilidade do regime legalmente previsto de restituição ou reparação).

No último Capítulo, e uma vez que os crimes cometidos com recurso a meios tecnologicamente avançados acarretam dificuldades de prova acrescidas, sendo pela elevada tecnicidade, especialidade e, tantas vezes, transnacionalidade que os caracterizam, de difícil deteção e comprovação, centraremos a nossa atenção na problemática dos meios de obtenção de prova e dos meios de prova previstos na Lei n.º 109/2009, de 15 de setembro (Lei do Cibercrime), e no Código de Processo Penal que se revelam pertinentes à investigação da existência do crime e à determinação do(s) respetivo(s) agente(s) e à responsabilidade dele(s).

Por fim, e ainda que de forma sumária, faremos referência às formas legalmente previstas de encerramento do inquérito que, atenta a concreta criminalidade em causa, se revelam aplicáveis.

1. As novas tecnologias e os meios informáticos – o repensar das soluções jurídico-penais tradicionais

Num mundo em constante mutação e aceleração, a crescente evolução tecnológica permite o aparecimento de novos crimes e de meios diversos de cometimento dos crimes ditos tradicionais – que, assim, se *modernizam* e se *facilitam* – com o *animus* de obtenção de elevados benefícios económicos.

No contexto da compreensão do uso (melhor será dizer, abuso) das novas tecnologias para efeitos de cometimento de crimes, é frequente a utilização, na dogmática jurídico-penal, da expressão *criminalidade informática*. Pese embora a definição e a circunscrição do âmbito de aplicação daquele conceito não se revelem, no estádio atual, uniformes, pode dizer-se, acompanhando GARCIA MARQUES e LOURENÇO MARTINS, que se refere a *"(…) todo o ato em*

que o computador serve de meio para atingir um objetivo criminoso ou em que o computador é o alvo simbólico desse ato ou em que o computador é o "objeto" do crime."[1]

Não obstante as virtualidades da acelerada evolução tecnológica, o aproveitamento dos meios informáticos e telemáticos para finalidades ilegais coloca a descoberto as fragilidades da atual sociedade digital, isto é, a perda de confiança e a insegurança.

Em face da constatação do desenvolvimento da criminalidade informático-digital, o Comité de Ministros dos Estados-Membros do Conselho da Europa adotou, em 13 de setembro de 1989, a **Recomendação n.º R (89) 9 relativa à criminalidade informática**, na qual constavam duas *listas* de incriminações: uma *lista mínima*, contendo um conjunto de condutas que teriam obrigatoriamente de ser punidas pelo direito interno dos Estados-Membros; e uma *lista opcional*, contendo, por sua vez, condutas cuja criminalização se apresentava como facultativa. De entre as condutas previstas na referida *lista mínima* destaca-se, pela proximidade àquela que viria a ser a construção típica da figura da burla informática em Portugal, a *"computer fraud"*.[2]

Posteriormente, no contexto internacional, foi adotada em 23 de novembro de 2001, em Budapeste, a **Convenção sobre o Cibercrime**, assinada pelo Estado Português no dia da sua adoção e ratificada em 15 de Setembro de 2009.[3]

A referida Convenção do Conselho da Europa surge animada pelos propósitos de proceder à harmonização da cibercriminalidade, prevendo, para tal, um conjunto de infrações[4], e, bem assim, de dotar os direitos nacionais dos mecanismos processuais necessários à investigação destes crimes e de instituir um regime célere e eficaz de cooperação internacional.

Também no contexto da União Europeia se tornou evidente a necessidade de responder adequadamente aos desafios colocados pela natureza transfronteiriça dos modernos sistemas de informação e de, procedendo à harmonização das legislações e impulsionando a cooperação em matéria penal, facultar aos cidadãos um elevado nível de proteção num espaço de liberdade, segurança e justiça, como resulta imposto pelo artigo 29.º, do Tratado da União Europeia.

---

[1] MARQUES, Garcia/ MARTINS, Lourenço – *Direito da Informática*, 2.ª Edição Refundida e Atualizada, Coimbra: Almedina, 2006, pág. 641. Para uma visão geral sobre a evolução da criminalidade informática, *vide* SANTOS, Rita Coelho – *O Tratamento Jurídico-Penal da Transferência de Fundos Monetários Através da Manipulação Ilícita dos Sistemas Informáticos*, Coimbra: Coimbra Editora, 2005, págs. 43 a 47.

[2] "COMPUTER FRAUD - The input, alteration, erasure or suppression of computer data or computer programs, or other interference with the course of data processing, that influences the result of data processing thereby causing economic or possessory loss of property of another person with the intent of procuring an unlawful economic gain for oneself or for another person".

[3] Sobre a evolução legislativa em matéria de criminalidade informática, *vide* MARQUES, Garcia/ MARTINS, Lourenço – *Op. Cit.*, págs. 639 e seguintes.

[4] Pela sua pertinência para o presente trabalho, destacamos o *crime de fraude informática* previsto no artigo 8.º da referida Convenção, através do qual se procura "(…) incriminar todas as condutas que se concretizem numa manipulação abusiva no decurso do tratamento de dados com vista a efectuar uma transferência ilícita de propriedade." Neste sentido, *vide* RODRIGUES, Benjamim Silva – *Da Prova Penal – Da Prova – Electrónico- Digital e da Criminalidade Informático-Digital*, Tomo IV, 1.ª Edição, Rei dos Livros, 2011, pág. 73.

No esforço intentado de dar adequada resposta à criminalidade cometida por via da tecnologia e da informática, sobreleva, de entre os instrumentos jurídicos adotados, a **Decisão-Quadro 2005/222/JAI do Conselho, de 24 de fevereiro de 2005**, cujo objetivo é a aproximação das disposições de direito penal dos Estados-Membros em matéria de ataques contra os sistemas de informação.

Ao nível de direito interno, procedeu-se à transposição daquela Decisão-Quadro através da **Lei n.º 109/2009, de 15 de setembro** (Lei do Cibercrime), que revogou a Lei n.º 109/91, de 17 de agosto (Lei da Criminalidade Informática), o primeiro diploma legal que, no ordenamento jurídico nacional, se revelou diretamente vocacionado para a previsão e regulamentação de crimes informáticos.

Paralelamente, na necessidade de compreender as novas realidades, redefinir conceitos e repensar soluções, os sistemas jurídicos têm procurado refúgio no Direito Penal, "(…) que na forma de "Direito Penal do Risco" responde numa lógica preventiva e antecipa a tutela dos bens jurídicos supraindividuais considerados essenciais."[5]

Assim, neste contexto, e como melhor se abordará no Capítulo que se segue, também o Código Penal português foi permeável às mutações verificadas, tendo o legislador nacional introduzido normas especificamente destinadas à repreensão de ofensas realizadas informaticamente, adequando, desta forma, e à semelhança do caminho trilhado em outros países da Europa Ocidental, a legislação penal aos desafios colocados pela nova criminalidade.

2. Burla informática

2.1. Considerações preliminares e breve referência histórica

A evolução tecnológica e a crescente utilização dos computadores – cada vez mais acessíveis –, bem como os riscos inerentes, tais como a manipulação fraudulenta dos computadores e programas informáticos, a introdução de dados inexatos no computador ou no sistema informático e o acesso e utilização indevidos de dados ou outras ingerências no tratamento de dados, leva(ra)m à constatação da incapacidade operativa dos tradicionais conceitos de crime para prevenir e reprimir a nova criminalidade, tornando premente – até pelo efeito dissuasor que se lhe reconhece – a necessidade de adequação do sistema jurídico-penal àquele desenvolvimento.

No âmbito da referida adequação, o legislador nacional procedeu à construção de uma figura jurídico-penal que, inspirada no tipo legal clássico da burla, procurou colmatar as (evidenciadas) lacunas de punibilidade resultantes da inadequação das *figuras criminais de*

[5] DIAS, Vera Marques – *A Problemática da Investigação do Cibercrime*, *in* "DataVenia" [Em linha], Ano 1, n.º 1, Julho 2012 [Consult. 20 Fev. 2018], disponível em https://www.datavenia.pt/ficheiros/edicao01/datavenia01_p063-088.pdf. Ainda sobre a *sociedade de risco* e suas implicações no Direito Penal, *vide* FERNANDES, Paulo Silva – *Globalização, "Sociedade de Risco" e o Futuro do Direito Penal – Panorâmica de Alguns Problemas Comuns*, Coimbra: Almedina, 2001, em especial págs. 71 e seguintes.

conteúdo patrimonial tradicionais[6] para a punição de determinadas condutas fraudulentas que, prescindindo, embora, do erro ou engano de qualquer pessoa, se concretizam em formas de manipulação informática lesivas do património e se apresentam marcadas, entre o mais, pelo automatismo, permanência e pela especificidade do *modus operandi* que as caracterizam. Podemos, assim, dizer, acompanhando MANUEL LOPES ROCHA, que o móbil da introdução legal do crime de burla informática no ordenamento jurídico-nacional foi a constatação das seguintes realidades:

> a) Frequência com que se verificaram utilizações abusivas de caixas automáticas;
> b) Existência de condutas que, em geral, envolvem riscos consideráveis para o comércio jurídico e para o tráfico ou sistemas de provas;
> c) Difícil deteção dessas condutas, que mereciam uma repulsa social cada vez mais forte
> d) Insuficiência dos tipos penais tradicionais (de enriquecimento patrimonial) para proteção do bem jurídico.[7]

Na verdade, e a propósito do último dos aspetos assinalados, pode, desde já, salientar-se que são elementos típicos do crime de burla o emprego de um processo enganatório astucioso e a circunstância de o agente determinar outrem à prática de atos causadores de prejuízo (para si ou para outra pessoa). Evidencia-se, assim, a existência de *"(…) um enlace entre uma conduta do agente e a uma conduta da vítima: aquela gera o processo enganatório, esta pratica os atos para os quais é determinada."*[8]

Diversamente, e como melhor resultará do estudo que, de seguida, encetaremos, no crime de burla informática não existe um processo enganatório incidente sobre uma pessoa, por via do qual esta seja determinada a adotar determinada conduta que lhe cause, ou cause a outrem, prejuízo patrimonial.

Na verdade, à semelhança de outras práticas criminosas, também a burla informática se caracteriza pela *despersonalização das condutas*[9], pelo que, sem a intermediação da vítima, consubstancia um *atentado direto ao património*[10] cuja especificidade reside no facto de ser levado a cabo através da utilização de meios informáticos.

Dito de outra forma – mais ilustrativa –, e acompanhando PAULO PINTO DE ALBUQUERQUE, o fundamento da tipificação *"(…) reside na circunstância de os computadores não poderem ser enganados, pelo que a manipulação informática com vista ao enriquecimento ilegítimo do agente ou de terceiro não se submete ao tipo clássico da burla (…)"*.[11]

---

[6] ROCHA, Manuel António Lopes – *A Revisão do Código Penal – Soluções de Neocriminalização*, *in* "Jornadas de Direito Criminal – Revisão do Código Penal", Centro de Estudos Judiciários, Lisboa, 1996, pág. 92.
[7] ROCHA, Manuel António Lopes – *Op. cit.*, pág. 93.
[8] BARREIROS, José António – *Crimes contra o património*, Lisboa: Universidade Lusíada, 1996, pág.156.
[9] SANTOS, RITA COELHO – *Op. cit.*, pág. 214.
[10] DIAS, Jorge de Figueiredo [dir.] – *Comentário Conimbricense do Código Penal*, Tomo II, Coimbra Editora, 1999, pág. 330. Em sentido discordante, defendendo tratar-se de uma *agressão mediatizada pelos meios informáticos*, SANTOS, RITA COELHO – *Op. cit.*, pág. 229.
[11] ALBUQUERQUE, Paulo Pinto de – *Comentário do Código de Processo Penal à luz da Constituição da República Portuguesa e da Convenção Europeia dos Direitos do Homem*, 3.ª Ed., Lisboa: Universidade Católica Editora, 2009,

Foi, assim, neste contexto, que o crime de burla informática, que não encontrava previsão na versão originária do Código Penal (1982), foi introduzido no sistema jurídico-penal português em 1995, com a revisão operada pelo Decreto-Lei n.º 48/95, de 15 de março, em cujo preâmbulo se refere que a neocriminalização assim operada se deve à *"(…) revelação de novos bens jurídico-penais ou de novas modalidades de agressão ou perigo (…)".*

Como ressalta RITA COELHO SANTOS, *"[A] premência da reforma penal [entre nós] impunha-se, pois era necessário acautelar a sociedade, em geral, e o tráfico jurídico-mercantil, em particular, face ao perigo das ofensas praticadas através da informática e da telemática, contra novas formas de riqueza, designadamente, o património sob a forma de dados eletrónicos."*[12]

A introdução do artigo 221.º foi alvo de discussão na Comissão de Revisão do Código Penal (conforme decorre da Ata n.º 39).[13] A posição acolhida pelo legislador foi a adotada pelo Conselheiro Sousa e Brito que, então, se pronunciou a favor da inclusão, em matéria de criminalidade informática, no Código Penal de um *tipo suficientemente esclarecido*, a burla informática.[14]

Como sobressai do debate então havido, foi intenção do legislador dotar o ordenamento jurídico-penal nacional de um regime idêntico àquele existente no sistema germânico. Colheu, assim, inspiração na *burla de computadores* (*Computerbetrug*)[15] prevista no § 263.a do StGB (*Straftgesetzbuch*) alemão e aí introduzida em 1986 pela Segunda Lei de Luta contra a Criminalidade Económica (*Zweites Gesetz zur Bekämpfung der Wirtschaftskriminalität – 2. WiKG*).

Alcançada a dita reforma com a introdução do crime de burla informática, cumpre agora proceder à análise deste ilícito criminal à luz do debate que, desde então, vem sendo firmado na doutrina e do caminho que vem sendo trilhado pela jurisprudência dos tribunais superiores portugueses.

pág. 859. Em sentido idêntico, GARCIA, M. Miguez/ RIO, J.M. Castela – *Código Penal Parte geral e especial com notas e comentários*, Coimbra: Almedina, 2014, pág. 908.

[12] SANTOS, Rita Coelho – Op. cit., pág. 197.

[13] Ministério da Justiça – *Código Penal – Actas e Projecto da Comissão de Revisão*, Lisboa: Rei dos Livros, 1993, págs. 453 a 455.

[14] Discordando desta inclusão, propugnando, ao invés, a previsão do tipo legal de burla informática na lei da criminalidade informática, BARREIROS, José António – *Op. cit.*, pág. 183. Manifestando reservas quanto à *opção neocriminalizadora* do legislador, sem, no entanto, colocar em causa a necessidade da previsão legal daquele tipo de crime, ROCHA, Manuel António Lopes – *Op. cit.*, pág. 92.

[15] É a seguinte a redação daquele normativo: "Quem, com a intenção de obter, para si ou para terceiro, um enriquecimento ilegítimo, causar um prejuízo patrimonial a terceiro, influindo no resultado de um tratamento de dados, mediante estruturação incorrecta do programa, utilização de dados incorrectos ou incompletos, utilização não autorizada de dados ou, então, através de intervenção não autorizada no seu processamento, será punido com pena prisão até 5 anos ou com pena multa."

2.2. Enquadramento jurídico-legal

2.2.1. Generalidades, bem jurídico protegido e natureza do crime

O crime de burla informática[16] encontra-se tipificado no artigo 221.º, n.º 1, do Código Penal, integrado no Titulo II que, na sistemática daquele diploma legal, prevê *os crimes contra o património*, mais concretamente no Capítulo III, relativo aos *crimes contra o património geral*.[17]

Como ressalta da sua inserção sistemática, da descrição típica e, bem assim, do fundamento teleológico da incriminação, o crime em análise comunga com os demais tipos de ilícito daquele Capítulo, a *referência ao património*.[18] Donde, e como vem sendo salientado pela doutrina, o **bem jurídico** protegido pela incriminação é o património.[19]

Porém, à semelhança do debate desenvolvido na doutrina italiana, alguma jurisprudência dos tribunais superiores portugueses vem entendendo – quanto a nós, com pertinência – que a burla informática é um crime pluri-ofensivo, alargando o caráter do bem jurídico protegido, aí englobando também a proteção da regularidade do funcionamento e da reserva da utilização dos sistemas informáticos.[20]

Relativamente à natureza do crime de burla informática, começando pelo grau de lesão do bem jurídico, trata-se de um **crime de dano**, na medida em que só se consuma quando ocorre um efetivo prejuízo patrimonial para outra pessoa.

A propósito, e partindo da conceção do crime de burla informática como ilícito que tutela o património, refere LEONES DANTAS que *"[E]ste prejuízo não é aquele que ocorre nos dados sobre os quais recaiu a ação do agente, porque esse é o espaço de um outro crime – os danos relativos a dados ou programas informáticos a que se refere o artigo 5.º, da Lei da Criminalidade Informática (Lei n.º 109/91, de 17 de agosto). Este prejuízo há de recair sobre o património da vítima, como consequência da manipulação de dados informáticos em que se subsume a ação do agente, o que permite aproximar o crime de burla informática dos outros crimes de burla, embora este tenha algumas diferenças de relevo relativamente à estrutura daqueles crimes."*[21]

---

[16] Sobre a *classificação* da burla informática como crime *tipicamente informático*, *vide* SANTOS, Rita Coelho – *Op. cit.*, pág. 32.
[17] Sobre a organização sistemática do Código Penal na parte relativa aos crimes contra o património, perspetiva histórica e concetual, *vide* BARREIROS, José António – Op. cit., págs. 5 e 6.
[18] Na expressão de GARCIA, M. Miguez/ RIO, J. M. Castela – *Op. cit.*, pág. 908.
[19] Neste sentido, SANTOS, Rita Coelho – *Op. cit.,* pág. 215, GARCIA, M. Miguez/ RIO, J.M. Castela – *Op. cit.,* pág. 935, ALBUQUERQUE, Paulo Pinto de – *Op. cit.,* pág. 608.
[20] Admitindo que o crime de burla visa proteger *secundariamente* o correto funcionamento e a inviolabilidade dos sistemas informáticos com aptidão para o desempenho das funções em vista da satisfação do utente, vide, entre outros, o Acórdão do Supremo Tribunal de Justiça de 20/10/2010, Relator: Pires da Graça, e o Acórdão do Supremo Tribunal de Justiça de 06/10/2005, Relator: Simas Santos, ambos acessíveis em www.dgsi.pt.
[21] DANTAS, Leones – *A Revisão do Código Penal e os Crimes Patrimoniais*, *in* "Jornadas de Direito Criminal do CEJ", Lisboa, 1998, págs. 514 e 515.

Trata-se ainda de um crime **material ou de resultado**, pois aquela consumação depende igualmente da saída dos bens ou valores da esfera de disponibilidade fáctica da vítima.
Na perspetiva da conduta do agente, cumpre, primeiramente, salientar que o legislador previu, de entre as modalidades de ação típica, uma cláusula geral (referimo-nos à intervenção por qualquer outro modo não autorizado no processamento) que, pela sua abrangência e elasticidade, permite abarcar uma multiplicidade de atuações não enquadráveis nas demais variantes legalmente previstas.

Não obstante, a burla informática apresenta-se ainda como um **crime de execução vinculada**, estando o respetivo *iter criminis* descrito na lei. Porém, tendo em conta a *tipologia aberta*[22] com que o crime vem previsto, e como salienta A. M. ALMEIDA COSTA, a referida *natureza vinculada* restringe-se à exigência, por um lado, de que a lesão do património seja o resultado da utilização de meios informáticos e, por outro, de que não se verifique o *modus operandi* da burla clássica.[23]

Por último, trata-se de um **crime comum**, na medida em que pode ser praticado por qualquer pessoa que, para o efeito, *"(…) tenha acesso a um sistema informático, aos dados a utilizar pelo mesmo ou à programação respetiva."* Por sua vez, o sujeito passivo da conduta criminosa é o titular do sistema informático ou a pessoa *"(…) cuja conduta patrimonial esteja dependente dos efeitos ou resultados de um sistema informático."*[24]

2.2.2. Tipo objetivo de ilícito

Preceitua o artigo 221.º, n.º 1, do Código Penal que *"Quem, com intenção de obter para si ou para terceiro enriquecimento ilegítimo, causar a outra pessoa prejuízo patrimonial, interferindo no resultado de tratamento de dados, ou mediante estruturação incorreta de programa informático, utilização incorreta ou incompleta de dados, utilização de dados sem autorização ou intervenção por qualquer outro modo não autorizado no processamento, é punido com pena de prisão até três anos ou com pena de multa."*

Procurando delimitar o escopo da nossa apreciação, deixamos uma nota para referir que, não obstante a amplitude da expressão legal *burla informática*, o crime de burla informática, entendido em sentido estrito e no rigor dos moldes típicos da sua previsão legal, distingue-se da burla praticada com (recurso a) meios informáticos. Na verdade, neste último caso estamos perante condutas em que o meio astucioso utilizado pelo agente para provocar o erro ou engano no sujeito passivo é o instrumento informático, havendo, em tudo o mais, coincidência com os elementos típicos da burla prevista no artigo 217.º, do Código Penal, quedando, portanto, tais condutas delituosas excluídas da nossa apreciação.

São, assim, elementos objetivos do crime de burla informática a *interferência no resultado* **de tratamento de dados através de** uma das seguintes variantes típicas:

[22] SANTOS, Rita Coelho – *Op. cit.,* pág. 240.
[23] DIAS, Jorge de Figueiredo [dir.] – *Op. cit.*, pág. 329.
[24] BARREIROS, José António – *Op. cit.,* pág. 184.

a) Estruturação incorreta de programa informático;
b) Utilização incorreta ou incompleta de dados;
c) Utilização de dados sem autorização; ou
d) Intervenção por qualquer outro modo não autorizado no processamento, causando, dessa forma, prejuízo patrimonial.[25]

Assim, a interferência no resultado do tratamento de dados – enquanto elemento típico – apresenta-se, por um lado, como consequência da manipulação informática, em qualquer uma das modalidades típicas, e assume-se, por outro, como a causa do prejuízo patrimonial.[26] O mesmo é dizer, quanto a este último aspeto, que a ação de interferir no resultado de tratamento de dados tem de estar causalmente ligada à verificação daquele prejuízo.

Quanto a este, e conforme se deixou já dito, o prejuízo patrimonial é elemento comum à burla informática e à burla prevista no artigo 217.º, do Código Penal. No entanto, apesar da proximidade das condutas típicas, o prejuízo patrimonial surge aqui como consequência adequada da conduta do agente, sem que, para isso, tenha contribuído a atuação da pessoa enganada, nessa medida se afastando da burla clássica.

Por outro lado, impõe-se ainda ressalvar que o prejuízo patrimonial pode produzir-se na esfera do proprietário ou utente dos dados ou programa informático ou de terceira pessoa.[27]

Procurando definir os conceitos contidos no normativo em análise, podemos dizer, acompanhando M. MIGUEZ GARCIA e J.M. CASTELA RIO, que no conceito de *tratamento de dados* se compreendem *"(…) os fenómenos técnicos que visam a obtenção de um resultado através da admissão de dados e da sua inserção num determinado programa"*; já quanto ao conceito de dados, deve o mesmo ser entendido *"(…) de forma alargada, abrangendo todas as informações suscetíveis de serem tratadas."*[28]

Ademais, e como adverte MANUEL LOPES ROCHA, aquela interferência (no resultado do tratamento de dados) pode fazer-se servindo-se o agente diretamente do computador – o que será a regra –, mas não só, podendo dar-se o caso, por exemplo, de este fornecer dados falsos a quem, por sua vez, tem por função introduzi-los no computador.[29]

[25] Neste sentido, que se nos afigura correto, entendendo que a interferência no resultado de tratamento de dados a que alude o preceito legal não é modo vinculado de execução do crime, e na senda da doutrina germânica, SANTOS, Rita Coelho – *Op. cit.,* pág. 241, GARCIA, M. Miguez/ RIO, J.M. Castela – *Op. cit.,* pág. 936, ALBUQUERQUE, Paulo Pinto de – *Op. cit.,* págs. 608 e 609. Em sentido, aparentemente, diverso, BARREIROS, José António – *Op. cit.,* págs. 184 e 185.
[26] Fazendo o paralelo com o crime de burla previsto no artigo 217.º do Código Penal, M. Miguez Garcia e J.M. Castela Rio referem que "(…) a interferência no resultado de tratamento de dados de programa informático desempenha aqui a função correspondente à da deslocação patrimonial determinada por erro; compreendida como "disposição computacional", tem como consequência a adequada diminuição do património do lesado." – *Op. cit.,* pág. 983.
[27] ALBUQUERQUE, Paulo Pinto de – *Op. cit.,* pág. 860.
[28] GARCIA, M. Miguez/ RIO, J.M. Castela – *Op. cit.,* pág. 982.
[29] ROCHA, Manuel António Lopes – *Op. cit.,* pág. 94. Em sentido idêntico, SANTOS, Manuel Simas/LEAL-HENRIQUES, Manuel – *Código Penal Anotado* – Art.ºs 131.º ao 235.º, Vol. II, 4.ª edição, Rei dos Livros, 2016, pág. 1011.

Procuraremos, de seguida, analisar as várias formas de conduta que, de modo alternativo ou conjugado, preenchem o crime de burla informática.

Iniciando a apreciação pela **estruturação incorreta de programa informático**, cumpre, primeiramente, definir o que se entende por *programa informático*.

Ora, nem o artigo 221.º, do Código Penal, nem a Lei n.º 109/2009, de 15 de setembro (Lei do Cibercrime) oferecem uma definição de programa informático. Diversamente, a revogada Lei n.º 109/91, de 7 de agosto (Lei da Criminalidade Informática), definia, no respetivo artigo 2.º, alínea c), programa informático como *um conjunto de instruções capazes, quando inseridas num suporte explorável em máquina, de permitir à máquina, que tem por funções o tratamento de informações, indicar, executar ou produzir determinada função, tarefa ou resultado*. Pode, assim, dizer-se que a expressão legal se refere ao *"(…) conjunto de instruções dadas ao computador para cumprir tarefas específicas."*[30]

Assim, a estruturação do programa informático será incorreta quando haja *"(…) modificação do programa em ordem a que as suas instruções sejam diferentes das inicialmente concebidas pelo proprietário – por exemplo, a introdução de novas instruções ou funções no programa, a eliminação ou alteração do seu processo de funcionamento, a modificação dos sistemas de controlo do próprio programa."*[31]

Através daquela atuação de manipulação do *programa informático*, as novas instruções não coincidem com as inicialmente concebidas pelo respetivo titular ou conduzem a resultados não previstos e *objetivamente contrários* àquela que é a finalidade do próprio programa.[32]

Por outro lado, a estruturação pode ocorrer pela manipulação de programa informático existente ou, diversamente, através da criação de um novo programa que produz resultados falsos.[33]

A **utilização incorreta de dados**, enquanto variante típica do crime em análise, corresponde às situações em que ocorre introdução de dados sem correspondência com a realidade (será, por exemplo, o caso da introdução de dados de pessoas que não existem[34]). Excluída está, portanto, nesta modalidade de conduta, a utilização de dados *desconformes com a realidade, manipulados ou modificados*.[35]

Por sua vez, a **utilização de dados** será **incompleta** quando ocorra *"(…) introdução parcial de dados verdadeiros, de tal modo que eles não representam a realidade (…)"*.[36]

[30] GARCIA, M. Miguez/ RIO, J. M. Castela – *Op. cit.,* pág. 936.
[31] ROCHA, Manuel António Lopes – *Op. cit.,* pág. 95.
[32] Assim, ALBUQUERQUE, Paulo Pinto de – *Op. cit.,* pág. 860, e SANTOS, Rita Coelho – *Op. cit.,* págs. 244 e 245.
[33] Neste sentido, ALBUQUERQUE, Paulo Pinto de – *Op. cit.,* pág. 860.
[34] O exemplo é de Paulo Pinto de Albuquerque – *Op. cit.,* pág. 860.
[35] Neste sentido, BARREIROS, José António – *Op. cit.,* pág. 185.
[36] Assim, ALBUQUERQUE, Paulo Pinto de – *Op. cit.,* pág. 860.

Comum às duas variantes agora analisadas é o conceito de dados, que, uma vez que o artigo 221.º, n.º 1, do Código Penal, não distingue, abrangerá não só os dados pessoais, como os dados informáticos.

Quanto aos primeiros, pode dizer-se, à luz do disposto no artigo 3.º, alínea a), da Lei n.º 67/98, de 26 de outubro (Lei da Proteção de Dados Pessoais), que são dados pessoais *qualquer informação, de qualquer natureza e independentemente do respetivo suporte, incluindo som e imagem, relativa a uma pessoa singular identificada ou identificável ('titular dos dados').*

Por sua vez, o artigo 2º, alínea b), da Lei n.º 109/2009, de 15 de setembro, define dados informáticos como *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*.

Como adverte PAULO PINTO DE ALBUQUERQUE, estes dados podem encontrar-se armazenados num sistema informático ou em suporte digital, como sejam as disquetes, os CD-ROM, cartões magnéticos ou eletrónicos.[37]

Diversamente, a **utilização de dados sem autorização** pressupõe o uso sem autorização por outrem que não o respetivo titular ou beneficiário ou em violação dos limites dos poderes de utilização conferidos. O agente atua, portanto, violando as regras de acesso aos dados ou os limites daqueles poderes, sem que, porém, a integridade dos dados seja afetada, não operando qualquer alteração no seu conteúdo.

A jurisprudência portuguesa tem subsumido ao tipo de ilícito de burla informática, nesta última variante típica, as situações de utilização de cartão de débito e do respetivo código de acesso em caixas automáticas de multibanco por pessoa que, para tal, não se encontra autorizada pelo respetivo titular, com intenção de, assim, obter um enriquecimento ilegítimo.[38]

Salienta ainda RITA COELHO SANTOS que se subsumem igualmente ao crime de burla informática, na variante típica ora referida, e a título de exemplo, os casos de uso ilegítimo dos sistemas de *telebanking*, *homebanking* ou dos terminais de "POS" (*Point of Sale*) por terceiro que, utilizando o código de acesso pessoal alheio, efetua pagamento ou realiza transferência monetária, ultrapassando o crédito do titular do cartão ou o saldo disponível da respetiva conta bancária.[39]

Relativamente à última modalidade de conduta típica – de caráter residual –, a ampla formulação legal adotada permite, pela sua abrangência, abarcar outras formas de manipulação informática não subsumíveis nas variantes anteriores.

[37] *Idem Ibidem*.
[38] Procedendo ao mesmo enquadramento ALBUQUERQUE, Paulo Pinto de – *Op. cit.,* págs. 860-861. Dando conta de uma corrente doutrinal italiana que exclui estas situações do âmbito da burla informática, SANTOS, Rita Coelho – *Op. cit.,* pág. 258.
[39] Neste sentido, SANTOS, Rita Coelho – *Op. cit.,* pág. 256.

Incluem-se na **intervenção por qualquer modo não autorizada no processamento**, entre outras, as situações de interferência no processo mecânico do sistema informático, consistindo tais manipulações do *hardware "(…) em interferências sobre as instruções de processamento de dados ou na alteração do processo mecânico do programa informático."*[40]

Relativamente ao conceito de *sistema informático*, refira-se, acompanhando RITA COELHO SANTOS, que se trata de *"(…) sistema de tratamento automatizado de dados mediante mecanismos informáticos e que, por isso, se caracteriza pela codificação da informação, objeto de tratamento, em forma não percetível ao homem, mas compreensível pelo computador (…)"*.[41]

Por último, e sem possibilidade de nos alongarmos neste ponto, deixamos uma nota final para referir que a generalidade da doutrina portuguesa não admite a omissão enquanto forma de comissão do crime de burla informática. Não obstante, em sentido divergente, há autores que defendem que a natureza de crime de execução vinculada da burla informática não colide com a admissibilidade da sua comissão por omissão nos casos em que sobre o agente recaia o dever de garante de evitar o resultado verificado.[42]

2.2.3. Tipo subjetivo de ilícito

A burla informática constitui um **crime doloso**, não se admitindo a sua punição a título de negligência. A conduta do agente pode revestir qualquer uma das modalidades de dolo previstas no artigo 14.º, do Código Penal (isto é, dolo direto, necessário ou eventual).

Para além do dolo genérico relativo aos elementos do tipo objetivo, exige-se ainda um elemento subjetivo específico consistente na intenção de enriquecimento ilícito para o agente ou para terceiro. Trata-se, portanto, de um **crime intencional**, na medida em que *"(…) o animus lucrandi figura apenas como referente expresso da intervenção do agente, sem interferir (…) no momento da consumação do crime"*.[43]

Na medida em que, não obstante a exigência do *animus lucrandi*, o crime de burla informática se consuma independentemente da verificação do efetivo enriquecimento do sujeito ativo ou de terceiro, impondo-se, apenas, o efetivo dano patrimonial da vítima, trata-se de um crime de **resultado parcial ou cortado**, marcado, portanto, pela descontinuidade entre os tipos subjetivo e objetivo de ilícito.

[40] SANTOS, Rita Coelho – *Op. cit.,* pág. 259.
[41] *Idem Ibidem*.
[42] Adotando esta posição, SANTOS, Rita Coelho – *Op. cit.,* págs. 261 e 262.
[43] SANTOS, Rita Coelho – *Op. cit.,* pág. 209.

2.3. Problemática do concurso de crimes

Após a análise do enquadramento jurídico-legal do crime de burla informática, cumpre agora abordar a problemática da relação que intercede entre este tipo de legal de crime e outros previstos no Código Penal e na Lei do Cibercrime.
Não tendo o ensejo de esgotar todas as hipóteses de concurso de crimes, procuraremos abordar as situações que se colocam com maior frequência na prática judiciária, sendo que esta análise assentará, essencialmente, nos contributos da doutrina nacional e na experiência que a jurisprudência dos tribunais superiores, a propósito, revela.

Uma nota apenas para dizer que constituindo a burla informática um tipo de crime relativamente recente na histórica jurídico-penal portuguesa, a sua construção doutrinal e jurisprudencial constitui ainda um "*work in progress*", o que se reflete na temática agora em análise.

2.3.1. Relação com o crime de burla

Como decorre do que vimos de expor, a burla informática, partilhando embora o *nomen iuris* com o tipo de ilícito previsto no artigo 217.º do Código Penal, assume-se como crime autónomo, prescindindo, no contexto dos específicos contornos típicos legalmente previstos, da verificação dos elementos caracterizadores da burla clássica, isto é, a conduta astuciosa do agente, o erro ou engano provocado no sujeito passivo e o nexo de causalidade entre a atuação deste último e o prejuízo patrimonial.

Ademais, igualmente se espartam os ilícitos pelo facto de, não obstante serem ambos os ilícitos de execução vinculada, no crime de burla (clássica) o agente determinar alguém, por meio de qualquer erro ou engano, à prática de um ato lesivo do património, enquanto o crime de burla informática se consuma mediante o recurso às operações especificamente descritas no respetivo preceito legal.

Atentas as diferenças encontradas entre a burla informática e a burla, e à semelhança do debate firmado em outros ordenamentos jurídicos, também entre nós se coloca a questão de saber se entre estes dois crimes se verifica uma relação de especialidade ou, ao invés, de alternatividade.

Com base nos fundamentos expostos, a doutrina nacional vem considerando que entre a burla informática e a burla clássica intercede uma **relação de exclusividade ou alternatividade**.[44]

[44] Nesse sentido, SANTOS, Rita Coelho – *Op. cit.,* pág. 286 e ALBUQUERQUE, Paulo Pinto de – *Op. cit.,* pág. 610.

2.3.2. Relação com as figuras típicas consagradas na Lei do Cibercrime

A Lei n.º 109/2009, de 15 de setembro (Lei do Cibercrime), prevê nos artigos 4.º a 8.º do Capítulo II (*disposições penais materiais*) um conjunto de tipos legais de crime.

Atenta a complexidade e densidade da matéria em causa, esta abordagem será, necessariamente, mais contida, não se pretendendo, tendo em conta, desde logo, o próprio âmbito do nosso trabalho, uma análise aprofundada dos tipos legais de crime previstos naquele diploma legal, cingindo-se a nossa apreciação às situações que surgem com maior frequência.

É relativamente ao **crime de falsidade informática** – previsto e punido pelo artigo 3.º do referido diploma legal – que a questão do concurso com a burla informática se tem colocado na prática judiciária com mais acuidade.

Neste contexto, existem dois entendimentos: um, no sentido de que em tais casos se estabelece uma relação de concurso efetivo; outro, propugnando a existência de concurso aparente.

Pugnam por aquele primeiro entendimento DUARTE RODRIGUES NUNES[45] e PAULO GONÇALVES TEIXEIRA[46], atenta a diversidade de bens jurídicos tutelados pelas incriminações e a autonomia de sentidos de ilicitude, ainda que o crime de falsidade informática seja crime-meio para o cometimento do crime de burla informática.

Na jurisprudência pode ver-se o **Acórdão do Tribunal da Relação do Porto, de 14 de setembro de 2016**, Relator: Ernesto Nascimento[47], no qual se considerou que os bens jurídicos tutelados pelos crimes de burla informática e de falsidade informática são diferentes, pelo que se terá de afirmar a existência de concurso efetivo, ainda que a falsidade informática seja meramente instrumental, enquanto forma de induzir a vítima em erro.

Na verdade, o bem jurídico protegido pelo crime de falsidade informática é a integridade dos sistemas de informação, procurando-se, através da incriminação, impedir os atos 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.

Diversamente, RITA COELHO SANTOS entende que a *falsidade informática realizada com o escopo de obter um enriquecimento ilegítimo, para o agente ou para terceiro, é consumida pelo crime de burla informática (consumpção pura)*.[48]

Neste particular, importa salientar que no crime de falsidade informática não se exige que o agente atue com a intenção de obter um benefício ilegítimo, para si ou para terceiro. Exige-se,

[45] NUNES, Duarte Alberto Rodrigues – *O crime de falsidade informática*, *in* "Julgar", Outubro de 2017.
[46] TEIXEIRA, Paulo Alexandre Gonçalves – *O fenómeno do phishing – Enquadramento jurídico-penal*, Universidade Autónoma de Lisboa, 2013.
[47] Acórdão acessível em www.dgsi.pt.
[48] SANTOS, Rita Coelho – *Op. cit.,* pág. 288. Em sentido idêntico, ALBUQUERQUE, Paulo Pinto de – *Op. cit.,* pág. 861.

sim, a intenção de provocar engano nas relações jurídicas e, ainda, de que os dados ou documentos não genuínos produzidos sejam considerados ou utilizados para finalidades juridicamente relevantes como se o fossem. Donde, o afastamento – não só ao nível do tipo de ilícito objetivo, mas igualmente ao nível dos elementos subjetivos – do crime de falsidade informática em relação ao tipo legal de burla informática.

O **crime de sabotagem informática** vem previsto no artigo 5.º, da Lei n.º 109/2009, de 15 de setembro (Lei do Cibercrime).

Atenta a concreta previsão típica do crime de sabotagem informática, não são de excluir eventuais relações de concurso com outros crimes ditos informáticos, como seja o de burla informática, sobretudo quando o agente atue finalisticamente orientado para a obtenção, para si ou para terceiro, de enriquecimento ilegítimo, o que, como se retira do artigo 5.º daquele diploma legal, não é elemento subjetivo do crime de sabotagem informática.

Procurando antecipar soluções, e porque ainda não há jurisprudência a propósito, entendemos que, não obstante as diferenças existentes ao nível dos tipos de ilícito objetivo e subjetivo de ambos os crimes, o bem jurídico aqui protegido é o correto funcionamento e a segurança do sistema informático, pelo que, atenta a proximidade entre os bens jurídicos em causa, podem idealizar-se situações de concurso aparente.

No que tange às relações estabelecidas entre o crime de burla informática e o **crime de acesso ilegítimo**, há autores, como RITA COELHO SANTOS[49] e PAULO PINTO DE ALBUQUERQUE[50] que defendem a existência de um concurso aparente, sendo os factos que consubstanciam a prática do crime de acesso ilegítimo ***factos prévios não puníveis***, na medida em que a prática da burla informática pressupõe, em regra, o acesso ilegítimo a um sistema informático.

Diferentemente há quem pugne pela existência de concurso efetivo, sendo relevante notar, a propósito, que em **Acórdão datado de 5 de novembro de 2008** e relatado por Henriques Gaspar, o Supremo Tribunal de Justiça considerou que *pela amplitude da descrição, o tipo do artigo 221.º, n.º 1, do Código Penal parece constituir um plus relativamente ao modelo de proteção contra o acesso ilegítimo previsto no artigo 6.º, da LCC*.[51]

2.3.3. Relação com os crimes de furto e de roubo

A problemática das relações estabelecidas entre o crime de burla informática e o **crime de furto** coloca-se, essencialmente e como a prática judiciária vem evidenciando, nos casos em que o agente se apropria de cartão multibanco contra a vontade do respetivo titular, fazendo-o seu e, tendo conhecimento do respetivo código pessoal, efetua, sem consentimento do ofendido, levantamentos em numerário ou procede a pagamentos, resultando de tais transações um prejuízo para o ofendido.

[49] SANTOS, Rita Coelho – *Op. cit.,* pág. 288.
[50] ALBUQUERQUE, Paulo Pinto de – *Op. cit.,* pág. 861.
[51] Acórdão acessível em www.dgsi.pt.

Ora, a jurisprudência tem, maioritariamente, entendido que em tais casos se estabelece uma relação de concurso efetivo. Neste sentido, e a título de exemplo, podem ver-se o **Acórdão do Tribunal da Relação de Évora, de 20 de janeiro de 2015**, Relator: João Amaro, o **Acórdão do Tribunal da Relação de Coimbra, de 10 de janeiro de 2001**, Relator: Santos Cabral, e o **Acórdão do Tribunal da Relação de Coimbra, de 29 de fevereiro de 2012**, Relator: Paulo Valério.

Idêntica questão se coloca quando o agente *obriga* a vítima a entregar-lhe o cartão multibanco e a revelar-lhe o respetivo código de acesso, procedendo, de seguida, ao levantamento de dinheiro em caixas automáticas com intenção de obter um enriquecimento.

Estamos já no âmbito da relação que intercede entre os crimes de burla informática e de **roubo**. Neste contexto, podemos descortinar dois entendimentos: por um lado, há quem defenda a existência, em tais casos, de um concurso efetivo, apelando, desde logo, aos bens jurídicos protegidos[52]; por outro lado, há quem defenda que, no plano da tipicidade e da configuração da ação em concreto, tais condutas se subsumem apenas ao crime de roubo.[53]

3. Burla nas comunicações

3.1. Enquadramento jurídico-legal

Procuraremos, de seguida e à semelhança do caminho percorrido no Capítulo anterior, proceder à análise dogmática do tipo legal de crime de burla nas comunicações.

Uma vez que o enquadramento a que procedemos a propósito do crime de burla informática se aplica, no essencial, a este tipo de ilícito, a análise que ora se enceta será, necessariamente e sem perdermos de vista as considerações já tecidas e que aqui se repristinam, menos extensa.

3.1.1. Generalidades, bem jurídico protegido e natureza do crime

O crime de burla nas comunicações encontra-se tipificado no artigo 221.º, n.º 2, do Código Penal, nos termos do qual *"[A] mesma pena é aplicável a quem, com intenção de obter para si ou para terceiro um benefício ilegítimo, causar a outrem prejuízo patrimonial, usando programas, dispositivos eletrónicos ou outros meios que, separadamente ou em conjunto, se destinem a diminuir, alterar ou impedir, total ou parcialmente, o normal funcionamento ou exploração de serviços de telecomunicações."*

[52] Assim, ALBUQUERQUE, Paulo Pinto de – *Op. cit.,* pág. 610; na jurisprudência, entre outros, o Acórdão do Tribunal da Relação de Coimbra de 29/02/2012, Relator: Paulo Valério e o Acórdão do Supremo Tribunal de Justiça de 6/10/2005, Relator: Simas Santos, ambos acessíveis em www.dgsi.pt.

[53] Neste sentido, os Acórdãos do Supremo Tribunal de Justiça de 5 de novembro de 2008 e de 20 de setembro de 2006, Relator: Henriques Gaspar, acessíveis em www.dgsi.pt, tendo-se considerado que, atendendo aos elementos vinculados de tipicidade e valorações inerentes ao bem jurídico, a burla informática perde qualquer autonomia.

O referido tipo legal de crime foi introduzido no Código Penal na Reforma de 1998 operada pela Lei n.º 65/98, de 2 de setembro, e trata-se, à semelhança do tipo que colhe previsão no artigo 221.º, n.º 1, daquele diploma legal, de um crime que tutela o **bem jurídico** do património.

Trata-se igualmente de um **crime de dano** e **material ou de resultado**, nos termos já referidos no Capítulo que antecede a propósito da burla informática.

O crime de burla nas comunicações assume-se ainda como um **crime de execução vinculada**, tendo, no entanto, o legislador adotado uma formulação típica de alguma amplitude, procedendo ao enunciado exemplificativo de concretas modalidades de ação, o que leva A. M. ALMEIDA COSTA a considerar que *"(…) o alcance da mencionada qualificação resume-se, por isso, à ideia de que a presente infração se esgota numa ofensa ao bem jurídico do património produzida através de uma interferência nos aludidos serviços de telecomunicações."*[54]

3.1.2. Tipo de ilícito objetivo e tipo de ilícito subjetivo

São elementos objetivos do crime de burla nas comunicações a utilização de programas, dispositivos eletrónicos ou outros meios de tratamento automatizado de informação que se destinem a diminuir, alterar ou impedir, total ou parcialmente, o normal funcionamento ou exploração de serviços de telecomunicações.

Assim, a burla de comunicações assenta na perturbação de um serviço de comunicações, conquanto o normal funcionamento ou exploração de tal serviço resulte diminuído, alterado ou impedido.

Ao nível do tipo de ilícito subjetivo, o crime de burla nas comunicações consubstancia um **crime doloso**, podendo a conduta do agente revestir qualquer uma das modalidades de dolo previstas no artigo 14.º, do Código Penal. Exige-se, ainda, e à semelhança da burla informática, um elemento subjetivo específico, qual seja a intenção do agente de obter, para si ou para terceiro, um benefício ilegítimo.

Na medida em que, não obstante a exigência do *animus beneficiendi*, o crime se consuma independentemente da verificação daquele benefício do sujeito ativo ou de terceiro, impondo-se, apenas, o efetivo dano patrimonial da vítima, trata-se de um **crime de resultado parcial ou cortado**.

3.2. Aspetos comuns à burla informática e à burla nas comunicações

O crime de burla informática simples é punido com pena de prisão até três anos ou com pena de multa, nos termos do disposto no artigo 221.º, n.º 1, do Código Penal. Igual **moldura penal**

[54] DIAS, Jorge de Figueiredo [dir.] – *Op. cit.,* pág. 333.

é, de resto, aplicável ao crime de burla nas comunicações, como decorre do preceituado no n.º 2 do mesmo artigo.

Ainda ao nível da moldura penal abstrata, são elementos qualificadores dos crimes em análise o *valor elevado* e o *valor consideravelmente elevado* do prejuízo causado, sendo, no primeiro caso, a pena de prisão elevada até cinco anos e a pena de multa até 600 dias e, no segundo caso, apenas aplicável uma pena de prisão de dois a oito anos, nos termos do disposto no artigo 221.º, n.º 5, alíneas a) e b), respetivamente, por referência ao preceituado no artigo 202.º, alíneas a) e b), ambos do Código Penal.

Nos termos do disposto no artigo 221.º, n.º 3, do Código Penal – aplicável ao crime de burla informática e ao crime de burla nas comunicações –, a **tentativa** é, nestes tipos de ilícito, sempre punível; punição que, de resto, terá de ser compreendida à luz do disposto nos artigos 22.º e 23.º, do mesmo diploma legal.

Por outro lado, e atento o preceituado no n.º 4 do referido artigo, o procedimento criminal pelos crimes de burla informática e de burla nas comunicações – quando assumem a sua forma simplificada – depende de queixa, tratando-se, portanto, de crimes de **natureza semipública**.

Para efeitos do disposto no artigo 113.º, n.º 1, do Código Penal, defende PAULO PINTO DE ALBUQUERQUE que tem legitimidade para exercer o direito de queixa a pessoa prejudicada e não o proprietário ou o utente dos dados ou programas informáticos.[55]

Diversamente, nas situações de agravação em função do valor – a que se reporta, como se referiu, o artigo 221.º, n.º 5, do Código Penal – os crimes de burla informática e de burla nas comunicações assumem **natureza pública**, não estando, portanto, o respetivo procedimento criminal dependente do exercício do direito de queixa por quem, para tal, se encontre legitimado nos termos legalmente previstos.[56]

Por outro lado, ao abrigo do preceituado no artigo 221.º, n.º 6, do Código Penal, é correspondentemente aplicável o disposto no artigo 206.º, do mesmo diploma legal. Tal remissão significa que haverá extinção da responsabilidade criminal se houver concordância do ofendido e do arguido, sem dano ilegítimo de terceiro, até à publicação da sentença da 1.ª instância, conquanto tenha havido reparação integral dos prejuízos causados (n.º 1) e, por outro, que em caso de reparação integral do prejuízo causado, sem dano ilegítimo de terceiro, até ao início da audiência de julgamento em 1.ª instância, a pena é especialmente atenuada (n.º 2). Diversamente, a pena pode ser especialmente atenuada se a reparação do prejuízo causado for apenas parcial (n.º 3).

[55] Assim, ALBUQUERQUE, Paulo Pinto de – *Op. cit.,* pág. 862.
[56] Neste sentido, ALBUQUERQUE, Paulo Pinto de – *Op. cit.,* pág. 862, GARCIA, M. Miguez/ RIO, J.M. Castela – *Op. cit.,* pág. 939 e DIAS, Jorge de Figueiredo [dir.] – *Op. cit.,* pág. 332; na jurisprudência, assumindo igual posição, *vide* o Acórdão do Tribunal da Relação de Lisboa de 05/02/2014, Relatora: Maria Margarida Almeida, acessível em www.dgsi.pt.

Refira-se, por último, que o artigo 11.º, n.º 2, do Código Penal, admite a **responsabilidade das pessoas coletivas** e equiparadas pelos crimes em análise quando concretamente verificadas as condições aí previstas.

4. Prática e gestão processual

The invisible man does not fear the State
Lessing

4.1. Generalidades

Como se dá conta no Relatório de Segurança Interna (RSI) de 2016,[57] o crime de burla informática e nas comunicações está entre a criminalidade mais participada, registando uma subida de 7,9% em face do ano anterior (2015).

Como igualmente aí se refere *"[N]o que concerne à área da criminalidade Informática e praticada com recurso a tecnologia informática verifica-se um aumento generalizado (…). O tipo de burla informática e nas comunicações regista igualmente tendência crescente, de cerca de 19%."*

Em face do aumento verificado, a Lei n.º 96/2017, de 23 de agosto, que define os objetivos, prioridades e orientações de política criminal para o biénio de 2017/2019, considera a cibercriminalidade como **fenómeno criminal de prevenção e investigação prioritárias**, como decorre do disposto no respetivo artigo 2.º, alínea c), e 3.º, alínea g).

4.2. Abertura de inquérito e diligências de investigação

Recebida a notícia do crime, o Ministério Público determina a abertura de inquérito, nos termos do disposto no artigo 262.º, n.º 2, do Código de Processo Penal.

Incumbe depois, e em cumprimento do preceituado no n.º 1, do mesmo artigo 262.º, realizar as diligências tidas como necessárias e pertinentes para o apuramento da existência dos crimes denunciados, para determinação do(s) seu(s) agente(s) e da responsabilidade dele(s).
Como decorre do disposto no artigo 7.º, n.º 3, alínea l), da Lei n.º 49/2008, de 27 de agosto (Lei de Organização da Investigação Criminal) e no Ponto II, n.º 1, da Circular da Procuradoria-Geral da República n.º 6/2002, de 11 de março, a investigação dos crimes informáticos e praticados com recurso a tecnologia informática é da **competência reservada da Polícia Judiciária**.

No delinear da estratégia de investigação, e atenta a concreta criminalidade em causa, são várias as dificuldades com que se depararam as autoridades judiciárias e órgãos de polícia criminal. Na verdade, os crimes cometidos com recurso a meios tecnologicamente avançados

[57] O RSI constitui o documento congregador dos registos globais da criminalidade participada em Portugal, a partir dos dados fornecidos pelas entidades que compõem o Sistema de Segurança Interna, estando o de 2016 disponível em:https://www.parlamento.pt/ActividadeParlamentar/Paginas/DetalheActividadeParlamentar.aspx?BID=104739&ACT_TP=RSI.

acarretam dificuldades de prova acrescidas, sendo, pela elevada tecnicidade, especialidade e, tantas vezes, transnacionalidade que os caracterizam, de difícil deteção e comprovação.

A determinação do respetivo agente apresenta-se, de resto, como uma das principais dificuldades, atentos os obstáculos inerentes à realização de um controlo eficaz da origem das operações informáticas efetuadas.

Como salienta RITA COELHO SANTOS, acerca da criminalidade informática em geral, mas igualmente com relevo para a nossa análise, *"[O]s crimes informáticos traduzem-se, em princípio, em crimes inteligentes e não aparentes ou invisíveis, quer pelo grau de sofisticação que o agente, particularmente habilitado com conhecimentos no domínio da informática, emprega no seu cometimento, quer por se tratar de um campo de investigação que requer especiais conhecimentos técnicos para apurar as utilizações feitas da rede e para as imputar, com segurança, ao respetivo autor."*[58]

O que se referiu torna evidente a necessidade de o Magistrado do Ministério Público titular do inquérito definir, o quanto antes, as pertinentes diligências de investigação, designadamente no primeiro despacho, atenta, desde logo, a (tantas vezes) reclamada urgência na recolha dos elementos de prova.

4.3. Os meios de obtenção de prova na Lei do Cibercrime

No âmbito da investigação de condutas subsumíveis à prática de crime de burla informática e nas comunicações assume particular relevo a obtenção de prova digital.

Neste contexto torna-se imperioso atender ao disposto na Lei n.º 109/2009, de 15 de setembro (Lei do Cibercrime), que, com caráter inovador e em cumprimento de compromissos internacionais assumidos pelo Estado Português, prevê um conjunto de normativos processuais penais – artigos 11.º a 19.º –, regulamentando a obtenção de prova em suporte eletrónico.

Assim, cumpre, primeiramente, referir que o artigo 11.º do mencionado diploma legal, definindo o *âmbito de aplicação das disposições processuais*, preceitua, no n.º 1, que, com exceção do disposto nos artigos 18.º e 19.º, as disposições processuais previstas Capítulo III se aplicam a processos relativos a crimes previstos naquela lei – alínea a); a crimes cometidos por meio de um sistema informático – alínea b); ou em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico – alínea c).

Como resulta do exposto, por via do disposto no artigo 11.º, alíneas b) e/ou c), do diploma legal mencionado – e sem prejuízo do que infra se referirá a propósito dos artigos 18.º e 19.º –, são aplicáveis à investigação do crime de burla informática e nas comunicações a preservação expedita de dados (artigo 12.º), a revelação expedita de dados (artigo 13.º), a injunção para apresentação ou acesso a dados (artigo 14.º), a pesquisa informática (artigo 15.º), a apreensão

[58] SANTOS, Rita Coelho – *Op. cit.,* pág. 54.

de dados informáticos (artigo 16.º) e a apreensão de correio eletrónico e registos de comunicações de natureza semelhante (artigo 17.º).

Sem possibilidade de procedermos a uma análise exaustiva, procuraremos, de seguida, abordar os referidos meios de obtenção de prova na perspetiva da competência do Ministério Público em contexto de inquérito relativo aos tipos de crime em estudo.

Preservação expedita de dados

Assim, nos termos do disposto no artigo 12.º, n.º 1, da Lei n.º 109/2009, de 15 de setembro, *se no decurso do processo for necessário à produção de prova, tendo em vista a descoberta da verdade, obter dados informáticos específicos armazenados num sistema informático, incluindo dados de tráfego, em relação aos quais haja receio de que possam perder-se, alterar-se ou deixar de estar disponíveis, o Ministério Público, enquanto autoridade judiciária competente, ordena a quem tenha disponibilidade ou controlo desses dados, designadamente a fornecedor de serviço*[59]*, que preserve os dados em causa*.

A preservação expedita de dados assume, assim, a natureza de medida cautelar, permitindo a conservação dos referidos dados.

Injunção para apresentação ou concessão do acesso a dados

Como decorre do preceituado no artigo 14.º, n.º 1, da Lei n.º 109/2009, de 15 de setembro, e ressalvadas as situações previstas nos n.ºs 5 e 6, do mesmo normativo, *se no decurso do processo se tornar necessário à produção de prova, tendo em vista a descoberta da verdade, obter dados informáticos específicos e determinados, armazenados num determinado sistema informático, o Ministério Público, enquanto autoridade judiciária competente, ordena a quem tenha disponibilidade ou controlo desses dados que os comunique ao processo ou que permita o acesso aos mesmos, sob pena de punição por desobediência*.

A este propósito impõe-se, no entanto, fazer uma ressalva. No contexto da investigação de crimes informáticos e de crimes cometidos por meios informáticos – como é o caso da burla informática e nas comunicações – a identificação do endereço IP (*Internet Protocol*) de onde partiu a comunicação em causa afigura-se, por vezes, de crucial importância, com vista à descoberta da localização geográfica a partir da qual teve origem a conduta criminosa.[60]

[59] Quanto à definição de fornecedor de serviço, *vide* o artigo 2.º, alínea d), da Lei do Cibercrime.
[60] Como consta da nota prática nº 2/2013 do Gabinete de Cibercrime da Procuradoria-Geral da República, e na sequência da nota prática n.º 1/2012, o pedido de identificação do utilizador de um determinado endereço IP, num dado dia e hora, não deve ser submetido ao regime dos dados de tráfego, por se entender que este pedido não se refere a informação sobre o percurso dessa comunicação nem sobre outro eventual tráfego comunicacional da pessoa em causa; concluindo-se que pertence ao Ministério Público a competência para pedir, a um operador de comunicações, a identificação do seu cliente que utilizou um determinado endereço IP num determinado dia e hora. Vide, no mesmo sentido a jurisprudência indicada naquela nota prática e que é acessível em https://simp.pgr.pt/simp_tematicos/documentos/mount/files/1365007943_2013_04_03_nota_pratica___jurisprudencia_sobre_ip.pdf.

Constatando aquela necessidade, a Procuradoria-Geral da República celebrou em 9 de julho de 2012 um **protocolo de cooperação** com operadores de comunicações, no âmbito da investigação da cibercriminalidade e da obtenção de prova digital.

Assim, a Circular n.º 12/2012, de 25 de setembro de 2012, da Procuradoria-Geral da República, uniformizando os procedimentos de informação dirigidos aos operadores de comunicações, estabelece que as solicitações às operadoras nacionais sejam efetuadas com recurso a formulários pré-elaborados, devendo os mesmos ser remetidos pelas vias e para os endereços aí indicados.

Quando a informação pretendida tenha de ser solicitada a fornecedores de serviços internacionais, tais como a *Microsoft*, a *Google* (abrangendo o *Blogger* e o *YouTube*) e a *Facebook* (abrangendo o *Instagram*), o Ministério Público pode, no contexto de uma cooperação informal e sem prejuízo dos canais tradicionais para a cooperação judiciária, solicitar informação referente à identificação do titular da conta (nome, morada e endereço de IP a partir do qual a conta foi aberta), que existem enquanto a conta estiver ativa, sendo certo que no caso de pedido de informação sobre concretos acessos à conta a identificação do endereço de IP a partir do qual foi feito o acesso apenas é guardada pelo prazo de noventa dias.[61]

Pesquisa de dados informáticos

À pesquisa de dados informáticos reporta-se o artigo 15.º, da Lei n.º 109/2009, de 15 de setembro, estabelecendo o respetivo n.º 1 que *quando no decurso do processo se tornar necessário à produção de prova, tendo em vista a descoberta da verdade, obter dados informáticos específicos e determinados, armazenados num determinado sistema informático, a autoridade judiciária competente autoriza ou ordena por despacho que se proceda a uma pesquisa nesse sistema informático, devendo, sempre que possível, presidir à diligência*.

A referida norma deve, de resto, ser compreendida em conjugação com o disposto no artigo 16.º, do mesmo diploma legal, que permite a ***apreensão de dados informáticos***, havendo pertinência na determinação simultânea da pesquisa e apreensão de dados informáticos.

Na verdade, à luz do disposto no artigo 16.º, n.º 1, da Lei n.º 109/2009, de 15 de setembro, *quando, no decurso de uma pesquisa informática ou de outro acesso legítimo a um sistema informático, forem encontrados dados ou documentos informáticos necessários à produção de prova, tendo em vista a descoberta da verdade, a autoridade judiciária competente autorize ou ordene por despacho a apreensão dos mesmos*.

[61] De acordo com a nota prática n.º 3/2014 do Gabinete de Cibercrime da Procuradoria-Geral da República, acessível em https://simp.pgr.pt/destaques/mount/anexos/3227_nota_pratica_isp_eua.pdf.

Interceção de comunicações

Atenta a remissão operada pelo artigo 18.º, n.º 1, alínea b), da Lei n.º 109/2009, de 15 de setembro, para os crimes previstos no artigo 187.º do Código de Processo Penal, é admissível, à luz do disposto no n.º 1, alínea a), deste último normativo, o recurso ao mecanismo da interceção de comunicações no contexto da investigação da prática de crime de burla informática e nas comunicações na sua forma agravada, uma vez que, em tal caso, o referido crime é punível com pena de prisão superior, no seu máximo, a três anos.

Ações encobertas

Por último, o artigo 19.º, n.º 1, alínea b), da Lei n.º 109/2009, de 15 de setembro, prevê o recurso às ações encobertas, regulamentadas na Lei n.º 101/2001, de 25 de agosto, no decurso de inquérito relativo a crime de burla informática e nas comunicações.

4.4. Meios de prova e de obtenção de prova no Código de Processo Penal

Paralelamente aos mecanismos processuais previstos na Lei n.º 109/2009, de 15 de setembro, mantêm aplicação os meios de obtenção de prova previstos no Código de Processo Penal, salientando-se, pela especial pertinência, a realização de **buscas e apreensões**, designadamente a apreensão de material informático, sujeitas, de resto, ao disposto nos artigos 174.º, 176.º, 177.º e 178.º e seguintes daquele diploma legal, ressalvando-se, de resto, a necessária coordenação entre estes mecanismos e aqueloutros.

Por outro lado, uma vez que a análise da prova digital ou em suporte digital requer frequentemente competências específicas e a nomeação de peritos com conhecimentos na área da informática e das tecnologias de informação e da comunicação, a realização de **perícia informática** revela-se essencial, estando tal meio de prova sujeito à disciplina prevista nos artigos 151.º e seguintes, do Código de Processo Penal.

4.5. Encerramento do inquérito

Por fim, e sem possibilidade de nos alongarmos, atenta a limitação do nosso trabalho, cumpre referir que, uma vez realizadas as diligências tidas como necessárias e pertinentes para o apuramento da existência dos crimes denunciados, para determinação do(s) seu(s) agente(s) e da responsabilidade dele(s), cumpre ao Ministério Público decidir, à luz do que dispõem, conjugadamente, os artigos 277.º, 280.º, 281.º e 283.º, do Código de Processo Penal, do desfecho do inquérito.

Assim, norteado pelo princípio da legalidade, consagrado no artigo 219.º, n.º 1, da Constituição da República Portuguesa, e por critérios de objetividade, deverá o Ministério Público proceder ao **arquivamento** do inquérito quando tiver sido recolhida prova bastante de não se ter verificado crime, de o arguido não o ter praticado a qualquer título ou, ainda, de ser

legalmente inadmissível o procedimento, conforme preceitua o artigo 277.º, n.º 1, do Código de Processo Penal.

Não se verificando as circunstâncias previstas na mencionada norma, deverá o Ministério Público, igualmente orientado pelos mesmos princípio e critério acima referidos, proceder ao arquivamento do inquérito, quando não tenha sido possível obter indícios suficientes da verificação do crime ou de quem foram os seus agentes, nos termos do disposto no n.º 2, do mesmo artigo 277.º.

Ao invés, e como momento fundamental do exercício da ação penal, deverá o Ministério Público deduzir **acusação** quando sejam recolhidos indícios suficientes de se ter verificado crime e de quem foi o seu agente, nos termos do disposto no artigo 283.º, n.º 1, do Código de Processo Penal, contendo o n.º 2, do mesmo preceito, o critério orientador do que devam considerar-se indícios suficientes.

Afigura-se ainda possível, quando esteja em causa o crime de burla informática e nas comunicações na forma *simplificada* (cfr. artigo 221.º, n.ºs 1 e 2, do Código de Processo Penal), a aplicação do **instituto da suspensão provisória do processo**, conquanto se verifiquem os pressupostos previstos no artigo 281.º do Código de Processo Penal, e o recurso ao **processo especial sumaríssimo**, previsto e regulamentado nos artigos 392.º a 398.º do mesmo diploma legal.

IV. Hiperligações e referências bibliográficas

Hiperligações

https://www.parlamento.pt/ActividadeParlamentar/Paginas/DetalheActividadeParlamentar.aspx?BID=104739&ACT_TP=RSIHiperligação2

https://simp.pgr.pt/simp_tematicos/documentos/mount/files/1365007943_2013_04_03_nota_pratica___jurispridencia_sobre_ip.pdfCentrodeEstudosJudiciários

https://simp.pgr.pt/destaques/mount/anexos/3227_nota_pratica_isp_eua.pdf

Referências bibliográficas

ALBUQUERQUE, Paulo Pinto de – *Comentário do Código de Processo Penal à luz da Constituição da República Portuguesa e da Convenção Europeia dos Direitos do Homem*, 3.ª Ed., Lisboa: Universidade Católica Editora, 2009.

BARREIROS, José António – *Crimes contra o património*, Lisboa: Universidade Lusíada, 1996.

DANTAS, Leones – *A Revisão do Código Penal e os Crimes Patrimoniais*, *in* "Jornadas de Direito Criminal do CEJ", Lisboa, 1998.

DIAS, Jorge de Figueiredo [dir.] – *Comentário Conimbricense do Código Penal*, Tomo II, Coimbra Editora, 1999.

DIAS, Vera Marques – *A Problemática da Investigação do Cibercrime*, *in* "DataVenia" [Em linha], Ano 1, n.º 1, Julho 2012 [Consult. 20 Fev. 2018], disponível em https://www.datavenia.pt/ficheiros/edicao01/datavenia01_p063-088.pdf.

FERNANDES, Paulo Silva – *Globalização, "Sociedade de Risco" e o Futuro do Direito Penal – Panorâmica de Alguns Problemas Comuns*, Coimbra: Almedina, 2001.

GARCIA, M. Miguez/ RIO, J.M. Castela – *Código Penal Parte geral e especial com notas e comentários*, Coimbra: Almedina, 2014.

MARQUES, Garcia/ MARTINS, Lourenço – *Direito da Informática*, 2.ª Edição Refundida e Atualizada, Coimbra: Almedina, 2006.

MINISTÉRIO DA JUSTIÇA – *Código Penal – Actas e Projecto da Comissão de Revisão*, Lisboa: Rei dos Livros, 1993.

NUNES, Duarte Alberto Rodrigues – *O crime de falsidade informática*, *in* "Julgar", Outubro de 2017.

RODRIGUES, Benjamim Silva – *Da Prova Penal – Da Prova – Electrónico- Digital e da Criminalidade Informático-Digital*, Tomo IV, 1.ª Edição, Rei dos Livros, 2011.

ROCHA, Manuel António Lopes – *A Revisão do Código Penal – Soluções de Neocriminalização*, *in* "Jornadas de Direito Criminal – Revisão do Código Penal", Centro de Estudos Judiciários, Lisboa, 1996.

SANTOS, Manuel Simas/LEAL-HENRIQUES, Manuel – *Código Penal Anotado – Art.º 131.º ao 235.º*, Vol. II, 4.ª edição, Rei dos Livros, 2016.

SANTOS, Rita Coelho – *O Tratamento Jurídico-Penal da Transferência de Fundos Monetários Através da Manipulação Ilícita dos Sistemas Informáticos*, Coimbra: Coimbra Editora, 2005.

TEIXEIRA, Paulo Alexandre Gonçalves – *O fenómeno do phishing – Enquadramento jurídico-penal*, Universidade Autónoma de Lisboa, 2013.

2.

Crime de burla informática e nas comunicações. Enquadramento jurídico, prática e gestão processual

Catarina Rodrigues

CENTRO
DE ESTUDOS
JUDICIÁRIOS

2. CRIME DE BURLA INFORMÁTICA E NAS COMUNICAÇÕES. ENQUADRAMENTO JURÍDICO, PRÁTICA E GESTÃO PROCESSUAL

Catarina Rodrigues

I. Introdução

O crime de burla informática e nas comunicações é na actualidade um fenómeno cada vez mais frequente.

Não obstante as vantagens proporcionadas pela sociedade de tecnologias de informação e comunicação em que nos situamos, um dos inconvenientes desta realidade é justamente a vulnerabilidade e facilidade de acesso dos sistemas e das redes informáticas que a suportam com inevitáveis reflexos no âmbito criminógeno, materializando-se no "aumento generalizado" da criminalidade informática.

Segundo dados do Relatório Anual de Segurança Interna, os crimes informáticos e com recurso a tecnologia informática registaram um aumento generalizado em 2016 face ao ano anterior. Em particular, os crimes de burla informática e nas telecomunicações apresentam um aumento de 7,9% no total da criminalidade participada.

O *computador*, aqui entendido em sentido amplo, torna-se num dos instrumentos preferidos dos agentes criminosos e descobrem-se novas técnicas de resolução criminosa que dificultam

a identificação do autor do crime. O *criminoso tipo* é hoje especialmente dotado de capacidade intelectual para adquirir conhecimentos no seio da informática e assim praticar actos ilícitos de investigação tendencialmente mais complexa.
Confrontado com o problema da "delinquência informática" e com as suas múltiplas ramificações, o legislador desde cedo percebeu que a burla informática era um tipo suficientemente carecido de tutela e, consequentemente, de autonomização típica no Código Penal. E é nesse contexto que em 1995 este tipo legal é acolhido no panorama jurídico-penal português.

Anos volvidos, com a reforma de 1998, conduzida pela Lei n.º 65/98, de 2 de Setembro, o artigo 221.º foi epigrafado de **"Burla informática e nas comunicações"** adicionando-se um n.º 2 para consagrar estoutra variante de burla.

Hoje, é este o quadro legal em vigor e é sobre o seu enquadramento jurídico que nos deteremos nas linhas seguintes.

De igual forma, mas numa outra vertente, os referidos recentes desenvolvimentos em matéria de tecnologias vieram outrossim colocar problemas específicos no domínio processual penal, obrigando, por um lado, a repensar a aplicabilidade do Direito *às novas práticas e capacidades da informática* e, por outro, apelando à superação das dificuldades na investigação do crime de burla informática e nas comunicações face *ao forte crescimento* verificado e estimado para este tipo de criminalidade.

São, assim, razões de ordem teórica e motivos de índole prática que tornam importante a realização da presente exposição/investigação.

II. Objectivos

Do que se trata neste trabalho, muito principalmente, é de procurar o sentido do artigo 221.º a partir de uma perspectiva teórico-prático.

Nesta medida, lançamo-nos nesta tarefa com o propósito específico de realizar uma análise global do enquadramento jurídico dos crimes de burla informática e nas comunicações, levando a cabo uma incursão crítico-reflexiva pelo direito penal substantivo em que os mesmos se encontram conformados.

No essencial, visamos trazer a debate alguns dos principais problemas e teses em confronto, tentado definir o actual panorama legislativo, doutrinário e jurisprudencial dos tipos legais sob apreciação, recorrendo, quando tal nos for possível, a exemplos colhidos da jurisprudência dos nossos tribunais.

Paralelamente, o estudo que apresentamos procurará indagar de que forma é que o direito processual penal português e outros diplomas legais encaram esta nova realidade típica, numa apreciação objectiva dos mecanismos destinados à investigação prática dos crimes em apreço.

Numa perspectiva prática e sempre na óptica do Ministério Público, faremos, sempre que oportuno e conveniente, pequenos apontamentos à luz da prática judiciária.

III. Resumo

O presente estudo está divido em duas partes.

Num primeiro momento da nossa exposição, faremos o **"Enquadramento jurídico"** dos tipos legais em apreço. Iniciaremos com uma análise da sua *origem*, reflectindo depois sobre o *bem jurídico* tutelado pela norma incriminadora e, bem assim, sobre a *natureza das infracções*. Cumprido este desígnio, lançar-nos-emos na tarefa de descortinar os *elementos do tipo legal*, começando por uma análise dos elementos do tipo objectivo, para depois nos determos sobre os elementos do tipo subjectivo. Após, e ainda que a título marginal a que a gestão de tempo e de espaço nos obriga, faremos uma apreciação de vários aspectos relevantes que a análise de um tipo legal não pode descurar, de entre os quais, *"Autoria. Cumplicidade. Ilicitude na Comparticipação."*, *"Punibilidade da tentativa"*, *"Cometimento por Omissão"*, *"Agravação."*, *"Aplicação do artigo 206.º do Código Penal"*, *"Pressupostos de procedibilidade"* e *"Responsabilidade da Pessoas Colectivas"*.

Neste nosso enlevo, terminaremos com uma apreciação da *relação que intercede entre o crime de burla informática e outros tipos legais*, consagrados no Código Penal e em legislação avulsa.

Por razões de sistematização, de gestão e, sobretudo, de melhor compreensão, das similitudes e das diferenças entre os dois tipos legais previstos no artigo 221.º faremos a exposição tendo por referência o crime de burla informática, para depois estendermos as considerações tecidas à burla nas comunicações, identificando em capítulo próprio as suas particularidades.

Num segundo momento, centrado na **"Prática e Gestão Processual"** no âmbito dos inquéritos que tenham por objecto os tipos legais em comento, faremos uma breve *contextualização*, onde caracterizaremos o *criminoso tipo*.

De seguida, ingressaremos no foco principal da investigação criminal, procurando identificar as particularidades inerentes à *direcção do inquérito* quando esteja em causa um crime de burla informática ou um crime de burla nas comunicações.

Neste âmbito, concederemos particular ênfase às soluções práticas de investigação encontradas no Código de Processo Penal e, mormente, na Lei do Cibercrime[1], focando-nos na *insuficiência dos meios comuns de investigação e prova do processo penal* para trazer ao espaço discursivo a aplicação do regime processual previsto para a criminalidade informática naquela lei.

A terminar, deixaremos como última nota uma referência às possibilidades de *desfecho do inquérito*.

[1] Lei n.º 109/2009, de 15 de Setembro.

Desonerando-nos de considerações de índole geral, transversais à direcção de qualquer inquérito, a análise que se fará sobre a linha investigatória encontrar-se-á balizada pelas singularidades reclamadas pelos tipos legais em apreço.

1. Enquadramento jurídico

1.1. Burla informática

O crime de burla informática encontra-se previsto no artigo 221.º, n.º 1, nos termos do qual: "Quem, com intenção de obter para si ou para terceiro enriquecimento ilegítimo, causar a outra pessoa prejuízo patrimonial, interferindo no resultado de tratamento de dados ou mediante estruturação incorrecta de programa informático, utilização incorrecta ou incompleta de dados, utilização de dados sem autorização ou intervenção por qualquer outro modo não autorizada no processamento, é punido com pena de prisão até três anos ou com pena de multa."

1.1.1. A origem

A essência do crime de burla informática reside no "erro directo com finalidade determinada, [n]um engano ou [n]um artifício sobre dados ou aplicações informáticas – interferência no resultado ou estruturação incorrecta de programa, utilização incorrecta ou incompleta de dados, utilização de dados sem autorização ou qualquer intervenção não autorizada de processamento."[2]

Na expressão cunhada pela lei por ocasião da Reforma de 1995, o *nomem* "burla informática" foi permeável ao acolhimento do tipo do **§ 263-a do Código Penal alemão** (*Strafgesetzbuch*) designado por *computerbetrug*. Surgido em 1986 na legislação germânica, este novo tipo legal correspondia directamente à "burla de computadores"[3]. Com efeito, prescindindo embora do erro ou engano em relação a uma pessoa, o crime de burla informática exigia, ao nível dos elementos do tipo objectivo, "actos com conteúdo final e material idêntico: manipulação dos sistemas informáticos, ou utilização sem autorização ou abusiva determinando a produção dolosa de prejuízo patrimonial."[4]

Passando em revista os fundamentos que estiveram na origem do tipo do § 263-a do *Strafgesetzbuch*, é usual dizer-se que se encontrou no preceito citado a resposta para fazer face à utilização abusiva de máquinas de pagamento automático (ATM) e às "dificuldades dos tipos penais tradicionais de conteúdo patrimonial, designadamente a burla, para proteger adequadamente o bem jurídico face a novas modalidades de ataque"[5].

[2] Seguimos a orientação do Acórdão do Supremo Tribunal de Justiça, de 05.11.2008, processo n.º 08P2817 (relator Henriques Gaspar).
[3] A mesma incriminação foi acolhida no direito austríaco.
[4] Citamos novamente o aresto *supra*.
[5] *Idem.*

Para de maneira equivalente atingirmos o **espírito do artigo 221.º, n.º 1**, servimo-nos do contributo de Lopes Rocha[6] que, em termos esquemáticos, identifica as quatro razões que presidiram à criação do tipo legal em apreço, a saber:

1. A frequência com que se verificaram utilizações abusivas de caixas automáticas;

2. A existência de condutas que, em geral, envolvem riscos consideráveis para o comércio jurídico e para o tráfico ou sistemas de provas;

3. A difícil detecção dessas condutas, que mereciam uma repulsa social cada vez mais forte;

4. E a insuficiência dos tipos penais tradicionais (de enriquecimento patrimonial) para protecção do bem jurídico.

De resto, motivações parcialmente coincidentes com as do legislador alemão.

1.1.2. O bem jurídico

Não existe unanimidade acerca da definição e delimitação do bem jurídico tutelado pelo crime de burla informática.

No arranjo de opiniões, há quem entenda que atendendo à inserção sistemática do artigo 221.º o bem jurídico tutelado é essencialmente o **património**[7].

Diversamente, outros[8] entendem que é *também* a **segurança, fiabilidade e integralidade dos programas e dados informáticos e respectivo processamento**.

De modo a afastar quaisquer equívocos, quem perfilha esta segunda solução rejeita que se diga que se as leis de criminalidade informática[9] tutelam já bens de natureza pessoal ou a funcionalidade dos sistemas informáticos, então a burla informática só pode tutelar o património. Na verdade, tal argumento está longe de ser decisivo uma vez que a especificidade desta figura delituosa é justamente a restrição da protecção dos dados e processamento às

[6] ROCHA, Manuel António Lopes, "A Revisão do Código Penal, Soluções de Neocriminalização*", in* Jornadas de Direito Criminal, Centro de Estudos Judiciários, Vol. I, Lisboa, 1996, p. 93.
[7] Na doutrina, podem ver-se nesta orientação, COSTA, José de Faria e MONIZ, Helena, "Algumas reflexões sobre a criminalidade informática em Portugal", *in Boletim da Faculdade de Direito da Universidade de Coimbra*, Vol. LXXIII, 1997, pp. 323-324, e COSTA, A. M. Almeida, *Comentário Conimbricense do Código Penal*, Tomo II, pp. 328 e ss.. Em sentido coincidente, manifestou-se, por exemplo, o Acórdão do Tribunal da Relação de Coimbra, de 15.05.2002, processo n.º 1318/02 (relator Barreto do Carmo).
[8] Na jurisprudência, *vide* os Acórdão do Supremo Tribunal de Justiça, de 06.10.2005, Processo n.º 05P2253 (relator Simas Santos) e do Tribunal da Relação de Évora, de 20.01.2015, Processo n.º 90/11.0GCLLE.E1 (relator João Amaro).
[9] Lei da Protecção Dados Pessoais (Lei n.º 67/98, de 26 de Outubro, a última vez alterada pela Lei n.º 103/2015, de 24 de Agosto) e Lei do Cibercrime (Lei n.º 109/2009, de 15 de Setembro). Doravante, referir-nos-emos a este último diploma sob a designação de LCib.

hipóteses em que o agente tem a "intenção de obter um enriquecimento ilegítimo e causa a outra pessoa prejuízo patrimonial"[10].

1.1.3. A natureza do crime

Olhando à natureza do crime de burla informática – sob o ponto de vista do *grau de lesão do bem jurídico protegido* –, estamos na presença de um **crime de *dano*** na justa medida em que respectiva consumação depende da verdadeira ocorrência de um prejuízo patrimonial de outra pessoa. Este prejuízo há-de recair sobre o património da vítima, "como consequência da manipulação de dados informáticos em que se subsume a acção do agente"[11], "sem a mediação do ofendido ou da pessoa enganada"[12]. Como bem explica Leones Dantas[13], "este prejuízo não é aquele que ocorre nos dados sobre os quais recaiu a acção do agente, porque esse é o espaço de um outro crime – os danos relativos a dados ou programas informáticos a que se refere o artigo 5.º da Lei da Criminalidade Informática (Lei n.º 109/91, de 17 de Agosto)."

Do prisma da *conduta*, estamos perante um crime de ***execução vinculada***. Vale isto por dizer que a lesão do património tem de ocorrer de um dos modos de execução da conduta típica consagrados no n.º 1 do artigo 221.º. Deles nos ocuparemos seguidamente.

Ocorre ainda observar que o crime de burla informática representa um **crime de *resultado parcial* ou *cortado***, pois "a intenção tipicamente requerida [dolo do tipo] tem por objecto uma factualidade [intenção de produção de um resultado] que não pertence ao tipo objectivo de ilícito"[14]. No sentido apontado, basta que se verifique, por isso, o prejuízo patrimonial da vítima – que não a concretização do enriquecimento intencionado pelo autor do delito – para a consumação do ataque ao bem jurídico. Ainda assim, a registar-se essa circunstância (agravante) andará bem o tribunal, segundo o nosso juízo, se a considerar em sede de determinação da medida concreta da pena (artigo 71.º, n.º 2).

[10] *Idem* nota 7.
[11] Cfr. DANTAS, Leonel, "A Revisão do Código Penal e os Crimes Patrimoniais", *in* Jornadas de Direito Criminal do Centro de Estudos Judiciários, Lisboa, 1998, pp. 514-515.
[12] ALBUQUERQUE, Paulo Pinto, *Comentário do Código Penal à luz da Constituição da República Portuguesa e da Convenção Europeia dos Direitos do Homem*, 3.ª edição actualizada, Universidade Católica Editora, Novembro, 2015, p. 860.
[13] *Idem* nota 15.
[14] DIAS, Jorge de Figueiredo*, Direito Penal – Parte Ger.al – Tomo I – Questões Fundamentais; A Doutrina Geral do Crime*, 2.ª edição, Coimbra Editora, 2011. – p. 691.

1.1.4. Elementos do Tipo

Objectivo	Subjectivo
Dano patrimonial causado a outra pessoa; Conduta expressa em: (i) interferência no resultado de tratamento de dados ou mediante incorrecta estruturação de programa informático (ii) uso incorrecto ou incompleto de dados (iii) aproveitamento de dados sem autorização (iv) intervenção no processamento por meio não autorizado	a. Dolo b. Intenção de obter ganho ilegítimo para o agente ou para terceiro;

A) O tipo objectivo

No que concerne ao primeiro elemento tipo objectivo do crime de burla informática, e acompanhando nesta temática a jurisprudência firmada pelo Supremo Tribunal de Justiça[15], dúvidas não subsistem de que a "dimensão típica remete, pois, para a realização de actos e operações específicas de intromissão e interferência em programas ou utilização de dados nos quais está presente e aos quais está subjacente algum modo de engano, de fraude ou de artifício que tenham a finalidade de obter enriquecimento ilegítimo e através do qual se realiza esta específica intenção, **causando a outra pessoa prejuízo patrimonial**." Assim, a verificação de um efectivo prejuízo patrimonial é elemento do tipo objectivo de ilícito, sem o qual o tipo legal não se preenche.

No que se refere ao segundo elemento, temos como orientação o artigo 221.º, n.º 1, do qual derivam as **seguintes modalidades de conduta típica**:

(i) Incorrecta estruturação de programa informático;

(ii) Uso incorrecto ou incompleto de dados;

(iii) Aproveitamento de dados sem autorização; ou

(iv) Intervenção no processamento por meio não autorizado.

Como primeira nota, impõe-se esclarecer que a "interferência no resultado de tratamento de dados" a que alude a norma não é, verdadeiramente, um modo vinculado de execução. Na verdade, a ser válida a doutrina exposta, não colhe a este respeito falar de uma quarta (primeira) modalidade de conduta típica, pois que a "interferência no resultado de tratamento de dados" é antes "consequência necessária da interferência no processamento de dados através dos modos de execução do crime e causa do prejuízo patrimonial"[16]. Ao que se nos afigura, é justamente este o sentido interpretativo congruente com a solução do § 263-a do

[15] Designadamente no Acórdão de 05.11.2008, processo n.º 08P2817 (relator Henriques Gaspar).
[16] Cfr. ALBUQUERQUE, Paulo Pinto, *op. cit.*, p. 861.

Código Penal alemão, onde aliás se fundamenta a norma incriminadora do artigo 221.º, n.º 1, devendo-se a autonomização da modalidade de execução a um possível lapso de tradução.

De resto, decompondo a norma e no que tange à primeira das modalidades, Paulo Pinto de Albuquerque[17] sugere que a *estruturação é incorrecta* (i) "quando é contrária à finalidade do programa informático", podendo operar por via de um "programa já existente ou da criação de um programa que produz resultados falsos". O propósito do agente é manipular o programa informático através de instruções opostas às que tenham sido inicialmente disponibilizadas.

Quanto à conduta (ii) de "*utilização incorrecta de dados*", está em causa a inclusão de dados sem correspondência com a realidade[18]. Por sua vez, o uso incompleto de dados reconduz-se à "introdução parcial de dados verdadeiros que não representam a realidade"[19].

Por outro lado, se o agente *aproveitar dados sem autorização* (iii), sem afectar a sua integridade e verificados que estejam os demais elementos do tipo, comete o crime de burla informática. São enquadráveis nestas operações, a título de exemplo, as seguintes condutas[20]:

- Utilização de cartão de débito e do respectivo código PIN em caixas automáticas por pessoa não autorizada pelo titular, com intenção de obter um enriquecimento ilegítimo, ou por banda do titular, este ultrapassando o limite da disponibilidade monetária concedida;

- Utilização de cartão de débito ou de crédito para pagamento não autorizado num terminal POS (*point of sale*); ou

- Carregamento não autorizado de moeda eletrónica (*smart card*, *pay before card, stored value card*) com o recurso ao código PIN de outrem[21].

Por fim, a "intervenção por qualquer outro modo não autorizado no processamento" (iv) é a variante residual e mais ampla do crime de burla informática, afirmando-se que o legislador, para obstar a lacunas, pretendeu incluir aqui uma plêiade de meios de intervenção não subsumíveis ou de difícil subsunção ao quadro de tipicidade específica do n.º 1 do artigo

[17] Cfr. ALBUQUERQUE, PAULO PINTO, *op. cit.*, p. 860.
[18] De pessoas que não existem, por exemplo. Cfr. ALBUQUERQUE, Paulo Pinto, *op. cit.*, p. 860. A jurisprudência das Relações tende para considerar que o levantamento indevido de dinheiro com cartões bancários ilegitimamente obtidos preenche o tipo de crime de burla informática, na medida em que supõe "utilização não autorizada de dados". Pode ler-se neste sentido a síntese constante da nota prática n.º 11/2017, de 02.11, do Gabinete do Cibercrime da Procuradoria-Geral da República, p. 6, acessível em cibercrime.ministeriopublico.pt..
[19] Como sugere ALBUQUERQUE, Paulo Pinto, *op. cit.*, p. 860, estes podem ser dados localizados no interior do sistema ou em suportes digitais móveis (disquetes, CD-roms, cartões magnéticos ou eletrónicos).
[20] Delas nos dá conta ALBUQUERQUE, Paulo Pinto, *op. cit* ., p. 861 e ROCHA, Manuel António Lopes, *op. cit.*, pp. 94-95.
[21] Não é, porém, esta a posição seguida por Pedro Verdelho. Na opinião do autor, é necessário saber se o PIN está ou não contemplado pelo conceito de dados informáticos, porquanto não existe ainda na lei portuguesa uma definição consistente do que sejam estes dados. Com efeito, Pedro Verdelho defende que o código PIN não se inclui no conceito de dados informáticos e, assim, não preenche os elementos tipo do crime de burla informática. Cfr. VERDELHO, Pedro, "Cibercrime", *in* Direito da Sociedade da Informação, Vol. IV, Associação Portuguesa do Direito Intelectual. Coimbra Editora *apud* AZEVEDO, Ana Helena França, *Burlas Informáticas: Modos de Manifestação*, Tese de Mestrado em Direito e Informática, Universidade do Minho, Janeiro, 2016, pág. 41.

221.º[22]. Assim, a parte final da norma integra uma "cláusula geral que retira à enumeração do preceito o seu carácter taxativo"[23], atribuindo-lhe tão só um carácter exemplificativo.

Na formulação em que se fixou o n.º 1 do artigo 221.º, as modalidades de comissão do crime de burla informática operam numa relação de alternatividade.

B) O tipo subjectivo

O crime de burla informática é um crime doloso, não se admitindo a punição a título de negligência. A conduta do agente pode revestir qualquer uma das modalidades de dolo previstas no artigo 14.º (directo, necessário ou eventual).

No entanto, para lá do dolo relativamente aos elementos objectivos do tipo o legislador requer a verificação de um *elemento subjectivo especial*[24]. Ou, dito de outra forma, requer que o agente prevarique com a intenção de causar um prejuízo patrimonial a outra pessoa ou de obter, para si ou para outrem, um enriquecimento ilegítimo. Ter-se-á aqui em vista o crime de burla informática enquanto crime de *resultado parcial* ou *cortado* na acepção acolhida *supra*, ou seja, "caracterizado por uma descontinuidade entre os tipos subjectivo e objectivo, em que se requer o aludido *animus* de enriquecimento, mas que se consuma com o dano patrimonial da vítima, independentemente da efectiva verificação do benefício económico do sujeito activo da infracção ou de terceiro"[25].

1.1.5. Autoria. Cumplicidade. Ilicitude na comparticipação

Não se registam especificidades a este nível, podendo qualquer uma das condutas catalogadas no n.º 1 do artigo 221.º ser cometidas a título de autoria material, autoria mediata, coautoria, instigação ou cumplicidade (moral ou material) nos termos gerais dos artigos 26.º e 27.º.

Uma palavra mais para dizer que a extensão da tipicidade decorrente do artigo 28.º, n.º 1 não pode ser aplicada ao crime de burla informática. Destarte, aderimos à doutrina de Paulo Pinto de Albuquerque[26] e somos a concordar que a "intenção de obter para si ou para terceiro enriquecimento ilegítimo não é um elemento comunicável por ser elemento subjectivo do tipo". De sorte que "só pode actuar como comparticipante quem tenha tido esta intenção [ou], no caso do cúmplice, o conhecimento da intenção de enriquecimento do autor".

[22] Desde a manipulação de *hardware* à possibilidade de accionar uma caixa automática através de um programa de computador obtido de forma ilegal. Cfr., neste sentido, AZEVEDO, Ana Helena França, *op. cit.*, p. 41.
[23] Citamos novamente o Acórdão do Tribunal da Relação de Coimbra, de 15.05.2002, processo n.º 1318/02 (relator Barreto do Carmo).
[24] *Vide,* para mais desenvolvida informação, DIAS, Jorge de Figueiredo, *op. cit.,* pp. 379-383.
[25] Cfr. COSTA, Almeida, *op. cit*., p. 279.
[26] Cfr. ALBUQUERQUE, Paulo Pinto, *op. cit.*, p. 861.

1.1.6. Punibilidade da tentativa.

Aqui entronca a questão – a que julgamos ser de dar, em termos gerais, resposta afirmativa – da punibilidade da tentativa (artigo 221.º, n.º 3).

Para que se verifique a prática de um crime de burla informática, na forma tentada, faz-se necessária a ocorrência das seguintes circunstâncias:

1) Que o agente *resolva ou decida*, com intenção de obter para si ou para terceiro enriquecimento ilegítimo ou causar a outra pessoa prejuízo patrimonial, utilizar dados sem autorização ou intervir de modo não autorizado no processamento;

2) Que tal crime que o agente decidiu perpetrar *não chegue a consumar-se,* por circunstâncias independentes da sua vontade; e

3) Que o agente pratique *actos de execução* do crime[27].

Uma vez verificadas estas condições, são nesta sede aplicáveis, *mutatis mutandis*, os artigos 22.º e 23.º.

1.1.7. O crime de burla informática por omissão.

No trabalho que aqui se expõe, merece ainda a nossa atenção o comportamento omissivo em sede de burla informática.

No pensamento a que obedece a doutrina italiana, admite-se que "a alteração, por qualquer modo, do funcionamento de um sistema informático ou telemático possa ser obtida através de uma acção ou de uma omissão"[28]. Entre nós, a mesma ideia inspira alguns autores.

---

[27] As considerações do Acórdão do Tribunal da Relação de Évora de 26.06.2012, processo n.º 264/06.6GBPSR.E1 (relator Martinho Cardoso) merecem-nos aqui plena concordância. Na espécie sobre que versou o aresto, discutiu-se se a conduta do agente integrou um acto de execução do crime de burla informática para efeitos do disposto n.º n.º 3 do artigo 23.º. Segundo o preceito, "a tentativa não é punível quando for manifesta a inaptidão do meio empregado pelo agente ou a inexistência do objecto essencial à consumação do crime". Diz assim o artigo que na tentativa impossível "o resultado não sobrevém, seja porque o meio utilizado não é idóneo, seja porque há carência do objecto". Em resposta à questão controvertida, a Relação de Évora julgou que digitar aleatoriamente três códigos não é, por natureza, um meio manifestamente inidóneo para acertar no código de um cartão multibanco (a que o agente acedeu, ilicitamente, contra a vontade do legítimo titular) e proceder ao levantamento de dinheiro, por aquele não ter acertado na combinação correcta. Antes era o "meio adequado de ele [arguido] (…) tentar produzir o resultado de proceder a um levantamento com aquele cartão, mas que, por não ter acertado, não logrou fazer". Desta feita, «verificou-se o circunstancialismo descrito no artigo 22.º, n.º 1, de que "há tentativa quando o agente praticar actos de execução de um crime que decidiu cometer, sem que este chegue a consumar-se", pois que, de acordo com o seu n.º 2 al. b), "são actos de execução ... os que forem idóneos a produzir o resultado típico".» Pelo exposto, outra não pôde ser a conclusão do tribunal se não a de que naqueles autos não se estava perante um caso de tentativa (impossível) não punível, antes o agente tendo cometido mesmo o crime de burla informática na forma tentada.

[28] Cfr. SANTOS, Rita Coelho, *O Tratamento Jurídico-Penal da Transferência de Fundos Monetários Através da Manipulação Ilícita dos Sistemas Informáticos*, *Studia* Jurídica, n.º 82, Coimbra Editora, 2005, pp. 260-261. A autora sumaria o exemplo do "operadora de informática que não cumpre as instruções de serviço, respeitantes à manutenção do sistema informático".

Assim, para melhor fazer compreender a admissibilidade da forma omissiva do delito, Rita Coelho Santos equaciona, "como base de raciocínio, duas hipóteses":

- Hipótese 1: "*A*, empregado de uma instituição bancária, sabendo que se não proceder à actualização obrigatória – imposta pelos seus superiores hierárquicos – do programa informático, não serão debitadas aos clientes (sendo alguns deles seus amigos) as unidades relativas à utilização de cartões de crédito, *nada faz* para evitar o correspondente prejuízo patrimonial para o banco." (Sublinhado nosso)

- Hipótese 2: "*B*, técnico responsável pela manutenção do sistema informático, apercebe-se de uma falha técnica no sistema de tratamento (absolutamente) automatizado de dados, que está a gerar, indevidamente, várias transferências de créditos para todas as contas dos empregados da mesma onde trabalha. Todavia, sabendo que, deste modo, obterá um enriquecimento (ilegítimo), *não procede* à necessária regularização do sistema, causando, em consequência, um prejuízo patrimonial para a entidade empregadora." (Sublinhado nosso)

No primeiro exemplo, o agente não actua sobre o programa informático, como lhe competia fazer, gerando com essa omissão o prejuízo patrimonial do banco. Admitindo que nesta situação "o agente detinha uma posição de garante da não verificação do resultado, face à instituição bancária", a autora citada equipara o cenário em comento à modalidade típica de "estruturação incorrecta de programa" para concluir pela verificação do crime de burla informática por omissão[29].

Na segunda situação moldada, "a alteração do resultado do tratamento informático de dados" apenas poderá ser imputada ao agente caso se entenda estar este "investido num dever (contratual) de garantia do regular funcionamento do sistema informático"[30].

Subjugada ao enquadramento temático descrito, Rita Coelho Santos funda a posição que assume na convicção de que "a natureza vinculada do crime de burla informática não colide com a admissibilidade da sua comissão por omissão, pois a legalidade da sua comissão encontrar-se-á assegurada nos casos em que sobre o agente-omitente recaia um dever jurídico (de fonte legal ou contratual) que pessoalmente o obrigue a evitar esse resultado"[31], em conformidade com o disposto no artigo 10.º, n.º 2[32].

Não fechamos, contudo, as nossas considerações sem dar notícia de outro modo de entender a matéria.

Escrevendo sobre a possibilidade de os crimes de burla informática e nas telecomunicações serem cometidos por omissão, José Atanásio Alfredo[33] aflora o problema noutra perspectiva e

[29] SANTOS, Rita Coelho, *op. cit.*, p. 261. Fica arredada, neste caso, a aplicabilidade do crime de burla, contanto que não se vislumbra qualquer execução vinculada para o tipo de delito. Em bom rigor, "o agente não provoca erro ou engano, uma vez que as suas operações encontram-se sujeitas a um mero controlo formal."
[30] *Idem.*
[31] Cfr. SANTOS, Rita Coelho, *op. cit.*, p. 262.
[32] A norma dispõe que "a comissão de um resultado por omissão só é punível quando sobre o omitente recair um dever jurídico que pessoalmente o obrigue a evitar esse resultado."
[33] Cfr. ALFREDO, José Atanásio, *Algumas questões referentes ao tipo legal da burla*, Universidade Lusófona do Porto, Faculdade de Direito, 2013, pp. 109-110.

explica que «tanto no seu tipo específico, quanto no seu *modus operandis* não parece defensável a ideia da forma omissiva para a sua execução. O texto da norma apresenta uma estrutura que impõe a necessidade de "provocação de factos" para que o delito possa ser concretizado.». O autor afasta assim a omissão com fundamento na natureza de execução vinculada do ilícito típico sob apreciação.

Neste particular, cumpre-nos evidenciar que se, sendo embora um crime de execução vinculada, "a burla [do artigo 217.º] admitirá, em princípio, a comissão por omissão"[34], por identidade de razão o crime de burla informática pode ser praticado não só por acção, como também por omissão.

1.1.8. Agravação da pena

O referido artigo 221.º, n.º 1, prevê o crime de burla informática simples para depois, no seu n.º 5, o agravar – "qualificar" na opinião de Paulo Pinto de Albuquerque[35] – em razão do "valor elevado" e "consideravelmente elevado" do prejuízo patrimonial ocorrido.

Na hipótese prevista na alínea a) do n.º 5 do artigo 221.º a pena aplicável é de prisão até cinco anos[36] ou de multa até seiscentos dias[37/38]. Quando a factualidade típica se enquadra na alínea b) do preceito a pena aplicável é de prisão fixada entre dois e oito anos. As expressões "valor elevado" e "valor consideravelmente elevado" são, já sabemos, conceitos densificados por referência às alíneas a) e b) do artigo 202.º.

De referir que, aos nossos olhos, este agravamento fica a dever-se a uma intenção do legislador no sentido de tutelar mais intensamente o prejuízo patrimonial sofrido pelo ofendido.

1.1.9. A remissão para o artigo 206.º do Código Penal.

A solução do artigo 206.º é aplicável ao crime de burla informática por força do estatuído do n.º 6 do artigo 221.º, ou seja, à burla informática, independentemente de só preencher o n.º 1 ou, também, o n.º 5 do artigo 221.º.

[34] Não obstante as dúvidas suscitadas sobre tal possibilidade, foi neste sentido que decidiu o Acórdão do Supremo Tribunal de Justiça, de 18.06.2008, processo n.º 08P901 (relator Maia Costa).
[35] Cfr. ALBUQUERQUE, Paulo Pinto, *op. cit.*, p. 862.
[36] O que, na fórmula do artigo 41.º, n.º 1, significa que o limite mínimo é de um mês.
[37] Nos termos do artigo 47.º, n.º 1, com o limite mínimo de 10 dias.
[38] Tudo ponderado, a opção pela pena de prisão ou pela pena de multa deve orientar-se pelo regime do artigo 70.º, ou seja, compete ao tribunal decidir pela pena não privativa da liberdade se esta realizar adequada e suficientemente as exigências de prevenção especial e geral que o caso concreto suscite (artigo 40.º).

1.1.10. Pressupostos de procedibilidade

Conforme decorre do preceituado no n.º 4 do artigo 221.º, o crime de burla informática tem natureza *semi-pública*[39], assim conservando a natureza definida para o crime base de burla.

Tal significa que a legitimidade do Ministério Público para o exercício da acção penal depende da prévia comunicação do facto pelo ofendido ou por pessoa legalmente legitimada para o efeito, fazendo-se necessária a apresentação de queixa[40] (artigos 113.º e 49.º do Código de Processo Penal).

Na opinião de Miguez Garcia e Castela Rio[41], a legitimidade para o exercício deste direito de queixa pertence à pessoa que sofre o prejuízo patrimonial e não ao proprietário ou utente dos dados ou programas informáticos.

Neste particular, uma referência é devida para registar que, no entendimento de Paulo Pinto de Albuquerque[42], o crime de burla informática apenas reveste natureza *semi-pública* quando cometido na sua *forma simples*, ou seja, quando se encontre abrangido pelos segmentos tipificados nos n.ºs 1 e 2 do artigo 221.º. Esta natureza já não subsistirá quando a situação for enquadrável no n.º 5 da mesma disposição legal – caso em que o autor defende que o crime é qualificado –, assumindo natureza pública.

Acolhendo esta teoria, achar-se-ia dispensada a apresentação de queixa, bastando que o Ministério Público tivesse conhecimento da infracção para que, em obediência ao princípio da oficialidade, instaurasse o competente inquérito (artigos 241.º e 262.º, n.º 2, do Código de Processo Penal).

Quanto a nós, entendemos que se é verdade que a inserção sistemática da norma de agravação poderia legitimar um tal entendimento, uma vez que o n.º 4 pelo qual se determina que "o procedimento criminal depende de queixa" antecede a norma de agravação, verdade é também que fosse essa a intenção do legislador e por certo o respectivo tipo legal estaria autonomizado.[43]

1.1.11. A responsabilidade penal das pessoas colectivas

O artigo 11.º consagra o princípio da responsabilidade penal das pessoas colectivas de acordo com o seguinte critério de imputação: actos dos órgãos ou representantes *em nome* e *no*

[39] A natureza do crime releva para controlar o prazo para o exercício do direito de queixa pelo respectivo titular e para aferir da legitimidade do Ministério Público para exercer a acção penal.
[40] O direito de queixa funciona como pressuposto de procedibilidade e traduz-se numa declaração de vontade do ofendido, correspondente a um direito pessoal do titular do interesse especialmente protegido pela incriminação.
[41] *Apud* ALBUQUERQUE, Paulo Pinto, *op. cit.*, p. 862.
[42] *Idem.*
[43] Decidindo que "o crime de burla informática, mesmo quando agravado, tem natureza semi-pública", o Acórdão do Tribunal da Relação de Lisboa, de 26.05.2011, processo n.º 1412/08.7TAVFX.L1, não aderiu à orientação exposta. No aresto pode ler-se que "se o legislador pretendesse que a burla informática agravada fosse um crime público seguramente que o teria previsto em artigo autónomo, tal como o fez para a burla (artigos 217.º e 218.º CP)."

interesse da pessoa colectiva. Fixada esta premissa, o texto do n.º 2 da norma permite-nos concluir que os crimes de burla informática (e nas comunicações) se subsumem à tipificação dos crimes do catálogo susceptíveis de virem a justificar a aplicação de uma sanção penal a uma pessoa colectiva, na medida em que sejam praticados por e através dela.

Queremos com isto dizer que o nosso legislador previu, *expressis verbis*, a possibilidade de uma pessoa colectiva vir a ser responsabilizada criminalmente pela prática de qualquer daquelas infracções.

Descortinando por que modo concreto uma pessoa colectiva pode ser responsabilizada no âmbito da investigação dos crimes de burla informática (e nas comunicações), atendemos ao que se prescreve nas alíneas a) e b) do n.º 2 sobre o "quem" que pode desencadear a responsabilidade penal de um ente colectivo. Destarte, do cotejo da alínea a) com a alínea b) deriva que "a pessoa colectiva, para efeitos da sua responsabilização penal, deve ter agido através dos seus representantes legais (…), que tenham agido no seu interesse e por sua conta."[44]

No mais, e sem particularidades de realce, a concretização da responsabilidade penal das pessoas colectivas pela prática dos crimes em apreço obedecerá às directrizes traçadas pelos restantes números do artigo 11.º.[45]

1.1.12. Relação que intercede entre o crime de burla informática e outros tipos legais

A. O crime de burla informática em confronto com o crime base de burla

O crime de burla informática distingue-se do crime base de burla do artigo 217.º. Em nossa opinião, são dois os critérios que orientam a apontada distinção entre as normas incriminadoras dos artigos 221.º e 217.º.

Primeiramente, e para os efeitos que temos em vista, os dois tipos legais afastam-se porque "no crime geral de burla o agente determina alguém (pessoa física ou colectiva), por meio de erro ou engano, à prática de um acto lesivo do património", ao passo que o crime de burla informática se consuma mediante o recurso às operações descritas no respectivo preceito, que se traduzem na manipulação abusiva dos meios informáticos. Num enunciado simplista, aqui não há a indução em erro de alguém; quem é induzido em erro é a máquina[46]. Já na esfera do

[44] MEIRELES, Mário Pedro, "A responsabilidade penal das pessoas colectivas ou entidades equiparadas na recente alteração ao Código Penal ditada pela lei 59/2007, de 4 de Setembro: algumas notas", *in* Julgar Online, N.º 5, Maio, 2008, pp. 121-138 (130). [retirado de http://julgar.pt/responsabilidade-penal-das-pessoas-colectivas/].

[45] A natureza sucinta e não exaustiva que imprimimos a esta passagem do nosso excurso, não nos autoriza a tratar aqui de questões de direito processual penal suscitadas pela sujeição de uma pessoa colectiva a um processo de natureza criminal. Nesta matéria, podem ter-se como orientações a seguir as perguntas e respostas cogitadas por Pedro Meireles.

[46] Neste sentido, "o prejuízo patrimonial é consequência adequada da conduta do agente, sem a mediação do ofendido ou da pessoa enganada, no que se afasta da estrutura tradicional do crime de burla". Cfr. ALBUQUERQUE, Paulo Pinto, *op. cit.*, p. 860. Em decisão lapidar, o Acórdão do Tribunal da Relação de Coimbra, de 15.05.2002, processo n.º 1318/02 (relator Barreto do Carmo) escreveu que "o crime de burla informática realiza-se num

artigo 217.º o **agente cria *no sujeito passivo*** um estado de erro que por seu turno o leva à prática de actos de diminuição patrimonial (própria ou alheia), deparando-se com um *iter criminis* que comporta um (duplo) nexo de causalidade.

A mais deste critério fundado no sujeito passivo do engano conscientemente entabulado pelo agente da infracção, os tipos legais em exame divergem pelo facto de o crime de burla poder ser cometido através de qualquer meio susceptível de causar na pessoa do ofendido erro ou engano e, em consequência da viciação da vontade de que foi objecto, determiná-lo à prática de actos lesivos do património, seu ou alheio, enquanto que no crime de burla informática – repisando os considerandos que *supra* se tomaram e que ora se dão por integralmente reproduzidos – a consumação tem de resultar da utilização de algum dos meios descritos no n.º 1 do artigo 221.º. Nas palavras de Pinto de Albuquerque[47], há uma relação de exclusão entre o crime de burla e o crime de burla informática, dado os diferentes modos de execução".

Com esta traça jurídica, o crime de burla informática afasta-se estruturalmente do crime base de burla, contanto que as situações enquadráveis no artigo 221.º não realizam a espécie de burla do artigo 217.º[48].

Para melhor ilustrar o que se deixa afirmado atentemos nos seguintes cenários[49]:

- Hipótese 1: O agente que apresenta um cartão falso a um empregado de um estabelecimento comercial que, na convicção errónea da sua legitimidade e titularidade, o passa num terminal POS, comete o **crime de burla do artigo 217.º**.

- Hipótese 2: Se o agente apresenta um cartão falso a pessoa autorizada a operar com um terminal POS, sabendo esta da falsidade do cartão, entre a conduta daquele e o processo automático de pagamento, decorrente da passagem do cartão no dispositivo, não há a intervenção de um sujeito passivo em erro sobre a veracidade do cartão de crédito. O agente comete, nesta hipótese, o **crime de burla informática**.

Em jeito de conclusão, entre os artigos 217.º e 221.º, n.º 1 há uma relação de alternatividade ou exclusividade típica, pois as situações enquadráveis no artigo 221.º, n.º 1 nunca realizam o tipo de burla previsto no artigo 217.º.

B. O concurso de crimes

Neste ensejo, o problema do concurso de crimes merece detida consideração.
Neste particular e por manifesta impossibilidade de esgotamento de todas as situações em que é conjecturável e discutível uma hipótese de concurso, seja efectivo ou aparente, entre a

atentado directo ao património, isto é, num processo executivo que não contempla, de permeio, a intervenção de outra pessoa (por isso não comporta o duplo nexo de imputação causal referido no artigo 217.º)."
[47] Cfr. ALBUQUERQUE, Paulo Pinto, *op. cit.*, p. 862.
[48] Esta é, de resto, a conclusão que se extrai de uma leitura atenta do Acórdão do Tribunal da Relação do Porto de 03.02.2016, processo n.º 482/10.2SJPRT.P1 (relator Eduarda Lobo).
[49] Que não são, contudo, da nossa autoria.

burla informática e outro tipo legal, cuidaremos de seguida das situações que se colocam com maior frequência na prática judiciária.

Burla informática vs. Falsidade informática

Analisado o problema, parece assente existir uma relação de *concurso efectivo* entre o crime de burla informática e o crime de falsidade informática (artigo 3.º, n.º 1, da Lei do Cibercrime) porquanto são diversos e autónomos, entre si, os bens jurídicos tutelados por cada uma das incriminações[50].

Na decisão colocada à apreciação do Tribunal da Relação do Porto, que se pronunciou em Acórdão datado de 14 de Setembro de 2016[51], teve-se por boa a jurisprudência do Acórdão Uniformizador de Jurisprudência de 5 de Junho de 2013[52], que teve a si subjacente a "similitude dos crimes de burla e de falsificação com os aqui enunciados, de burla e de falsidade na variante informática", para se concluir pela verificação de *concurso efectivo* entre as normas incriminadoras do artigo 221.º, n.º 1 e do artigo 3.º, n.º 1 da LCib. Esta foi outrossim a linha de pensamento secundada pela Relação do Porto na decisão citada.[53]

Burla informática vs. Acesso ilegítimo

Alguns autores tendem a sustentar uma relação de *concurso aparente* entre o crime de burla informática e o crime de acesso ilegítimo (artigo 6.º da Lei do Cibercrime). De entre eles, Paulo Pinto de Albuquerque[54] e Rita Coelho Santos[55] explicam que a prática do crime de burla informática pressupõe como acto prévio, via de regra, "o acesso ilegítimo a um sistema ou rede informáticos ou a intercepção não autorizada de comunicações electrónicas". Em razão desta premissa, a incriminação prevista no citado artigo 6.º da Lei do Cibercrime é consumida pela consagrada no artigo 221.º.

---

[50] A ideia do texto é partilhada por NUNES, Duarte Alberto Rodrigues, "O crime de falsidade informática", *in* Julgar Online, Outubro, 2017, p.43 [retirado de http://julgar.pt/o-crime-de-falsidade-informatica/]. Ao invés, Paulo Pinto de Albuquerque comenta que há uma relação de concurso aparente (consunção) entre o crime de burla informática e o crime de falsidade informática. Cfr. ALBUQUERQUE, Paulo Pinto, *op. cit.*, p. 861. Na doutrina, discute-se se o concurso efectivo a que se adere no texto existe mesmo que "o crime de falsidade informática seja cometido enquanto crime-meio para cometer o crime de burla informática e nas comunicações". Para Duarte Nunes e Paulo Teixeira a resposta não pode deixar de ser afirmativa. Cfr. NUNES, Duarte Alberto Rodrigues, *op. cit.*, p 44 (nota 65) e TEIXEIRA, Paulo Alexandre Gonçalves, *O fenómeno do Phising, Enquadramento Jurídico-Penal*, Dissertação de Mestrado, Lisboa, 2013, p. 23. Contra, manifesta-se MACEDO, João Carlos Barbosa, "Algumas considerações acerca dos crimes informáticos em Portugal", *in* Direito Penal Hoje – Novos desafios e novas respostas, Coimbra Editora, 2009, p. 237 (nota 55).

[51] Processo n.º 2177/09.0PAVNG.P1 (relator Ernesto Nascimento).

[52] Que uniformizou jurisprudência quanto à existência de concurso efectivo entre o crime de falsificação do artigo 256.º, n.º 1, al. a) e o crime de burla do artigo 217, n.º 1.

[53] Para Paulo Pinto de Albuquerque, a relação entre os dois tipos legais focados no texto é de concurso aparecente. Cfr. ALBUQUERQUE, Paulo Pinto de, *op. cit.*, p. 861.

[54] Cfr. ALBUQUERQUE, Paulo Pinto, *op. cit.*, p. 861. Para o autor, identicamente, é aparente a relação de concurso entre o crime de burla informática e os crimes de dano relativo a dados ou programas informáticos, sabotagem informática e intercepção ilegítima, "sendo estes factos não puníveis". Cfr. ALBUQUERQUE, Paulo Pinto, *op. cit.*, p. 861.

[55] SANTOS, Rita Coelho, *op. cit.*, p. 288.

Já Paulo Alexandre Teixeira[56] sufraga opinião diversa, neste âmbito concluindo por uma relação de *concurso efectivo*. Para o autor, não parece ser correcta a afirmação de que o ilícito tipificado no artigo 6.º da Lei do Cibercrime se reduz a um "mero acto de execução" do crime de burla informática, pois se é verdade que nesse acto assenta a consumação deste delito não é menos verdadeiro o facto de os agentes do crime terem acesso a dados pessoais da vítima que não se esgotam em informações bancárias.

Ademais, a punição em concurso aparente lograria mitigar a aplicação do n.º 2 do artigo 6.º da Lei do Cibercrime.

Na jurisprudência do Supremo Tribunal de Justiça[57], lê-se que "pela amplitude da descrição, o tipo do artigo 221.º, n.º 1, do Código Penal, parece constituir um *plus* relativamente ao modelo de protecção contra o acesso ilegítimo a um sistema ou rede informática, previsto no artigo 7.º da Lei 109/91, de 17-08 (Lei da Criminalidade Informática)."

Burla informática vs. Furto

Outra hipótese de concurso com ampla verificação na prática diária dos tribunais dá-se entre o crime de burla informática e o crime de furto, previsto e punido no artigo 203.º.

A este propósito, ocorre convocar o exemplo relatado no Acórdão do Tribunal da Relação de Évora de 20 de Janeiro de 2015[58]. Na situação sobre que versou o aresto, os arguidos subtraíram à ofendida dois cartões de multibanco, tendo-se de seguida deslocado a uma caixa ATM onde levantaram, por duas vezes, quantias em dinheiro. Com a sua conduta, lograram os arguidos concretizar a intenção deliberada de se apoderarem das quantias monetárias existentes na conta bancária da ofendida e assim obterem "um enriquecimento que sabiam não ser legítimo, em virtude de utilizarem dados da ofendida, contra a sua vontade e causando-lhe prejuízo". No caso em apreço, o Tribunal da Relação dúvidas não teve de que "foram integrados os elementos constitutivos de dois tipos legais de crime distintos – o crime de furto e o crime de burla informática" – e, negando provimento ao recurso interposto, confirmou a condenação dos arguidos em *concurso efectivo*. Neste particular, foi a bipolaridade dos bens jurídicos protegidos por um e outro tipo legal que legitimou a conclusão da verificação de um *concurso efectivo* entre o crime de burla informática e o crime de furto.[59]

[56] TEIXEIRA, Paulo Alexandre Gonçalves, *op. cit.*, pp. 37-39.
[57] Ilustra esta doutrina, designadamente, o Acórdão de 20.09.2006, processo n.º 06P1942 (relator Henriques Gaspar) e de 05.11.2008, processo n.º 08P2817 (relator Henriques Gaspar).
[58] Processo n.º 90/11.0GCLLE.E1 (relator João Amaro).
[59] Passamos a transcrever, por expressivo, o pensamento da Relação de Évora: «(…) reportando-nos ao concurso efetivo que se verifica, enquanto no crime de burla informática está em causa não só o património, ou seja, a integridade patrimonial, mas também a fiabilidade dos dados e a sua proteção, tendo em linha de conta o específico *modus operandi* do sistema informático, no crime de furto o bem protegido é a "disponibilidade da fruição das utilidades da coisa com um mínimo de representação jurídica" (no lapidar dizer do Prof. José de Faria Costa, *in* "Comentário Conimbricense do Código Penal", Tomo II, pág. 30)». Ainda na jurisprudência, *vide* o Acórdão do Tribunal da Relação de Coimbra, de 29.02.2012, Processo n.º 183/10.1GATBU.C1 (relator Paulo Valério). De entre as posições correntes na doutrina sobre o assunto, salientamos que Paulo Pinto de Albuquerque perfilha pensamento idêntico ao que fica relatado no texto. Cfr. ALBUQUERQUE, Paulo Pinto de, *op. cit.*, p. 862.

Em sentido diverso decidiu o Tribunal da Relação de Guimarães, em aresto de 14 de Março de 2012, sobre um caso com contornos substancialmente idênticos.

Na verdade, também aqui o quadro fáctico se reconduziu à utilização de um cartão multibanco – furtado por desconhecidos – com conhecimento do respectivo código, na compra de alguns bens, e para pagamento "de uma prestação de um motociclo". Assim sendo, a questão a decidir era igualmente a da responsabilidade penal de quem utilizou o cartão subtraído e ilegitimamente apropriado, por via da introdução do código no sistema informático de caixas ATM, obtendo um enriquecimento ilegítimo com o correspondente prejuízo patrimonial do titular do cartão.

Porém, analisando a fundamentação do Tribunal constata-se que a questão apreciada pelo tribunal não foi a de saber se estávamos ou não perante uma situação de concurso efectivo de crimes, ou de uma relação de consumpção, mas sim, afastadas tais hipóteses, a de saber qual das previsões típicas, em alternatividade, se mostrava preenchida: a de furto (artigo 203.º) ou a de burla informática (artigo 221.º, n.º 1). Nos termos do decidido, o recurso interposto pelo Ministério Público mereceu provimento e, em consequência, alterou-se a qualificação jurídica dos factos subsumindo-os à previsão do artigo 221.º, n.º 1, condenando os arguidos pela prática de um crime de burla informática.

Burla informática vs. Cartão de crédito

Há quem entenda que o crime de burla informática e o crime de passagem/colocação em circulação de cartão de crédito[60] falsificado como *legítimo*[61/62,] em conluio com o falsificador (artigos 264.º e 265.º), encerram entre si uma relação de *concurso efectivo*, pois que a protecção dispensada ao segundo não esgota a protecção reclamada pelo primeiro.[63]

Chamado a decidir sobre o assunto que ora nos ocupa, o Acórdão do Supremo Tribunal de Justiça de 12 de Setembro de 2009[64] consignou expressivamente que a norma incriminatória

[60] Por força do artigo 267.º, n.º 1, al. c), do Código Penal, o cartão de crédito é equiparado à moeda.
[61] De bastante diversa maneira, o artigo 3.º, n.º 4 da LCib cuida da colocação em circulação de cartões bancários falsos como *falsos*.
[62] Na esteira do que vimos de dizer, a falsificação de cartão de crédito corresponde, se não erramos, à segmentação do artigo 256.º, n.º 1, als. e) e f) e n.º 2, por referência às als. a) e c) do artigo 255.º. O método actualmente mais utilizado na falsificação de cartões de crédito consiste no recurso a uma técnica informática conhecida por *skimming*. Através de um dispositivo de leitura e gravação de bandas magnéticas (*skimmer*) efectua-se a "cópia da banda magnética de um cartão de pagamento, sem o conhecimento ou o consentimento do titular do cartão, que acontece geralmente quando o cartão de pagamento está a ser utilizado pelo titular numa ATM genuína ou num terminal de um ponto de venda [POS - *point of sale*]. Os dados são depois escritos (clonados) em novos cartões que são utilizados para fazer levantamentos ilícitos de dinheiro, o que geralmente acontece fora do país de residência do titular do cartão. O sumariamente descrito consta do Relatório Geral sobre as Atividades da Europol de 2010. Na jurisprudência, o Acórdão do Tribunal da Relação do Porto de 21.11.2012, processo n.º 1001/11.9JAPRT.P1 (relator Borges Martins) bordou identicamente algumas considerações sobre o que acabamos de aflorar.
[63] Nos termos do artigo 264.º, o "passador" de concerto com o falsificador incorre nas penas indicadas nos artigos 262.º e 263.º.
[64] Processo n.º 1008/11.6JFLSB-L1.S1 (relator Armindo Monteiro). O Supremo Tribunal condenou os arguidos que tiveram acesso a cartões de crédito do sistema VISA e *Mastercard* genuínos e, através da duplicação dos caracteres de identificação electrónica codificados na banda magnética, efectuaram cópias das mesmas, obtendo os dígitos que compõem os códigos secretos (PIN) referentes a vários desses cartões validamente emitidos. A manipulação da

da passagem de moeda falsa[65] não consome a tutela dos sistemas informáticos, "o que, à luz de um critério teleológico adoptado pelo legislador na definição da unidade-pluralidade de infracções, no artigo 30.º, n.º 1, do CP, aferida pelo número de tipos legais de crime efectivamente cometidos, leva a conformar uma situação de concurso real, excludente de um concurso aparente de normas"[66].

Burla informática vs. Roubo

É tempo agora de nos debruçarmos sobre a hipótese de concurso entre o crime de burla informática e o crime de roubo.

A este respeito, foi decidido pelo Supremo Tribunal de Justiça[67], que a conduta dos arguidos integrava a prática, em *concurso efectivo*, do crime de roubo e do crime de burla informática. Neste caso, o Tribunal *a quo*[68] tinha entendido que entre o crime de burla informática e o crime de roubo intercedia uma relação de *concurso aparente na modalidade de consumpção*, por considerar, no cerne da sua argumentação, que o "bem jurídico por ambas as incriminações tutelado é o património de terceiro (acrescendo no roubo o elemento pessoal), sendo apenas diversa a forma de obtenção do resultado. Na burla informática mediante aquela interferência em meios telemáticos, no roubo pelo constrangimento de outrem. Porém, tal não acrescenta nenhum elemento de protecção de bem jurídico diverso no caso da burla informática através da utilização de código a que o agente teve acesso mediante a prática de actos idóneos àquele constrangimento."

Inconformado, recorreu o Ministério Público que, na sua motivação e em síntese, concluiu o seguinte: "A utilização pelos arguidos do cartão de débito da vítima no levantamento de quantias em caixas ATM, no pagamento de combustíveis e outros produtos adquiridos deriva de uma ***autónoma resolução criminosa***, que surge já depois de se terem apoderada da carteira da vítima. O acesso ao código daquele cartão não derivou de qualquer forma de coacção autónoma dirigida à vítima pelos arguidos, mas antes de um facto inesperado pelos arguidos, qual seja o número correspondente ao código estar escrito num papel que se encontrava junto ao cartão. A autonomia existente entre as condutas decorrentes da matéria de facto impõe a verificação de uma situação de concurso de infracções, nos termos do artigo 30.º, n.º 1, e 77.º do C.P. Mesmo que tal não ocorresse, **não há coincidência entre os bens**

banda magnética "permitia que, ao serem introduzidos os cartões nos terminais de pagamento ATM ou POS, o sistema informático daqueles os identificasse *como se verdadeiros cartões fossem* e permitisse o levantamento de dinheiro ou o pagamento em terminais POS, digitado o código secreto (PIN) respectivo" (sublinhado nosso).

[65] Na expressão do aresto, o bem jurídico a que a norma assegura tutela é a intangibilidade da moeda, "agora sob uma nova modalidade denominada de dinheiro de plástico, equiparado a moeda".

[66] Em sentido diverso, antes, decidiu o Acórdão do Tribunal da Relação de Lisboa, de 24.04.2007, processo n.º 843/2007-5 (relator Martinho Cardoso).

[67] Em Acórdão de 6 de Outubro de 2005, Processo n.º 05P2253 (relator Simas Santos). Na hipótese vertente, o Supremo Tribunal sumariou nos seguintes termos: "Se depois de roubarem uma carteira, os agentes descobrem nela um cartão multibanco e respectivo código e decidem então utilizá-lo até esgotarem o saldo, o que executam, sem estarem autorizados, cometem um crime de roubo e, em concurso real, um crime de burla informática. No caso há igualmente uma autonomia e pluralidade de resoluções que sempre afastaria a consumpção da burla informática pelo roubo."

[68] Tribunal Colectivo da 1.ª Vara Mista de Sintra, por decisão proferida em 08.04.2000.

jurídicos que são tutelados pelo crime de roubo e os bens jurídicos tutelados pelo crime de burla informática, o que, só por si, impõe a existência de uma situação de concurso efectivo: no roubo, os bens jurídicos assegurados pelo tipo são o direito de propriedade e de detenção, – e a liberdade individual, a integridade física e a vida – já na burla informática os bens jurídicos tutelados são a integridade patrimonial e a fiabilidade dos dados e a sua protecção" (destaques nossos).

1.2. Burla nas Comunicações

O crime de burla nas comunicações cabe na previsão do n.º 2 do artigo 221.º, nos termos do qual incorre na prática deste delito "quem, com intenção de obter para si ou para terceiro um beneficio ilegítimo, causar a outrem prejuízo patrimonial, usando programas, dispositivos electrónicos ou outros meios que, separadamente ou em conjunto, se destinem a diminuir, alterar ou impedir, total ou parcialmente, o normal funcionamento ou exploração de serviços de telecomunicações".

No essencial, os enquadramentos dogmáticos feitos a propósito da burla informática aplicam-se ao delito em apreço[69].

Consuma-se com o preenchimento dos mesmos elementos subjectivos (dolo e intenção de se obter ganho ilegítimo) mas a conduta típica traduz-se em:

1. Uso de programas, dispositivos electrónicos ou outros meios;

2. Destinados a diminuir, alterar ou impedir (total ou parcialmente) o normal funcionamento ou exploração de serviços de telecomunicações.

Na solução perfilhada pelo Acórdão do Tribunal da Relação de Lisboa de 23 de Março de 2011[70], o crime de burla nas comunicações "não exige, apenas, que o agente queira obter um benefício ilegítimo utilizando dispositivos electrónicos ou outros, sendo também necessário que **a utilização desses dispositivos tenha a virtualidade de diminuir, alterar ou impedir o normal funcionamento** dos serviços de telecomunicações" (destaque nosso).

Acresce que, atentos ao texto da norma, afigura-se-nos **não ser igualmente exigível a "intervenção do prejudicado** na concretização do delito"[71], podendo o agente através de meios (programas, dispositivos electrónicos ou outros) que afectem (diminuindo, alternando ou impedindo) o normal funcionamento ou exploração de serviços de comunicação "agir e/ou

[69] "São duas figuras de delito diferentes, porém, equiparáveis. Tanto assim é que, dentro do código foram integradas em uma espécie de regime comum". Cfr. ALFREDO, José Atanásio, *op. cit.*, p. 106. Não assim para Pedro Verdelho, que segue o caminho da distinção entre o crime de burla informática e o crime de burla nas telecomunicações a partir do critério da "vertente patrimonial". *Vide,* VERDELHO, Pedro, *op. cit.*, p. 358.
[70] Processo n.º 4252/07.7TDLSB.L15 (relator Carlos Espírito Santo).
[71] Cfr. nota 46. De maneira equivalente, o n.º 2 do artigo 221.º pressupõe uma ofensa ao património de uma pessoa, sem a sua intermediação em estado de erro que caracteriza a tipicidade do crime de burla.

intervir directamente sobre bens do património da vítima (dados, programas e informações) com um *animus delicte* a fim de causar o prejuízo patrimonial."[72]

A burla nas comunicações caracteriza-se por ser um delito de ***execução vinculada***, perpetrado através da "interferência no processo mecânico do sistema informático e na manipulação do hardware"[73].

Assim, em paralelo com o que se disse a propósito do tipo objectivo do crime de burla informática[74], a actuação do agente apreciada a partir do enunciado do n.º 2 do artigo 221.º tem de ocorrer por via de uma daquelas variantes, sendo que a cláusula geral "outros meios" inserida na parte final da norma não atribui à enumeração do preceito um carácter taxativo, mas tão só exemplificativo. Neste sentido, a especificidade típica da burla nas comunicações como crime de execução vinculada esgota-se na ideia de que a infracção se consome numa ofensa ao bem jurídico do património produzida através de uma interferência nos serviços de telecomunicações.

A título elucidativo, e entre outras igualmente apropriadas, são reconduzíveis à tipicidade específica do n.º 2 do artigo 221.º as seguintes condutas:

- A ligação não autorizada a infraestruturas de rede ligação, usufruindo assim o agente de serviços de televisão sem prévia celebração de contrato para o seu fornecimento[75].

[72] Cfr. ALFREDO, José Atanásio, *op. cit.*, p. 107.
[73] ALBUQUERQUE, Paulo Pinto, *op. cit.*, p. 861.
[74] Cfr. *supra* p. 12.
[75] Foi esta a factualidade investigada nos autos que originaram o Acórdão do Tribunal da Relação de Lisboa, de 22.03.2011 (proc. n.º 4252/07.7TDLSB.L1-5). *In casu*, a assistente ZON TV Cabo Portugal, S.A. recorreu do despacho de não pronúncia proferido nos autos de instrução, pedindo se qualificasse a conduta em causa como integradora dos crimes de burla nas telecomunicações e de furto. Com efeito, a decisão recorrida julgou afastada a prática do crime de burla informática, "porquanto na factualidade descrita não é alegado que, em concreto, tenha havido qualquer *perturbação* do normal funcionamento ou de exploração de serviços de telecomunicações" (sublinhado nosso). De seguida, o tribunal concluiu que se numa primeira abordagem poderia estar em causa a denúncia de um crime de furto, uma análise mais detalhada do sistema vigente desmente esta impressão. Na verdade, "o modelo cristalizado pelo Decreto-Lei n.º 176/2007, de 8 de Maio, alterou a Lei das Comunicações Electrónicas (Lei n.º 5/2004, de 10 de Fevereiro), passando a punir como contra-ordenação a "aquisição, utilização, propriedade ou mera detenção, a qualquer título, de dispositivos ilícitos para fins privados do adquirente, do utilizador, do proprietário ou do detentor, bem como de terceiro (artigos 104.º, n.º 1, al. d), e 113.º, n.º 1, al. sss), da Lei n.º 5/2004)". Quer dizer que por efeito desta alteração legislativa, a detenção ou utilização de equipamentos ilícitos que permitam aceder ilegitimamente ao sinal emitido pela TV Cabo passou a ser punida como contra-ordenação. Sem esgotarmos a argumentação pela qual se determinou a decisão recorrida, certo é que desta feita ficou afastada a prática do crime de furto previsto e punido pelo artigo 203.º. Por seu turno, a Relação de Lisboa tomou posição nos seguintes termos: "O agente que efectuar uma ligação não autorizada a infraestruturas da rede TV Cabo não comete o crime de burla nas comunicações, nem o crime de furto; O mesmo agente, não comete, ainda, a contra-ordenação prevista nos arts. 104, n.º 1, al. d) e 113.º, n.º 1, al. sss), da Lei n.º 5/04, de 10 Fev., que apenas prevêem a circunstância de se adquirir, deter ou utilizar equipamentos ilícitos que permitam aceder de forma não autorizada ao sinal emitido pela TV Cabo." Bebendo de idênticas fontes de inspiração, o mesmo Tribunal tivera já oportunidade de se pronunciar em data anterior sobre a situação moldada. Todavia, o resultado que preconizou foi diferente e resume-se ao seguinte: "O estabelecimento de uma ligação não autorizada à infra-estrutura de rede da TV Cabo, que permite a fruição de um serviço não contratualizado e, por isso, não pago e causa um prejuízo patrimonial àquela empresa, consubstancia apenas a contra-ordenação prevista e punida nos termos da Lei n.º5/2004". *Vide*, para mais desenvolvimentos, o Acórdão do Tribunal da Relação de Lisboa de 17.12.2008, processo n.º 10876/2008-3 (relator Carlos Almeida). Pela nossa parte, recordamos que a Lei das Comunicações Electrónicas foi sendo sucessivamente alterada, correspondendo hoje o citado artigo 113.º, n.º 1, al. sss) à al. oo) do n.º 2 do preceito.

- A entrada no tráfego da operadora telefónica, desviando assim o agente o tráfego, sobretudo internacional, das chamadas destinadas a clientes de uma operadora móvel para equipamentos localizados em Portugal nas instalações de uma sociedade da qual era administrador[76].

2. Prática e gestão processual

No capítulo que agora se abre, no qual se procurará adoptar uma perspectiva mais prática, ainda que não descurando necessárias considerações de índole teórico-explicativa, definiremos, em linhas gerais, o trajecto a percorrer em sede de investigação criminal desde o momento da aquisição da notícia do crime até ao momento do encerramento do inquérito.

Um alerta é devido para registar que, por razões de economia e de razoabilidade, não se traçará uma linha modelo de direcção de inquérito relativo aos tipos legais sob análise, contanto que considerações gerais sobre a instrução do inquérito e a condução do mesmo pelo Ministério Público não são o objecto primordial do presente estudo, optando-se outrossim por identificar as especificidades reclamadas pela investigação dos crimes de burla informática e nas comunicações.

2.1. Considerações introdutórias

Não podemos deixar de referir que a tipicidade de execução dos crimes de burla informática e nas comunicações revela necessidades de **especialidade técnica quanto à sua investigação**.

Assim, os inquéritos relativos à criminalidade informática encerram dificuldades acrescidas em termos de prova e a sua investigação reclama, não raras vezes, conhecimentos especializados, que vão desde as perícias a sistemas informáticos à recolha de prova digital.

Face ao evoluir das características do tecido da criminalidade informática e à constância das dificuldades que a sua investigação suscita (de entre elas destacando-se o avolumar de processos e a carência de meios humanos especializados) são necessárias alterações ao nível das estruturas de resposta em ordem a evitar o prolongamento excessivo dos inquéritos dedicados a este tipo de delitos.

O **criminoso informático** não tem a mesma personalidade do infractor ou criminoso tradicional: não é marginal e inadaptado, mas, pelo contrário, socialmente bem integrado.

[76] Cfr. Acórdão do Tribunal da Relação de Lisboa, de 24.01.2007, Proc. n.º 5990/2006-3 (relator Pedro Mourão). Depois de entregar esse tráfego aos destinatários através de chamada telefónica por si realizada, o agente transformava o tráfego fixo-móvel e internacional em tráfego que para a operadora figurava como tráfego móvel-móvel, ficando esta impedida de receber a respectiva contrapartida. No caso *sub judice*, o Tribunal sentenciou que, logrando o arguido, ao desviar o fluxo de chamadas internacionais, «"mascarar" o tráfego por ele cursado», se verificou a perturbação do normal funcionamento ou exploração de serviços de telecomunicações prevista pelo n.º 2 do artigo 221.º. De facto, a conduta descrita surtiu efeitos negativos para a operadora "quanto à respectiva qualidade de serviço, qualidade da entrega, interconexão entre custos e receitas, comissões pagas e descontos contratualmente aplicáveis, falha na prestação do serviço de *roaming,* dificuldade no registo de clientes estrangeiros nas redes das operadoras e no programa de exclusividade de contratado de interligação".

Neste âmbito, vale a pena distinguir o criminoso informático do infractor tradicional.

Conhecendo algumas características que lhe são comuns, o perfil daquele é descrito como alguém especialmente dotado de capacidade intelectual para adquirir conhecimentos no seio da informática e assim praticar actos ilícitos. Quer dizer, por isso, que é a personalidade do agente, e bem assim o móbil potenciador da resolução criminosa – no quadro de equipamentos sofisticados e de especialidade de programas informáticos – que distinguem o perfil do criminoso informático, permeável e à consumação de crimes que por outros meios eventualmente não praticaria.

No sentido apontado, a burla informática, "é frequentemente obra dos agentes que pertencem à categoria criminológica do col blanc ou do white colar"[77].

2.2. Dados Estatísticos

Segundo dados do Relatório Anual de Segurança Interna[78], os crimes de burla informática e nas comunicações apresentam um aumento de 7,9% no total da criminalidade participada.

Não obstante, cumpre referir que este valor poderá não ser exacto e justificável pelo facto de em razão de irregular classificação, terem sido ali incluídos crimes informáticos previstos na Lei do Cibercrime e outros que podem ser praticados com recurso à tecnologia informática.

2.3. Investigação criminal

A iniciar, cumpre aqui recordar o que a propósito dos pressupostos de procedibilidade se deixou dito, salientando que, via de regra, os crimes de burla informática e nas comunicações assumem natureza semi-pública, estando nessa medida **dependentes de queixa**. Apenas não será assim para quem, como Paulo Pinto de Albuquerque[79], entenda que nos casos previstos no artigo 221.º, n.º 5, o crime reveste natureza pública.

2.3.1. Primeiro despacho/Delegação de competências

Em primeira linha, não poderá descurar-se que os tipos legais previstos no artigo 221.º integram a previsão normativa do artigo 3.º, alínea g), da Lei n.º 96/2017, de 23 de Agosto, que define os objectivos, prioridades e orientações de política criminal para o biénio de 2017-2019, constituindo nessa medida um **crime de investigação prioritária**.

[77] *Apud* CORREIA, Pedro Miguel Alves Ribeiro e JESUS, Inês de Oliveira Andrade de, "Combate às transferências bancárias ilegítimas pela Internet no direito português: entre as experiências domésticas e políticas globais concertadas", *in* Revista Direito GV, São Paulo, V. 12, n.º 12, Maio-Agosto 2016, pp. 543-563 (548).
[78] Cfr. *supra* nota 1.
[79] Cfr. *supra* p. 15.

No mais, os tipos legais sob apreciação encontram-se, igualmente, abrangidos pela alínea l), do n.º 3, da Lei de Organização da Investigação Criminal[80], sendo a **investigação da competência reservada da Polícia Judiciária**.

Por outro lado, impõem-se três advertências de cariz prático:

a. Havendo já algum indício de que o crime tenha sido praticado através de sistema informático bancário, deverá oficiar-se às entidades bancárias, solicitando a remessa dos elementos bancários pertinentes;

b. Existindo algum elemento que permita a identificação sobre o fornecer de serviço de internet, deverá preencher-se e remeter-se o respectivo formulário – Circular da Procuradoria Geral da República n.º 12/2012 e Nota Prática do Gabinete do Cibercrime n.º 8/2016, de 18 de Fevereiro de 2016.

De resto, a linha investigatória será definida em função do circunstancialismo presente nos concretos autos.

2.3.2. Meios de prova/Meios de obtenção de prova

Neste tocante, os meios comuns de investigação e prova em processo penal – meios de prova e meios de obtenção de prova – mantêm a sua vigência nos termos gerais do Código de Processo Penal.

A este propósito, pensamos no recurso à **busca e apreensão de material informático** que serve de suporte à prática do crime de burla informática.

Identicamente, a **prova pericial** conserva a sua valia se pensarmos, por exemplo, na realização de uma perícia ao material informático apreendido a um arguido indiciado pelo crime de burla informática com o fito de demonstrar que *software* específico o agente utilizou e que instruções determinou em ordem ao tratamento de dados relativos a ATM's, considera-se justificadamente útil para se poder concluir, ou não, pela prática daquele delito[81].

Não obstante, o incremento da prática do crime de burla informática traz consigo a discussão de questões processuais de implicação prática que nos obrigam a superar o quadro normativo do Código de Processo Penal, hoje deficitário para responder a novas realidades de criminalidade informática.

[80] Lei n.º 49/2008, de 27 de Agosto, a última vez alterada pela Lei n.º 57/2015, de 23 de Junho.
[81] Acórdão do Tribunal da Relação de Évora de 19.11.2015, processo n.º 133/13.3GBODM.E1 (relator Carlos Jorge Berguete).

➢ **Lei do Cibercrime**

Reconhecendo a inadequação das diligências processuais (meios de prova e meios de obtenção de prova) "tradicionais" à criminalidade situada no âmbito informático-digital, o legislador reconheceu a necessidade de ultrapassar o regime processual penal, de modo a fornecer ao sistema normas que permitam a aquisição e produção de prova na investigação de crimes informáticos em geral, e bem assim de crimes perpetrados por via de sistemas informáticos/computadores.

Neste ensejo, a adopção de medidas especiais para a investigação dos crimes em espécie concretizou-se por via da Lei do Cibercrime.

Assim, o regime processual das escutas telefónicas previsto nos artigos 187.º a 190.º, do Código de Processo Penal deixou de ser aplicável por extensão às «telecomunicações electrónicas», «crimes informáticos» e «recolha de prova electrónica (informática)» desde a entrada em vigor daquele diploma[82].

Para a prova electrónica preservada ou conservada em sistemas informáticos existe um novo sistema processual penal: o previsto nos artigos 11.º a 19.º da LCib coadjuvado pela Lei n.º 32/2008[83], de 17 de Julho, neste caso se estivermos perante dados de "localização celular conservada"[84].

Neste conspecto e muito em particular, releva esclarecer e densificar a aplicação da Lei do Cibercrime à burla informática.

Desde logo, cumpre notar que neste diploma coexistem **dois regimes processuais distintos**:

a. O regime dos artigos 12.º a 17.º;

b. O regime dos artigos 18.º a 19.º.

[82] "Alteração envergonhada do Código de Processo Penal pela lei do Cibercrime" lhe chama Dá Mesquita. O autor é de opinião que o Capítulo III (disposições processuais) da Lei do Cibercrime deve ser tido como um «"escondido Capítulo V" ("Da prova electrónica"), do Título III ("Meios de obtenção de prova") do Livro III ("Da prova") do Código de Processo Penal». Cfr. DÁ MESQUITA, Paulo, in "Processo Penal, Prova e Sistema Judiciário", Wolters Kluwer/Coimbra Editora, 2010, p. 101 e 117.

[83] A Lei n.º 32/2008, de 17 de Julho, impõe aos fornecedores de serviços de comunicações electrónicas, publicamente disponíveis ou de uma rede pública de comunicações, a obrigação de conservarem pelo período de um ano, os dados necessários para: encontrar e identificar a fonte de uma comunicação; encontrar e identificar o destino de uma comunicação; identificar a data, a hora e a duração de uma comunicação; identificar o tipo de comunicação; identificar o equipamento de telecomunicações dos utilizadores, ou o que se considera ser o seu equipamento.

[84] Face ao teor da exposição *supra,* afirma-se que o diploma de 2008 somente está em vigor na parte "arquivística", porquanto os seus artigos 3.º e 9.º foram revogados pelo regime processual penal (para dados informáticos) contido nos artigos 11.º a 19.º da LCib. Vale destacar que as disposições processuais da Lei n.º 32/2008 se apresentam revogadas e substituídas pelo regime processual que consta dos artigos 11.º a 19.º da LCib para todos os dados em geral, isto é, para todos os dados que não estejam especificamente previstos no n.º 1 do artigo 4.º daquela lei. Já não assim relativamente a todos os dados que se furtem à previsão desta norma, como sejam os dados de "localização celular conservada."

"A diferenciação de regimes assenta na circunstância de os dados preservados nos termos dos artigos 12º a 17º [da Lei do Cibercrime] se referirem à pesquisa e recolha, para prova, de dados já produzidos mas preservados, armazenados, enquanto o artigo 18º do diploma se refere à intercepção de comunicações electrónicas, em tempo real, de dados de tráfego e de conteúdo associados a comunicações específicas transmitidas através de um sistema informático"[85/86].

Aquele primeiro regime (**artigos 12.º a 17.º**) surge como regime processual geral do cibercrime e da prova electrónica e **aplica-se**, por remissão do artigo 11.º da LCib, aos crimes nela previstos [alínea a)], que são ou foram cometidos **por meio de um sistema informático** [alínea b)] ou em relação aos quais seja necessário **proceder à recolha de prova em suporte electrónico** [alínea c)], *desde que não esteja em causa a intercepção de comunicações.*

O regime do **artigo 18.º, n.º 1**, que disciplina a intercepção das comunicações, conservando a aplicação do Código de Processo Penal (por remissão do seu n.º 4[87]), **aplica-se** aos crimes previstos na Lei do Cibercrime [alínea a)] e aos crimes cometidos por meio de um sistema informático ou em relação aos quais seja necessário proceder à recolha de prova em suporte electrónico quando tais crimes se encontrem previstos no artigo 187.º do Código de Processo Penal [alínea b)].

No que se refere o **artigo 19.º**, que prevê as "Acções Encobertas", aplica-se igualmente aos crimes previstos na Lei do Cibercrime [alínea a)] e aos "cometidos por meio de um sistema informático, quando lhes corresponda, em abstracto, pena de prisão de máximo superior a 5 anos ou, ainda que a pena seja inferior, e sendo dolosos, os crimes contra a liberdade e autodeterminação sexual nos casos em que os ofendidos sejam menores ou incapazes, a burla

[85] Cfr. Acórdão do Tribunal da Relação de Évora, de 06.01.2015, Processo n.º 6793/11.2TDLSB-A.E1 (relator João Gomes de Sousa).
[86] Fazendo uso da elucidativa explanação contida na decisão *supra*, "que o regime processual de aquisição de prova nos crimes informáticos responde às seguintes regras":
– Nos artigos 11.º a 17.º da LCib prevê-se um regime processual de aquisição e produção de prova cujo pressuposto de aplicação, se não estiver em causa a intercepção de comunicações, é que esteja em causa um os crimes do n.º 1 daquele artigo 11.º;
– Se estiver em causa a intercepção de comunicações, a LCib estabelece, no seu artigo 18.º, n.º 1, alínea a), que relativamente aos crimes nela previstos se aplica o regime dos artigos 18.º e 19.º;
– Da mesma forma se aplica o regime dos artigos 18.º e 19.º da LCib se igualmente estiver em causa a intercepção de comunicações e se se tratar de crimes a que se referem as alíneas a) e b) do artigo 18.º do diploma. Com duas nuances, por assim dizer: uma é a especial inclusão dos crimes previstos na alínea b) no elenco no n.º 1 do artigo 187.º do Código de Processo Penal; outra o facto de o regime dos artigos 187.º a 190.º do Código de Processo Penal ser chamado a título de direito subsidiário, aplicável apenas na medida em que não contraria as disposições dos artigos 18.º (artigo 18.º, n.º 4, da LCib).
– O 189.º do Código de Processo Penal, como procurámos aclarar, nunca é aplicável a crimes informáticos.
Com efeito, relativamente aos crimes informáticos, onde pensamos incluir-se o crime de burla informática, o Código de Processo Penal passou a ser uma fórmula vazia de sentido, qual "diploma dispensável e secundário", se não houver "intercepção de comunicações" e se não estiverem em causa as infracções da consignada alínea b) do artigo 18.º da Lei do Cibercrime.
Do nosso ponto de vista, faz-se notar que o crime de burla informática integra a previsão das als. b) e c) do n.º 1 do artigo 11.º da LCib, observando-se que "a pretensão do legislador é a de, declaradamente, alargar o âmbito de aplicação da lei até onde haja necessidade de fazer prova com o conteúdo existente em qualquer "sistema informático"».
[87] "No que constitui uma remissão expressa que substitui o regime de extensão previsto no artigo 189.º do Código de Processo Penal. Na prática, a aplicabilidade actual do artigo 189.º do Código de Processo Penal aos crimes informáticos é nenhuma." Assim pode ler-se na decisão da Relação de Évora *supra* citada.

qualificada, a **burla informática e nas comunicações**, a discriminação racial, religiosa ou sexual, as infracções económico-financeiras, bem como os crimes consagrados no título iv do Código do Direito de Autor e dos Direitos Conexos [alínea b)].

Sendo necessário o recurso a estas acções encobertas previstas pelo artigo 19.º da LCib observam-se, naquilo que for aplicável, as regras previstas para a intercepção de comunicações, impondo-se, designadamente, a adequação aos fins de prevenção e repressão criminais identificados em concreto e proporcionais, quer a essas finalidades, quer à gravidade do crime sob investigação (artigo 3.º, n.º 1, da Lei n.º 101/2001, de 25 de Agosto); e fundadas suspeitas da prática de um dos crimes previstos no n.º 1 do artigo 19.º, n.º 1, da LCib). No mais, e por remissão do n.º 2 do artigo 19.º da LCib para o artigo 18.º da mesma lei, o recurso às acções encobertas "só pode[m] ser autorizado[s] durante o inquérito, se houver razões para crer que a diligência *é indispensável para a descoberta da verdade* ou que a *prova seria, de outra forma, impossível ou muito difícil de obter*, por *despacho fundamentado do juiz de instrução* e mediante *requerimento do Ministério Público* (sublinhados nossos). Por último, o legislador apela à necessidade de delimitação dos dados cuja obtenção se tem em vista em razão das particularidades da investigação (artigo 18.º, n.º 3, *ex vi* artigo 19.º, n.º 2, ambos da LCib).

Assentes estas considerações e focando-nos naquele que é o nosso desígnio primordial, em termos esquemáticos, o(s) regime(s) de prova previstos na **Lei do Cibercrime aplicar-se-ão à burla informática e nas comunicações** nos seguintes termos:

a. O regime previsto nos artigos 12.º a 17.º, *ex vi* do artigo 11.º, n.º 1, alíneas b) e/ou c);

b. O regime do artigo 18.º apenas será aplicável, considerando o disposto na sua alínea b), se em causa estiver o crime de burla informática agravado (artigo 221.º, n.º 5), já que só nesse caso a burla informática integrará o catálogo de crimes previsto no artigo 187.º, especificamente a alínea a), não sendo em qualquer caso um crime da alínea a) daquele artigo 18.º;

c. O regime do artigo 19.º será sempre aplicável à burla informática e nas comunicações, porquanto esta se encontra expressamente prevista no seu n.º 1, desde que se verifiquem os requisitos que a lei impõe.

Assim, impõe-se a questão: *quais são, afinal, os meios de obtenção de prova que "o crime de burla informática e nas comunicações irá buscar na Lei do Cibercrime"?*

I. O referido artigo 11.º da LCib remete para um conjunto de instrumentos processuais que a lei apresenta sequencialmente nos seus **artigos 12.º a 17.º**. Nesta medida, na investigação do crime de burla informática recorrer-se a qualquer das diligências processuais previstas nesses artigos, a saber:

a. Preservação expedita de dados (artigo 12.º)

b. Revelação expedita de dados de tráfego (artigo 13.º)

c. Injunção para apresentação ou concessão do acesso a dados (artigo 14.º)

d. Pesquisa de dados informáticos (artigo 15.º)

e. Apreensão de dados informáticos (artigo 16.º)

f. Apreensão de correio electrónico e registos de comunicações de natureza semelhante (artigo 17.º).

Ressalvados os casos[88] em que operam as causas que desencadeiam a obrigatoriedade legal de intervenção do juiz, a competência para ordenar ou autorizar as operações previstas nos citados artigos 12.º a 16.º é da autoridade judiciária concretamente competente na fase processual em que se situarem os autos. Pontualmente, podem os órgãos de polícia criminal ordenar algumas dessas diligências[89]. Na situação moldada pelo artigo 17.º da LCib é o juiz quem pode ordenar ou autorizar a respectiva apreensão.

II. As acções encobertas previstas no artigo 19.º

No que se refere às acções encobertas[90] no contexto da investigação dos crimes de burla informática e nas telecomunicações, cabe-nos destacar apenas a necessidade de requerimento do Ministério Público dirigido ao JIC, no qual conste[91], fundamentadamente:

- A adequação da acção aos fins de prevenção e repressão criminais identificados em concreto, nomeadamente a descoberta de material probatório;

- A proporcionalidade da mesma, quer àquelas finalidades pretendidas, quer à gravidade do crime em investigação; e

- A sua indispensabilidade *para a descoberta da verdade* ou que a *prova seria, de outra forma, impossível ou muito difícil de obter*, por *despacho fundamentado do juiz de instrução* e mediante *requerimento do Ministério Público* (sublinhados nossos).

➢ **Notas práticas do Gabinete de Cibercrime da Procuradoria Geral da República**

Com particular relevo nesta matéria, deverá atentar-se ao conteúdo das Notas Práticas do Gabinete de Cibercrime da Procuradoria Geral da República, designadamente, Nota Prática n.º

[88] Referidos a dados pessoais ou íntimos do artigo 16.º, n.º 3, da LCib, de acesso e apreensão de correio electrónico ou semelhante e a segredo profissional, de funcionário ou de Estado.
[89] No caso dos artigos 12.º, n.º 3, 15, n.º 3 e 16, n.º 3, da LCib.
[90] Cfr. Lei n.º 101/2001, de 25 de Agosto.
[91] Em cumprimento das disposições conjugadas dos artigos 3.º, n.º 1 da Lei n.º 101/2001 e artigo 18.º da LCib, *ex vi* do artigo 19.º, n.º 2, da LCib.

1/2012, Nota Prática n.º 2/2013, Nota Prática n.º 3/2014, Nota Prática n.º 4/2014, Nota Prática n.º 5/2015, Nota Prática n.º 6/2015, Nota Prática n.º 7/2015, Nota Prática n.º 8/2016, Nota Prática n.º 9/2016, Nota Prática n.º10/2016, Nota Prática n.º 17/2017.

2.3.3. Encerramento do inquérito

Realizada a investigação e esgotando as diligências investigatórias a realizar, importa dar destino ao inquérito, cabendo ao Ministério Público o acto decisório de submeter ou não a causa a julgamento.

As possibilidades de desfecho são as comuns, com algumas especificidades:

a. Arquivamento (artigo 277.º, n.ºs 1 e 2, do Código de Processo Penal)

b. Suspensão provisória do processo (artigo 281.º do Código de Processo Penal)

c. Requerimento para aplicação de pena em processo sumaríssimo (artigo 392.º do Código de Processo Penal)

d. Acusação (artigo 283.º do Código de Processo Penal)

No que se refere ao **arquivamento do processo**, é de ressaltar desde logo que se encontra excluída a possibilidade de arquivamento com dispensa de pena, previsto no artigo 280.º, porquanto não se encontra expressamente prevista na lei penal essa possibilidade.

Por outro lado, importa não descurar a possibilidade, a que *supra* de se referência, de extinção da responsabilidade do procedimento por força do disposto no artigo 206.º, n.º 1, aplicável *ex vi* do artigo 221.º, n.º 6. Neste caso, o inquérito deverá ser arquivado nos termos do artigo 277.º, n.º 1, do Código de Processo Penal, por inadmissibilidade do procedimento criminal.

Debruçando-nos agora sobre a **suspensão provisória do processo**, convocamos a orientação hierárquica expressa na Directiva da Procuradoria-Geral da República n.º 1/2014 nos termos da qual "Os Magistrados do Ministério Público devem optar, no tratamento da pequena e média criminalidade, pelas soluções de consenso previstas na lei, entre as quais assume particular relevo a suspensão provisória do processo", convocando todas as orientações nela contidas. Assim, quando estejam verificados os pressupostos previstos no artigo 281.º, n.º 1, do Código de Processo Penal, o Ministério Público deverá sempre privilegiar a sua aplicação.

Cumprirá uma nota apenas para ressalvar que no caso que nos ocupa a aplicação desde instituto encontra-se liminarmente excluída nos casos que integrem a previsão normativa prevista no artigo 221.º, n.º 5, alínea b), com referência aos n.ºs 1 e 2, porquanto a pena de prisão aplicável excede os 5 anos.

Mostrando-se inviável a aplicação da suspensão provisória do processo, deverá então o Ministério Público lançar mão do **Processo Sumaríssimo** cuja utilização é igualmente

incentivada na Directiva da Procuradoria-Geral da República 1/2016, dando curso "ao imperativo constitucional de participação e execução da polícia criminal definida por órgão de soberania, privilegiando soluções de consenso no tratamento de casos da pequena e média criminalidade.

Neste particular, valem igualmente os considerandos tecidos a propósito da inaplicabilidade da suspensão provisória do processo aos casos abrangidos no artigo 221.º, n.º 5, alínea b), com referência aos n.ºs 1 e 2, na medida em que o máximo da moldura penal excede os 5 anos.

A terminar, e não havendo lugar ao arquivamento dos autos ou à aplicação da suspensão provisória do processo nem ainda à utilização do processo sumaríssimo, o Ministério Público deduzirá **acusação**, sendo que a competência do Tribunal será definida nos termos gerais.

IV. Hiperligações e referências bibliográficas

Hiperligações

Relatório Anual de Segurança Interna, disponível para consulta em http://www.ansr.pt/InstrumentosDeGestao/Documents/Relat%C3%B3rio%20Anual%20de%20Seguran%C3%A7a%20Interna%20(RASI)/RASI%202016.pdf.

Referências bibliográficas

ALBUQUERQUE, Paulo Pinto, *Comentário do Código Penal à luz da Constituição da República Portuguesa e da Convenção Europeia dos Direitos do Homem*, 3.ª edição actualizada, Universidade Católica Editora, Novembro, 2015.

ALFREDO, José Atanásio, *Algumas questões referentes ao tipo legal da burla*, Universidade Lusófona do Porto, Faculdade de Direito, 2013.

AZEVEDO, Ana Helena França, *Burlas Informáticas: Modos de Manifestação*, Tese de Mestrado em Direito e Informática, Universidade do Minho, Janeiro, 2016.

CORREIA, Pedro Miguel Alves Ribeiro e JESUS, Inês de Oliveira Andrade de, "Combate às transferências bancárias ilegítimas pela Internet no direito português: entre as experiências domésticas e políticas globais concertadas", *in* Revista Direito GV, São Paulo, V. 12, N.º 12, Maio-Agosto, 2016, pp. 543-563.

COSTA, A. M. Almeida, *Comentário Conimbricense do Código Penal*, Tomo II, Coimbra Editora, 1999.

COSTA, José de Faria e MONIZ, Helena, "Algumas reflexões sobre a criminalidade informática em Portugal", *in Boletim da Faculdade de Direito da Universidade de Coimbra*, Vol. LXXIII, 1997.

DÁ MESQUITA, Paulo, "Processo Penal, Prova e Sistema Judiciário", Wolters Kluwer, Coimbra Editora, 2010.

DANTAS, Leonel, "A Revisão do Código Penal e os Crimes Patrimoniais", *in* Jornadas de Direito Criminal do Centro de Estudos Judiciários, Lisboa, 1998.

DIAS, Jorge de Figueiredo, *Direito Penal – Parte Geral – Tomo I – Questões Fundamentais; A Doutrina Geral do Crime*, 2.ª edição, Coimbra Editora, 2011.

MACEDO, João Carlos Barbosa, "Algumas considerações acerca dos crimes informáticos em Portugal", *in* Direito Penal Hoje – Novos desafios e novas respostas, Coimbra Editora, 2009.

MEIRELES, Mário Pedro, "A responsabilidade penal das pessoas colectivas ou entidades equiparadas na recente alteração ao Código Penal ditada pela lei 59/2007, de 4 de Setembro: algumas notas", *in* Julgar Online, N.º 5, Maio, 2008 [retirado de : http://julgar.pt/responsabilidade-penal-das-pessoas-colectivas/].

NUNES, Duarte Alberto Rodrigues, "O crime de falsidade informática", *in* Julgar Online, Outubro, 2017 [retirado de http://julgar.pt/o-crime-de-falsidade-informatica/].

ROCHA, Manuel António Lopes, "A Revisão do Código Penal, Soluções de Neocriminalização", *in* Jornadas de Direito Criminal, Centro de Estudos Judiciários, Vol. I, Lisboa, 1996.

SANTOS, Rita Coelho, *O Tratamento Jurídico-Penal da Transferência de Fundos Monetários Através da Manipulação Ilícita dos Sistemas Informáticos*, *Studia* Jurídica, n.º 82, Coimbra Editora, 2005.

TEIXEIRA, Paulo Alexandre Gonçalves, *O fenómeno do Phising, Enquadramento Jurídico-Penal*, Dissertação de Mestrado, Lisboa, 2013.

VERDELHO, Pedro, "Cibercrime", *in* Direito da Sociedade da Informação, Vol. IV, Associação Portuguesa do Direito Intelectual, Coimbra Editora.

CENTRO
DE ESTUDOS
JUDICIÁRIOS

3.
Crime de burla informática e nas comunicações. Enquadramento jurídico, prática e gestão processual

Dália Sotero Palma

CENTRO
DE ESTUDOS
JUDICIÁRIOS

3. CRIME DE BURLA INFORMÁTICA E NAS COMUNICAÇÕES. ENQUADRAMENTO JURÍDICO, PRÁTICA E GESTÃO PROCESSUAL

Dália Sotero Palma

I. Introdução

O uso generalizado das tecnologias de informação e comunicação potenciou uma transformação manifesta na sociedade actual, com a criação e desenvolvimento de um mundo virtual, paralelo ao físico já existente, no qual as pessoas são representadas, além do mais, por "dados informáticos" e informações inseridas numa estrutura virtual e tecnológica, com novas oportunidades de comunicação, interacção e disponibilidade.

Assim, o ciberespaço depressa se assumiu como um ambiente de acção e meio de actuação privilegiado para o cometimento de ilícitos, incluindo novas modalidades delituosas, porquanto a sua especialidade e complexidade não só escapa ao entendimento da maioria dos utilizadores, como dificulta em muito a sua investigação e a identificação dos respectivos agentes.

Este "novo mundo" não poderia ficar arredado do Direito e sem qualquer regulamentação e, nesse contexto, a Lei n.º 109/91, de 17 de Agosto – apelidada de Lei do Cibercrime – acolheu os principais ilícitos informáticos.

Foi neste contexto que surgiu, entre outros, o crime de burla informática, introduzido na lei penal portuguesa com a Reforma de 1995, operada pelo Decreto-Lei n.º 48/95, de 15 de Março, na esteira da incriminação já existente na Alemanha e Áustria, com correspondência na *Computerbetrug* (burla de computadores) do §263a do StGB germânico[1].

Partindo do *nomen iuris* «burla informática» à partida estaríamos no âmbito dessa lei, contudo, foi opção do legislador incluir o crime de burla informática no Código Penal.

A Reforma de 1995 teve em vista dotar a ordem jurídica portuguesa de mecanismos de resposta face à «…*revelação de novos bens jurídico-penais ou de novas modalidades de agressão ou perigo …*» (cfr. preâmbulo do Decreto-Lei n.º 48/95, de 15 de Março). Posteriormente, através da Reforma do Código Penal de 1998, operada pela Lei n.º 65/98, de 02 de Setembro, surgiu a incriminação da burla nas telecomunicações, acrescentando-se o n.º 2, ao artigo 221.º, do Código Penal.

A pertinência do tema abordado neste Guia prende-se com o aumento exponencial[2] do número de crimes praticados com recurso às tecnologias de informação, além de que a globalização permanente das redes informáticas[3] e a crescente transnacionalização de fenómenos criminais não fizeram surgir unicamente novas formas de criminalidade, mas novas formas de recolha de prova.

II. Objectivos

O presente Guia visa proporcionar aos Auditores de Justiça, bem como aos Magistrados do Ministério Público, uma breve abordagem teórica do crime de burla informática e nas comunicações, incluindo algumas incursões nos crimes conexos e na jurisprudência, bem como uma abordagem prática quanto à sua investigação, incluindo os métodos e recolha de prova, tentando antecipar algumas questões e dificuldades que poderão verificar-se no decurso do inquérito, em face da especialidade técnica que este crime reveste.

[1] *In* ROCHA, Manuel António Lopes, *A Revisão do Código Penal Soluções de Neocriminalização, Jornadas de Direito Criminal,* Conferências proferidas na Aula Magna da Reitoria da Universidade de Lisboa, em 3 e 4 de Julho de 1995, Lisboa 1996, página 92.

[2] De acordo com os dados recolhidos junto do Relatório Anual de Segurança Interna, concretamente dos anos de 2014 a 2017 verifica-se um acréscimo bastante significativo de cometimento de burlas informáticas e nas telecomunicações, ao longo dos últimos anos. No ano de 2014, a burla informática e nas comunicações apresentou um aumento de 30.4%, em relação ao ano anterior. No ano de 2015 voltou a verificar-se a tendência crescente, com um aumento correspondente a 73,7 %. No ano de 2016 o aumento foi correspondente a 7,9%.

[3] Segundo os dados da Consultora Marktest, em Portugal existem actualmente 5,9 milhões de utilizadores de *internet*. Se a estes números acrescentarmos o número de utilizadores mundiais, que em 2016, de acordo com os dados publicados no sítio *Statista* (www.statista.com/stas/internetacess) se calculava ascender a 2,34 mil milhões utilizadores activos, estima-se que no mundo haja 7,5 mil milhões de pessoas. Em 2020, as previsões apontam para os 2,95 mil milhões de utilizadores.

III. Resumo

O presente Guia aborda o crime de burla informática e nas comunicações, previsto e punido pelo artigo 221.º do Código Penal, de duas perspectivas distintas, uma teórica e outra prática.
A primeira encontra-se direccionada à análise das principais características do crime de burla informática e nas comunicações, desde o enquadramento jurídico, passando pela análise da acção típica nas vertentes prescritas no n.º 1 e no n.º 2, tratamento dos elementos subjectivos do tipo, reflexões sobre pontos de contacto entre a norma do Código Penal e as demais normas incriminadoras constantes da legislação destinada a regular os crimes cometidos por meios informáticos – a Lei do Cibercrime.

A segunda, já com uma vertente mais prática, aborda a investigação, com vista à gestão eficiente do inquérito – enquanto fase processual por excelência dirigida ao apuramento da existência de crime – da identidade dos seus agentes e de recolha de provas, com vista à decisão final.

A fim de potenciar a pretendida abordagem prática, incluiremos uma breve apreciação dos elementos pertinentes a contemplar nos despachos a proferir pelo Magistrado do Ministério Público, delimitação da estratégia de investigação e instrumentos hierárquicos a ter em consideração.

1. Enquadramento jurídico

1.1. O Bem Jurídico Protegido e Natureza do Crime

O crime de burla informática e nas comunicações, previsto e punido pelo artigo 221.º do Código Penal, vem inserido sistematicamente no *«Capítulo III, Dos crimes contra o património em geral», do «Título II – Dos Crimes Contra o Património»*, razão pela qual tem vindo a ser entendido pela doutrina que o **bem protegido é** essencialmente **o património**[4]. Todavia, cumpre relevar que o Supremo Tribunal de Justiça passou a seguir a orientação de que neste crime o bem jurídico não é só o património protegido pela previsão legal (concretamente, a integridade patrimonial) como, ainda, no caso previsto no n.º 1 do referido preceito «… *a fiabilidade dos programas informáticos, o respectivo processamento e os dados*»[5].

Por sua vez, no crime previsto no n.º 2 do artigo 221.º do Código Penal, o bem jurídico protegido pela incriminação não só engloba o património, como também o normal funcionamento ou exploração de serviços de comunicações[6].

[4] MONIZ, Helena, FARIA COSTA, José de, *Algumas reflexões sobre a criminalidade informática em Portugal*, *in* BFDUC, Vol. LXXIII, 1997, págs. 323-324, e COSTA, Almeida, *in Comentário Conimbricense do Código Penal*, Tomo II, 1999, págs. 328 e ss.
[5] *In* Acórdão do Supremo Tribunal de Justiça, de 06.10.2005, proferido no proc. n.º 05P2253, Relator Simas Santos; no mesmo sentido, os Acórdão do Tribunal de Guimarães e de Évora, respectivamente proferido em 18.12.2012 no proc. n.º 541/10.GAPTB.G1, Relator Ana Teixeira e proferido em 20.01.2015, no proc. n.º 90/11.0GCLLE.E1, Relator João Amaro, todos acessíveis em www.dgsi.pt .
[6] VERDELHO, Pedro, *in Comentário das Leis Penais Extravagantes,* volume 1, 1.ª Edição, Universidade Católica Editora, Novembro de 2010, pág. 511, ponto 8.

Efectivamente, não obstante a sua localização, normas existem que protegem bens jurídicos diversos daqueles que identificam a sua concreta integração no Código Penal, podendo um só tipo legal proteger mais do que um bem jurídico.

É igualmente um **crime de dano**, pois, tal como resulta da norma incriminadora, a sua consumação verifica-se com a ocorrência de um prejuízo patrimonial de outrem, seja de diminuição do património, seja através do aumento do passivo.

O crime de burla informática e nas comunicações constitui ainda um **crime material ou de resultado** – embora de resultado parcial ou cortado[7]– por oposição aos crimes de mera actividade ou formais – porquanto a sua consumação depende da verificação de um evento, espácio-temporalmente destacado da acção, e que consiste na saída dos bens ou valores da esfera da disponibilidade fáctica da vítima.

Por conseguinte, as vítimas deste crime são aquelas que sofrem e suportam o prejuízo patrimonial, podendo coincidir, ou não, com a entidade titular do sistema informático.

Do ponto de vista da conduta, a lesão do património tem de suceder como consequência dos comportamentos típicos definidos pelo legislador, motivo pelo qual constitui um **crime de execução vinculada**[8], à semelhança do crime de burla, previsto e punido pelo artigo 217.º, n.º 1, do Código Penal, deste, todavia, distinguindo-se, desde logo, pela exigência de que a lesão do património da outra pessoa seja produzida pela utilização de meios informáticos [9].

O ilícito em análise exige, no plano da tipicidade, que a lesão do património se produza através da intromissão nos sistemas e da utilização em certos termos de meios informáticos, não obstante a cláusula geral quanto ao modo de comissão, como de seguida melhor se desenvolverá.

O artigo 221.º, do Código Penal contempla duas figuras tipo de delito, a burla informática, a que se refere o n.º 1 do referido preceito legal e a burla nas comunicações, a que se refere o n.º 2.

1.2. As Modalidades da Conduta Típica do n.º 1

A redacção da norma incriminadora reflecte para uma dimensão muito técnica, por isso tem vindo a ser densificada de forma distinta pela doutrina e jurisprudência.

[7] Cfr. Acórdão do Supremo Tribunal de Justiça, proc. n.º 08p2817, de 05.11.2008, ambos do Relator Henriques Gaspar, acessíveis em www.dgsi.pt.
[8] Cfr. Acórdão do Supremo Tribunal de Justiça, de 20.09.2006, proferido no âmbito do proc. n.º 06P1942, proc. n.º 08p2817, de 05.11.2008, ambos do Relator Henriques Gaspar, acessíveis em www.dgsi.pt.
[9] VERDELHO, Pedro, *Op. cit.*.

Para alguns autores[10], a burla informática constitui um desenvolvimento do crime de burla, partilhando os mesmos elementos integradores do tipo, unicamente se diferenciando pela especificidade do meio ou processo utilizado – utilização de meios informáticos. Por isso, para os seguidores deste entendimento, a burla informática, na construção típica e na correspondente execução vinculada, há-de consistir sempre num comportamento que constitua um artifício, engano ou erro consciente, não por modo de afectação directa em relação a uma pessoa (como na burla – artigo 217.º do Código Penal), mas por intermediação da manipulação de um sistema de dados ou de tratamento informático, ou de equivalente utilização abusiva de dados, que remeterá necessariamente para a dimensão típica da burla a que diz respeito o artigo 217.º, n.º 1, do Código Penal.

A outra posição seguida pela doutrina[11], e com a qual concordamos, vai no sentido de que a norma incriminadora não individualiza qualquer elemento do tipo de indução de alguém em erro e na prática por este, como consequência da vontade viciada de que foi alvo, de actos lesivos do seu património ou de património alheio, logo, são normas distintas da burla prevista no artigo 217.º, n.º 1, do Código Penal, não partilhando com esta os mesmos elementos típicos.

Mais acresce que, se a norma em apreço individualizasse tais elementos (erro e um acto praticado pela vítima em função desse erro) «*…os **out puts,** produto da manipulação dos dados levada a cabo pelo agente, assumiriam aqui o papel do artifício fraudulento na estrutura do tipo base de burla. Desse modo, nada autonomizaria o crime de burla informática relativamente ao crime base de burla*[12].

Assim, o artigo 221.º do Código Penal não se dirige à manipulação de vontade de uma pessoa – não contemplando, assim, o duplo nexo de imputação causal referido no artigo 217.º do Código Penal, tal como as condutas relevantes são as que se encontram previstas nas modalidades típicas previstas no artigo 221.º, do Código Penal.

Por estes motivos, julgamos que os artigos 217.º e 221.º, ambos do Código Penal, existem numa relação de alternatividade ou exclusividade típica[13] [14].

Quanto aos elementos que integram a acção típica, cumpre agora apurar o significado da sua previsão.

[10] VENÂNCIO, Pedro Dias, *Breve Introdução da Questão da Investigação e Meios de Prova na Criminalidade Informática*, Verbo Jurídico, Dezembro de 2006, pág. 11; ASCENSÃO, José de Oliveira, *Estudos sobre o Direito da Internet e da Sociedade de Informação*, Almedina, Abril de 2001, págs. 216 e 217; no mesmo sentido o já citado Acórdão proferido no proc. n.º 06P1942, Relator Henriques Gaspar.
[11] SANTOS, Manuel Simas, LEAL-HENRIQUES, Manuel, Código Penal Anotado, Volume III, 4.ª Edição, Reis dos Livros, pág. 1007.
[12] ROCHA, Manuel António Lopes, *Op. cit.*.
[13] *Idem*.
[14] Neste sentido, Acórdão do Tribunal da Relação de Coimbra, de 15.05.2002, proferido no proc. n.º 1318/02, Relator Barreto do Carmo e Acórdão do Tribunal da Relação do Porto, proferido no proc. n.º 482/10.2SJPRT.P1, de 03.02.2016, Relatora Eduarda Lobo, ambos acessíveis em www.dgsi.pt.

O tipo de ilícito objectivo do crime a que se refere o n.º 1 do artigo 221.º do Código Penal, o prejuízo patrimonial deverá ser realizado através da utilização de meios informáticos e *consiste na interferência* no resultado de tratamento de dados, a qual poderá suceder através de «*estruturação incorrecta de programa informático*», ou «*utilização incorrecta ou incompleta de dados*», ou «*utilização de dados sem autorização*» ou «*intervenção por qualquer outro modo não autorizado no processamento*».

Antes de mais, e referindo-se o preceito legal a «dados» bem como a «programa informático», cumpre compreender a sua definição, em ordem a conhecer a extensão do conceito que constitui o elemento típico da norma.

Julgamos que, quando a norma incriminadora se refere a «dados», inclui na sua acepção tanto os dados pessoais – cuja definição se encontra na Lei n.º 67/98, de 26 de Outubro (Lei da protecção de dados pessoais) – como dados informáticos – cuja definição consta do artigo 2.º, alínea b), da Lei n.º 109/2009, de 15 de Setembro, a Lei do Cibercrime.

Por outro lado, a definição de programa informático não consta da Lei n.º 109/2009, de 15 de Setembro, mas constava anteriormente no artigo 2.º, alínea e), da Lei n.º 109/91, de 7 de Agosto (que entretanto veio a ser revogada pela Lei n.º 109/2009, de 15 de Setembro), à qual podemos recorrer.

A formulação prevista na norma incriminadora apresenta-se em termos alternativos, bastando a verificação de uma das modalidades de comissão previstas para se verificar o crime, em que o dano/prejuízo assume-se como a consequência da interferência do agente. Isto significa que a interferência no resultado de tratamento de dados é a consequência necessária dos modos de execução do crime descritos na norma e previstos em alternativa, e não uma das formas de comissão do crime.

Como salienta Manuel António Lopes Rocha[15], assistimos a uma **estruturação incorrecta** quando o programa informático é modificado a fim de contemplar instruções diferentes das inicialmente concebidas pelo seu proprietário, o que poderá suceder quando se introduzem novas instruções ou novas funções no programa, se elimina ou altera o processo de funcionamento, modificando os sistemas de controlo do programa. A estruturação pode ter lugar igualmente ou pela manipulação de um programa já existente, ou pela criação de um novo programa que não produz resultados falsos, por exemplo, através da manipulação do *browser*[16].

Por seu turno, a **utilização incorrecta** de dados «*consiste na introdução de dados que não correspondem à realidade, como por exemplo na introdução de dados de pessoas que não*

[15] ROCHA, Manuel António Lopes, *A Revisão do Código Penal Soluções de Neocriminalização, Jornadas de Direito Criminal,* Conferências proferidas na Aula Magna da Reitoria da Universidade de Lisboa, em 3 e 4 de Julho de 1995, Lisboa 1996, pág. 95.
[16] *In* ALBUQUERQUE, Paulo Pinto de, *in Comentário do Código Penal à luz da Constituição da República Portuguesa e da Convenção Europeia dos Direitos do Homem*, 3.ª Edição actualizada, Universidade Católica Editora, Novembro de 2015, pág. 860, ponto 8.

existem», referindo-se primordialmente à fase de entrada de dados no computador[17], ao passo que «*a **utilização incompleta** de dados consiste na introdução parcial de dados verdadeiros, de tal modo que eles não representam a realidade. Esses dados podem encontrar-se no interior dos sistemas informáticos ou em suportes digitais móveis, como disquetes, CD-ROM, cartões magnéticos ou electrónicos*».[18]

Quanto à **utilização de dados sem autorização**, tem esta vindo a ser descrita como a utilização de dados alheios com vista a obtenção de uma vantagem patrimonial e «*…implica a violação de regras de acesso aos dados, sem que a integridade desses dados seja afectada. O exemplo típico consiste na utilização de um cartão de débito e respectivo código em caixas automáticas por pessoa não autorizada pelo titular, com intenção de obter um enriquecimento ilegítimo».*[19] Todavia, não integra a conduta típica a utilização do cartão por terceiro autorizado pelo titular em violação das regras contratuais de cedência a terceiros (com base na cláusula de tais cartões serem, por via da regra, pessoais e intransmissíveis).

A maioria da jurisprudência dos Tribunais das Relações tem vindo a considerar que incorre na prática de crime de burla informática quem, sem autorização do seu legítimo titular, se apoderar ilicitamente dos cartões bancários e respectivo código de acesso para obtenção de quantia em dinheiro, na modalidade de «*utilização de dados sem autorização*».[20] Cumpre relevar que foi justamente para combater a frequência das utilizações abusivas de caixas automáticas, entre outras condutas que mereciam igualmente regulação, que foi criado este novo tipo de crime, além de que também o § 263.ºa do Código Penal Alemão – que esteve na origem do artigo 221.º do Código Penal – teve em vista igualmente combater a utilização abusiva de ATMs.

Quanto à utilização de cartão bancário, de débito ou crédito, Paulo Pinto de Albuquerque defende que a «*utilização de cartão de débito ou de crédito para pagamento não autorizado num terminal POS ou o carregamento não autorizado de cartão de moeda electrónica (smart card, pay before card) com o PIN de outrem*» integra a conduta típica prevista no artigo 221.º do Código Penal[21].

Não é, porém, esta a posição seguida por Pedro Verdelho, o qual afirma que é necessário saber se o PIN é ou não abrangido pelo conceito de dados informáticos, pois a definição ainda não se encontra descrita na lei portuguesa. Nessa sequência, o referido autor postula que o código PIN não se inclui no conceito de dados informáticos e, assim, não preenche os elementos tipo do crime de burla informática[22].

[17] SANTOS, Manuel Simas, LEAL-HENRIQUES, Manuel, *Op. cit.*, pág. 1011.
[18] *In* ALBUQUERQUE, Paulo Pinto de, *Op. cit*., pág. 860, ponto 8.
[19] *In* ALBUQUERQUE, Paulo Pinto de, *Op. cit*., pág. 860, ponto 10.
[20] Na nota prática n.º 11/2017, de 02.11.2017 – Jurisprudência sobre Cibercrime, vem enumerada uma lista de Acórdãos, e respectivos resumos, que consideraram a utilização de cartões bancários sem autorização como crime de burla informática, acessível em cibercrime.ministeriopublico.pt.
[21] ALBUQUERQUE, Paulo Pinto de, *Op. cit.*, pág. 861, ponto 10.
[22] AZEVEDO, Ana Helena França*, Burlas Informáticas: Modos de Manifestação*, Tese de Mestrado em Direito e Informática, Universidade do Minho, Janeiro de 2016, pág. 39.

Contudo, independentemente da classificação atribuída ao PIN, julgamos que a sua utilização por pessoa não autorizada em caixa automática sempre preencherá o tipo de «utilização de dados sem autorização».

Por fim, a **intervenção por qualquer modo não autorizado no processamento** de dados abrange a interferência no processo mecânico do sistema informático, desde a manipulação de *hardware,* que se poderá materializar na interferência sobre as instruções de processamento de dados ou na alteração do processo mecânico do programa informático, incluindo a possibilidade de accionar uma caixa automática através de um programa de computador obtido de forma ilegal[23]. Esta modalidade de comissão, no entendimento de Manuel António Lopes Rocha[24], apresenta-se como uma formulação propositadamente ampla a fim de abranger outras situações não subsumíveis às modalidades previstas ou de duvidosa subsunção, para evitar possíveis lacunas legais.

Em face do que ficou exposto, resulta que o enquadramento do tipo remete, especificamente, para um prejuízo patrimonial causado pela interferência e a intromissão ilegítimas, abusivas ou intencionalmente incorrectas em dados e/ou programas informáticos, com a intenção de obter um enriquecimento ilegítimo.

Existirá necessariamente uma relação de causalidade, sendo que a manipulação informática terá de ser causa adequada na interferência no resultado de tratamento de dados e esta interferência terá de ser causa do prejuízo patrimonial.

Não obstante a burla clássica poder vir a ser praticada através de meios informáticos, configurando o instrumento informático o meio engenhoso para enganar ou induzir em erro, do qual irá resultar um prejuízo patrimonial, tal não sucederá no âmbito da burla informática, pois aqui o prejuízo patrimonial decorre directamente de uma operação informática, totalmente automatizada.

1.3. As Modalidades da Conduta Típica do n.º 2

Analisando as condutas típicas previstas no n.º 2 do artigo 221.º do Código Penal e decompondo a norma resulta que a acção típica consubstancia, igualmente, na lesão patrimonial, desta feita através de uso *«de programa, dispositivos electrónicos ou outros meios»;* destinados «*a diminuir, alterar ou impedir, total ou parcialmente, o normal funcionamento ou exploração de serviços de telecomunicações».*

Para a verificação da previsão do n.º 2 do artigo 221.º, do Código Penal exige-se que a utilização de programa ou dispositivos tenha a virtualidade de diminuir, alterar ou impedir o

[23] AZEVEDO, Ana Helena França*, Burlas Informáticas: Modos de Manifestação*, Tese de Mestrado em Direito e Informática, Universidade do Minho, Janeiro de 2016, pág. 41.
[24] ROCHA, Manuel António Lopes, *op. cit.*, pág. 95.

normal funcionamento das telecomunicações, pois caso tal modificação não se verifique, não se encontra preenchida a tipicidade prevista na norma[25].

A modificação verificada poderá ocorrer através da manipulação de *hardware* ou das estruturas físicas das telecomunicações, incluindo a interferência em linha telefónica para a realização de chamadas, podendo ser lesado pela conduta tanto o operador de telecomunicações como o próprio utilizador de um serviço, dependendo da forma de interferência praticada pelo agente se reflicta na esfera de um ou de outro.

Para melhor configurar a conduta típica, vejamos alguns exemplos retirados da jurisprudência:

I. Sinal televisivo – ligação não autorizada à infra-estruturas de rede para usufruto de serviços de televisão: considerou-se que a ligação não autorizada à rede da TvCabo não diminuiu, alterou ou impediu que o serviço se desenvolvesse com normalidade, pelo que, consequentemente, não integra a factualidade típica do artigo 221.º, n.º 2, do Código Penal [26];

II. Entrada no tráfego da operadora telefónica – o agente desviava o tráfego (sobretudo internacional) das chamadas destinadas aos clientes da operadora móvel para equipamentos localizados em Portugal, localizados na sociedade da qual era administrador. Posteriormente entregava esse tráfego aos destinatários através de chamada telefónica por si realizada, transformando o tráfego fixo-móvel e internacional em tráfego que para a operadora aparecia como tráfego móvel-móvel, ficando, desta forma, a operadora impedida de receber a respectiva contrapartida[27], pelo que se considerou burla nas comunicações;

III. Alteração ilícita das terminações de chamadas internacionais – "fraude de interligação" – na alteração ilícita das terminações de chamadas internacionais efectuadas através de cartões de acesso ao serviço telefónico móvel, de forma a que tais chamadas fossem consideradas pela operadora chamadas "intra-rede" e, por essa via, a empresa não lhes possa aplicar as tarifas destinadas ao tráfego internacional, deixando de auferir os correspondentes proventos[28].

Do que fica exposto, afigura-se necessária a diminuição, alteração ou impedimento normal do funcionamento.

[25] Neste sentido, pronunciou-se o Tribunal da Relação de Lisboa, por Acórdão de 22.03.2011, no âmbito do proc. n.º 4252/07.7TDLSB.L1-5, Relator Carlos Espírito Santo, acessível em www.dgsi.pt.
[26] Acórdão do Tribunal da Relação de Lisboa, de 22.03.2011, proc. n.º 4252/07.7TDLSB.L1-5.
[27] Acórdão do Tribunal da Relação de Lisboa, de 24.01.2007, proc. n.º 5990/2006-3.
[28] Acórdão do Tribunal da Relação de Évora, de 06.01.2015, proc. n.º 6793/11.2TDLSB-A.E1. Apesar de no Acórdão se enquadrar a situação no artigo 221.º, n.º 1, do Código Penal, consideramos que fará mais sentido o enquadramento no artigo 221.º, n.º 2, do mesmo diploma legal, apesar de não ignorarmos tratar-se de um recurso de um despacho que indeferiu a pretensão do Ministério Público em sede de inquérito, pelo que a factualidade não se encontra ainda bem especificada.

1.4. O Tipo Subjectivo

De acordo com as disposições conjugadas dos artigos 13.º e 221.º do Código Penal, a burla informática e nas comunicações é um **crime doloso**, admitindo qualquer modalidade de dolo[29], nos termos previstos no artigo 14.º do Código Penal, não admitindo, contudo, a punição a título de negligência.

Considerando a imprevisibilidade das consequências da manipulação informática, nem sempre é possível ao agente prever e controlar o resultado da sua conduta, pelo que deverá considerar-se a possibilidade de imputar a conduta ao agente a título de dolo eventual.

Ora, o dolo enquanto elemento do tipo, pressupõe um elemento cognitivo – o qual inclui o conhecimento dos elementos descritivos do tipo e que permite ao agente a tomada de uma decisão ou pela preservação do bem jurídico, ou pela não preservação – e um elemento volitivo – o agente tem de querer a realização típica.

Contudo, no ilícito criminal em apreço, a actuação dolosa do agente vai além do conhecimento dos factos e a vontade de os realizar, pois o artigo 221.º, na formulação do n.º 1 e do n.º 2, do Código Penal, exige um elemento subjectivo adicional: a necessidade de o agente ser movido por um propósito, actuando com: a «… *intenção de obter, para si ou para terceiro, um enriquecimento ilegítimo*», tal como se prescreve no n.º 1, do artigo 221.º, do Código Penal, e ainda a « …*intenção de obter para si ou para terceiro um benefício ilegítimo*», a que se refere o n.º 2 do mesmo preceito legal.

Assim, o dolo exigido pelas duas normas em apreço deve igualmente ter em consideração o dolo intencional referente ao intuito de obtenção de enriquecimento ou benefício ilegítimo, porquanto «*O dolo específico, quando existe no tipo, **é um elemento subjectivo que acresce ao dolo que também tem de existir no tipo de ilícito**.*[30]

Como critério diferenciador do crime de burla informática (n.º 1 do artigo 221.º do Código Penal) e do crime de burla nas telecomunicações (n.º 2 do artigo 221.º, do Código Penal), tem sido apontado por Pedro Verdelho[31] o critério patrimonial, isto porque, tendo em conta a redacção do tipo subjectivo, a burla informática prevê um enriquecimento ilegítimo do agente, pelo que da actuação criminosa advirá uma vantagem patrimonial, ao passo que na burla nas comunicações se prevê um benefício ilegítimo, já no sentido que da actuação resultará uma "isenção" em suportar o respectivo custo.

Esta distinção não se afigura despicienda, porquanto o benefício não corresponde, nem poderá ser considerado enriquecimento e não poderá considerar-se existir enriquecimento através do valor do custo da comunicação.

[29] ALBUQUERQUE, Paulo Pinto de, Op. cit., pág. 861, ponto 15.
[30] *In* Acórdão do Tribunal da Relação de Lisboa, de 29.09.2009, proferido no proc. n.º 3792/04.4TALRS.L1-5, Relator Pedro Martins, acessível em www.dgsi.pt) (itálico, destaque e sublinhado nossos.
[31] VERDELHO, Pedro, *Op. cit.*, pág. 512, ponto 8.

Daqui decorre que não basta a produção de um dano patrimonial na esfera da vítima, sendo ainda necessário o intuito de obtenção de um enriquecimento ilegítimo, o *animus lucrandi* [32] *ou* obtenção de um benefício ilegítimo*,* o *animus beneficiendi.*

Como salienta Paulo Pinto de Albuquerque, uma vez que o dolo intencional, correspondente ao enriquecimento e benefício ilegítimos, constitui elemento do tipo subjectivo este não é comunicável no caso de comparticipação, tendo os mesmos de se verificar na esfera do comparticipante ou, no caso de cumplicidade, o cúmplice deverá ter conhecimento do *animus lucrandi ou animus beneficiendi* do autor[33].

De relevar que, não obstante a norma incriminadora prescrever a intenção de enriquecimento e benefício ilegítimos, ela não exige a verificação de um efectivo enriquecimento ou benefício para a consumação do crime, pelo que este se considera verificado no momento em que ocorre o prejuízo patrimonial e não quando se interfere nos dados ou programa informático ou uso de programas e dispositivos.

Em jeito de conclusão, haverá burla informática (n.º 1) quando existe uma interferência – especificamente prevista – no *sofware*, ao passo que existirá burla nas comunicações quando, além dessa interferência, existe uma manipulação de *hardware* ou outras estruturas físicas de telecomunicações que não caibam na definição deste último conceito.

1.5. As Formas Especiais do Crime

1.5.1. Tentativa

Em face da disposição vertida no n.º 3 do artigo 221.º do Código Penal é admissível a burla informática e nas comunicações na forma tentada, pelo que terão integral aplicação as normas constantes do artigo 22.º e 23.º do Código Penal.

1.5.2. Responsabilidade Penal dos Entes Colectivos

Pela prática de burla informática e nas comunicações haverá lugar à responsabilização penal da pessoa colectiva na medida em que o agente o seja também, exigindo-se o nexo de imputação do facto a um agente da pessoa colectiva, que será aquele que nela exerça liderança ou um seu subordinado, tal como prescreve o artigo 11.º do Código Penal.

1.5.3. Omissão

Como já abordado *supra*, o crime de burla informática e nas comunicações é um crime de execução vinculada, pelo que poderia ser de rejeitar, à partida, a sua realização por omissão por se revelar necessário interferir e provocar factos que provoquem uma lesão patrimonial.

[32] COSTA, Almeida, *in Comentário Conimbricense do Código Penal*, Tomo II, 1999, pág. 331.
[33] ALBUQUERQUE, Paulo Pinto de, *Op. cit*., pág. 861, ponto 15.

Da mesma forma, o crime de burla previsto no artigo 217.º, n.º 1, do Código Penal é, também ele, um crime de execução vinculada, porquanto prevê igualmente uma forma especial de execução e contudo, a jurisprudência tem vindo a admitir a possibilidade de ser cometido por omissão, nos casos em que o agente, com o seu silêncio e sem praticar qualquer acto positivo, contribui para a manutenção do engenho fraudulento e enganador da vítima[34].

Nesta esteira, e perfilhando o entendimento de Rita Coelho Santos[35], cremos que é possível equacionar que o tipo previsto no artigo 221.º do Código Penal contempla tanto a acção, como a omissão, quando impender um dever de garante sobre o comitente, o qual deverá ser pessoal, nos termos previstos no artigo 10.º, n.º 2, do Código Penal, existindo uma omissão relevante quando ao agente seja exigível ou imposto o ónus de evitar um resultado concreto.

1.6. A Problemática do Concurso de Crimes

A relação estabelecida entre a natureza do bem jurídico protegido e a especificidade típica supõe que a produção do resultado derive de acções do agente. Pode, contudo, suceder que as acções do agente, no plano da unidade ou pluralidade de infracções, incluam elementos de outras infracções típicas.

Esta questão é apreciada pelo artigo 30.º do Código Penal, o qual enforma um princípio geral de solução: o número de crimes determina-se pelo número de tipos de crime efectivamente cometidos, ou pelo número de vezes que o mesmo tipo de crime for preenchido pela conduta do agente, sendo o critério determinante o que resulta da consideração dos tipos legais efectivamente violados, o que aponta para um critério teleológico com referência ao bem jurídico.

Assim, tal critério teleológico delimita os casos de concurso efectivo (pluralidade de crimes através de uma mesma acção ou de várias acções) das situações em que, não obstante a pluralidade de tipos de crime eventualmente preenchidos, não existe efectivo concurso de crimes (os casos de concurso aparente e de crime continuado).

1.6.1. Burla Informática e os Crimes Previstos na Lei do Cibercrime (aprovada pela Lei n.º 109/2009, de 15 de Setembro)

Em face das considerações aduzidas *supra* – concretamente o facto do bem jurídico não ser apenas o património, mas igualmente a fiabilidade dos programas informáticos, o respectivo processamento e os dados, e bem assim os meios utilizados para a concretização das acções

[34] Neste sentido, o Acórdão do Supremo Tribunal de Justiça, de 18.06.2008, proferido no âmbito do proc. n.º 08º901, acessível em www.dgsi.pt.

[35] SANTOS, Rita Coelho (*O Tratamento Jurídico-Penal da Transferência de Fundos Monetários Através da Manipulação Ilícita dos Sistemas Informáticos*, Studia Jurídica, n.º 82, Coimbra Editora, 2005, pág. 261) exemplifica: um técnico responsável pela manutenção de um sistema informático, apercebe-se de uma falha técnica no sistema de tratamento automatizado de dados que está a gerar, indevidamente várias transferências de créditos para todas as contas dos empregados da empresa onde trabalha. Todavia, sabendo que irá obter um enriquecimento (ilegítimo) não regulariza o sistema, causando um prejuízo patrimonial à empregadora.

típicas da burla informática e nas comunicações – poderá existir uma relação com os crimes informáticos previstos na Lei do Cibercrime.

Não obstante o presente Guia não ter em vista a apreciação deste tipo de criminalidade, afigura-se relevante uma breve abordagem, porquanto as ténues fronteiras entre as normas incriminadoras exigirão, por um lado, a delimitação de critérios para a sua diferenciação, como, por outro lado, poderão revelar-se úteis, em termos de investigação criminal.

Nos crimes previstos na Lei do Cibercrime o bem jurídico protegido 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*[36] ».

No crime de falsidade informática previsto no artigo 3.º, n.º 1, da Lei do Cibercrime pretende-se a produção de documentos ou dados não genuínos para posterior utilização como se de verdadeiros se tratassem (engano nas relações jurídicas).

O crime previsto no artigo 4.º da Lei do Cibercrime verifica-se quando, além do mais, alguém «*tornar não utilizáveis ou não acessíveis programas ou outros dados informáticos alheios ou por qualquer forma lhes afectar a capacidade de uso*» sem estar autorizado pelo proprietário ou titular do sistema ou de parte dele. O objecto deste crime são os dados informáticos[37].

O crime do artigo 5.º da Lei do Cibercrime, apesar de próximo do previsto no preceito anterior, é dele distinto porque o seu objecto são sistemas informáticos, e daí a agravação da moldura penal[38].

Ora, partindo destas considerações e confrontando as redacções destas normas previstas na Lei do Cibercrime e a do artigo 221.º do Código Penal, resulta evidente que a sua *ratio* é distinta, não só com referência ao bem jurídico protegido, como do ponto de vista da especificidade, aquelas normas não incluem qualquer menção ao prejuízo patrimonial, que no caso do crime de burla informática e nas comunicações surge como elemento típico.

Em face do que se acabou de dizer, sempre poderia argumentar-se que, embora a previsão referente ao «prejuízo patrimonial» não surja nos artigos 4.º e 5.º, da Lei do Cibercrime, a verdade é que existe no n.º 2 do artigo 3.º do mesmo diploma legal.

[36] Como resulta do preâmbulo da Convenção sobre o Cibercrime do Conselho da Europa, aprovada por Resolução da Assembleia da República n.º 88/2009, *in* DR I Série, de 15.09.2009. Neste sentido, o Acórdão do Tribunal da Relação de Lisboa, de 30-06.2011, proferido no proc. n.º 189/09.3JASTB.L1-5, e o Acórdão do Tribunal da Relação do Porto, de 24.04.2013, proferido no proc. n.º 585/11.6PAOVR.P1, ambos acessíveis em www.dgsi.pt.

[37] Como por exemplo sucederá no caso de o agente aceder à conta de *Facebook* da vítima e alterar a password desta, impedindo-a de aceder ao seu perfil. Além de poder integrar a prática de outros ilícitos, integra o crime de dano relativo a programas ou outros dados informáticos, pois o lesado ficou sem a capacidade de usar o sistema (assim foi considerado no Acórdão do Tribunal da Relação de Lisboa, de 22.01.2013, proferido no processo n.º 581/12.6PLSNT-A.L1-5, Relator Alda Tomé Casimiro.

[38] VERDELHO, Pedro, *Op. cOp. cit.it.*, pág. 513, ponto 3.

Ora, a este propósito, Rita Santos salienta que «*a falsidade informática (artigo 4.º da LCI) pode constituir uma forma de prática de burla informática, desde que tal se concretize numa interferência no resultado do tratamento informático dos dados, total ou parcialmente falsificados. A falsidade informática realizada com o escopo de obter um enriquecimento ilegítimo, para o agente ou para terceiro, é, deste modo, consumida pelo crime de burla informática (consumpção pura), a menos que, atendendo à diversidade dos bens jurídicos protegidos, se entenda verificar-se um concurso efectivo de crimes*»[39] (itálico e sublinhado nossos).

Com efeito, a genética do crime de burla informática e nas comunicações assenta na obtenção de uma vantagem ou benefício, exigindo que seja produzido um prejuízo patrimonial de alguém, o que, de acordo com a jurisprudência, não é esse o prejuízo a que se refere a norma agora em anotação[40].

Destarte, em face do que ora ficou exposto entendemos que os crimes do artigo 221.º do Código Penal e os artigos 3.º, 4.º e 5.º da Lei do Cibercrime encontram-se numa relação de **concurso efectivo** – por não se verificar qualquer relação de especialidade, subsidiariedade ou consumpção entre as normas – em face dos distintos bens jurídicos tutelados por cada uma das incriminações, não ficando afectado o princípio do *ne bis in idem*[41].

Acresce que, no que respeita aos crimes previstos no artigo 6.º e 7.º, ambos previstos na Lei do Cibercrime, e a sua relação com o crime previsto no artigo 221.º do Código Penal, o critério dos bens jurídicos protegidos para a distinção entre as normas incriminadoras não surge tão demarcada, como nos artigos anteriormente analisados. Os respectivos bens jurídicos estão muito próximos – no crime de acesso ilegítimo está em causa a segurança dos sistemas informáticos e no crime de burla informática e nas comunicações, além do património, está em causa a fiabilidade dos dados e a sua protecção – razão que implica uma análise mais aprofundada das normas.

O acesso corresponde a uma entrada num sistema informático sem autorização, pelo que, as acções tipificadas no artigo 221.º, n.º 1, do Código Penal implicarão uma forma de acesso – integrada no conceito de «interferência».

Como salienta Pedro Verdelho, «…*por este novo tipo de crime pune-se a actuação daqueles que, recorrendo a meios informáticos fraudulentos, obtêm a informação confidencial pertencente a terceiros…*» sendo que a utilização desses dados – dados de acesso a locais reservados do mundo virtual e ilegitimamente obtidos – «…*terá outros enquadramentos:*

[39] SANTOS, Rita Coelho, O Tratamento Jurídico-Penal da Transferência de Fundos Monetários Através da Manipulação Ilícita dos Sistemas Informáticos, Studia Jurídica, n.º 82, Coimbra Editora, 2005, pág. 288.
[40] «*Neste crime, o prejuízo não tem de ser patrimonial, pois o bem jurídico que nele se protege não é o património, mas a confidencialidade, integridade e disponibilidade de sistemas informáticos, das redes e dados informáticos*» – *in* Acórdão do Tribunal da Relação do Porto, de 24.04.2013, proferido no proc. n.º 585/11.6PAOVR.P1, acessível em www.dgsi.pt.
[41] ALBUQUERQUE, Paulo Pinto de, *Op. cit*., pág. 861, ponto 17, defende existir uma relação de concurso aparente (consumpção) entre os crimes de falsidade informática, dano relativo a programas ou outros dados informáticos, sabotagem informática, acesso ilegítimo e intercepção ilegítima, entendendo ainda que estes actos prévios não são puníveis.

poderá ser por via da burla informática (Artigo 221.º, n.º 1, do Código Penal) ou eventualmente pelo n.º 1 deste mesmo Artigo 6.º … consoante a intenção do agente»[42].

Efectivamente, para lograr-se a burla informática deverá existir uma interferência, o que, por via da regra, pressupõe o acesso ilegítimo a um sistema ou rede informáticos, pelo que, para alguns autores, com os quais concordamos, o crime de burla informática do artigo 221.º, n.º 1, do Código Penal consome o crime de acesso ilegítimo previsto no artigo 6.º da Lei do Cibercrime[43].

A norma incriminadora constante do artigo 7.º da Lei do Cibercrime encontra-se muito próxima da norma anterior, sendo que o conceito «intercepção» encontra a sua definição no respectivo artigo 2.º, alínea e). Aqui o bem jurídico protegido é a privacidade na comunicação de dados[44], ou melhor, segurança e privacidade nas comunicações electrónicas[45], pelo que também quanto a este crime, consideramos que será consumido pelo crime previsto no artigo 221.º do Código Penal.

1.6.2. Burla Informática e o Crime de Passagem de Moeda Falsa (artigo 265.º do Código Penal)

A presente anotação vem na sequência do entendimento postulado pelo Acórdão do Tribunal da Relação de Lisboa, de 24.04.2007[46] no qual «*I - Sempre que um caso concreto se mostre, em simultâneo, reconduzível aos tipos legais da burla [burla informática] e da colocação em circulação de moeda falsa, está-se perante um concurso aparente ou de normas* (…) *Ao instituir a "integridade" ou "intangibilidade do sistema monetário legal ou oficial" como bem jurídico dos crimes de moeda falsa, o legislador estabeleceu uma espécie de "guarda avançada" ou "protecção de largo espectro" em relação a um conjunto indiscriminado de outros bens jurídico-penais — entre os quais se conta o património* (…)»

Ora, são equiparados a moeda, além do mais, os cartões de garantia ou de crédito, por força do artigo 267.º, n.º 1, c), do Código Penal.

Entendemos que o artigo 265.º do Código Penal não se encontra numa relação de concurso aparente (consumpção) não só porque os bens jurídicos protegidos são distintos, como a protecção dispensada ao facto jurídico da passagem de moeda falsa não abrange a protecção que o crime de burla informática pressupõe, porquanto ficaria sem protecção penal a interferência no sistema informático que reclama igualmente protecção jurídica específica e a qual se encontra abrangida pelo artigo 221.º, n.º 1, do Código Penal.

[42] VERDELHO, Pedro, *Op. cit*., pág. 517, ponto 5.
[43] SANTOS, Rita Coelho, *Op. cit.*.
[44] VERDELHO, Pedro, *Op. cit*., pág. 518, ponto 3.
[45] VENÂNCIO, Pedro Dias, Coimbra Editora, *A Lei do Cibercrime Anotada e Comentada*, 1.ª Edição, Janeiro de 2011, pág. 67.
[46] Proferido no proc. n.º 843/2007-5, Relator Martinho Cardoso, acessível em www.dgsi.pt.

Assim, consideramos existir entre as infracções em confronto uma relação de concurso efectivo porquanto existe uma pluralidade de infracções, à luz do disposto no artigo 30.º do Código Penal[47].

1.6.3. Burla Informática e os Crimes de Furto e Roubo

Das considerações já exaradas *supra* acerca do bem jurídico protegido pelo artigo 221.º do Código de Processo Penal – para as quais remetemos – julgamos que não se verifica qualquer relação de especialidade, subsidiariedade ou consumpção entre as normas, havendo, assim, concurso efectivo de crimes na medida em que não têm campo de aplicação coincidente[48].

2. Prática e Gestão Processual

2.1. Da Abertura do Inquérito

Ao Magistrado do Ministério Público compete decidir quais os actos ou diligências que deve levar a cabo para realizar as finalidades do inquérito (artigo 267.º do Código de Processo Penal) estando obrigado a promover o processo penal, dando início ao inquérito, sempre que tenha adquirido a notícia do crime (cfr. artigo 262.º, n.º 2, do Código de Processo Penal).
Na fase de inquérito, o único acto legalmente obrigatório é o interrogatório do arguido caso se verifiquem as circunstâncias previstas no artigo 272.º, n.º 1, do Código de Processo Penal, pelo que, se os factos denunciados não consubstanciarem a prática de qualquer crime, o Ministério Público não deverá abrir inquérito.

2.1.1. Condições de Procedibilidade

Tal como resulta da previsão do artigo 221.º do Código Penal, este ilícito penal reveste **natureza semipública**, dependendo de queixa do ofendido ou de pessoa a quem a lei confira tal direito (cfr. artigos 113.º a 116.º do Código Penal), tal como resulta expressamente do n.º 4 do mesmo preceito legal.

Com efeito, a **queixa** apresenta-se como pressuposto/condição objectiva de punibilidade, imprescindível ao desenvolvimento da acção penal, cabendo ao Ministério Público promover o exercício da acção penal após o titular lhe levar ao conhecimento o facto, ou depois de o ter feito perante entidade com a obrigação legal de lha transmitir (cfr. artigos 48.º, 49.º, 246.º e 248.º do Código do Processo Penal).

Não obstante, a verdade é que o crime de burla informática e nas comunicações apenas reveste a natureza semipública quando cometido na sua forma simplificada, ou seja, nos

[47] Neste sentido, o Acórdão do Supremo Tribunal de Justiça, de 12.09.2012, proferido no proc. n.º 1008/11.6JFLSB-L1.S1, Relator Armindo Monteiro, acessível em www.dgsi.pt.
[48] Neste sentido, ALBUQUERQUE, Paulo Pinto, *Op. cit.*, pág. 862, ponto 19.

segmentos tipificados no artigo 221.º, n.ºs 1 e 2, do Código Penal, não mantendo essa natureza quando se trate de uma situação enquadrável no n.º 5 do mesmo preceito legal.

Com efeito, prevendo o artigo 221.º, n.º 5, do Código Penal a agravação em função do valor (por referência ao artigo 202.º, alíneas a) e b)), o crime de burla informática e nas comunicações assume, nestes casos, **natureza pública**[49], não estando já o procedimento dependente e condicionado, na sua tramitação, aos actos de outros sujeitos processuais, podendo o Ministério Público promover o processo penal, ao abrigo do disposto no artigo 48.º do Código de Processo Penal.

2.2. Diligências de Inquérito e Recolha de Prova

Os processos de burlas informáticas encerram uma factualidade extremamente complexa, requerendo a sua investigação conhecimentos especializados.

O inquérito deverá obedecer a um certo plano estratégico, avaliando-se as diligências que deverão e/ou poderão ser realizadas – incluindo as que se afiguram urgentes – tendo em consideração a preservação e actualidade da prova, definindo-se quais os elementos de prova que podem ser imediatamente solicitados às entidades competentes e, bem assim, a realização das diligências destinadas à demonstração dos elementos típicos do crime em investigação, em obediência ao disposto nos artigos 124.º a 126.º do Código de Processo Penal.

Quanto à prova em ambiente digital, Armando Dias Ramos classifica-a como a «*informação passível de ser extraída de um dispositivo electrónico (local, virtual ou remoto) ou de uma rede de comunicações. Pelo que esta prova digital, para além de ser admissível, deve ser também autêntica, precisa e concreta.*» [50]

Assim, sendo os factos denunciados cometidos através de meios informáticos verifica-se, por essa razão, a necessidade de pesquisar e recolher prova nesse suporte, afigurando-se tal recolha de dados uma diligência indispensável e essencial para a descoberta da verdade, o que, necessariamente, convocará o regime previsto na Lei do Cibercrime, a Lei n.º 32/2008, de 17 de Julho[51] e no Código de Processo Penal.

---

[49] Neste sentido, já se pronunciou a jurisprudência, designadamente o Supremo Tribunal de Justiça, por Acórdão de 03.07.20103, no proc. n.º 122/03-5aSASTJ, referenciado no Acórdão do Tribunal da Relação de Lisboa, de 05.02.2014, proferido no proc. n.º 7950/05.6TDLSB.L1-3, acessível em www.dgsi.pt.

[50] RAMOS, Armando Dias, A Prova Digital em Processo Penal, Chiado Editora, 1.ª ed., Novembro 2014, pág. 86.

[51] Não obstante ter sido defendido que a Lei n.º 32/2008 é, desde 8 de Abril de 2014, um acto contrário ao Direito da União Europeia, em virtude do Acórdão do Tribunal de Justiça, de 8 de Abril de 2014 (processos apensos C-293/12 e 594/12) ter declarado inválida a Directiva 2006/24/CE por violação dos artigos 7.º, 8.º e n.º 1, do artigo 52.º, da Carta dos Direitos Fundamentais da União Europeia, por aquela transposta (RAMALHO, David Silva *in Métodos Ocultos de Investigação Criminal em Ambiente Digital*, Universidade de Lisboa, 2015, pág. 22), segundo a análise realizada pelo Gabinete do Cibercrime da Procuradoria-Geral da República e vertida na Nota Prática n.º 7/2015, tal decisão não afecta a validade da lei nacional, em virtude de a lei nacional ter ido muito para lá das exigências da Directiva, introduzindo um quadro mais complexo de regulamentação do processo de retenção de dados.

Para uma melhor compreensão, dos dados informáticos que constituirão prova, estes, na acepção do artigo 2.º, alínea c), da Lei do Cibercrime e do artigo 2.º, da Lei de Protecção de Dados Pessoais, no âmbito das Telecomunicações (Lei n.º 41/2004, 18 de Agosto), poderão classificar-se em:

a) Dados de base – constituem os dados referentes ao acesso à rede, designadamente através da ligação individual e para utilização própria do respectivo serviço; nestes dados incluem-se elementos importantes como a identificação do utilizador, a sua morada, número de telefone, endereço de correio electrónico, entre outros que habitualmente são solicitados pela operadora da rede de telecomunicações e fornecidos pelo cliente quando este contrata o fornecimento do serviço;

b) Dados de tráfego – constituem os dados necessários ao estabelecimento e à direcção da comunicação, os quais permitem identificar os utilizadores, o relacionamento directo entre os utilizadores através da rede, a localização, a frequência, a data, a hora e a duração da comunicação;

c) Dados de conteúdo – constituem o teor concreto da comunicação realizada, ou seja, os elementos relativos ao próprio teor da comunicação[52].

2.2.1. Aplicação da Lei do Cibercrime

Este diploma encerra, além do mais, disposições de carácter processual e de cooperação internacional relevantes para a actividade investigatória do Ministério Público e, em face do que se expôs no ponto antecedente, tratando-se a burla informática e nas comunicações de um crime cometido através de sistema informáticos terá integral aplicação a Lei do Cibercrime (cfr. respectivo artigo 1.º e artigo 11.º, n.º 1).

Assim, poderá o Ministério Público utilizar os meios de obtenção de prova previstos **nos artigos 12.º a 17.º da Lei do Cibercrime**, a saber, a preservação e revelação expedita de dados (artigo 12.º e 13.º), a injunção para apresentação ou concessão do acesso a dados (artigo 14.º), a pesquisa e apreensão de dados informáticos (artigos 15.º e 16.º)[53], a apreensão de correio electrónico e registos de comunicações de natureza semelhante (artigo 17.º) **quando pretenda a preservação de dados já verificados e produzidos**[54].

O Ministério Público e os órgãos de polícia criminal – estes *«mediante autorização da autoridade judiciária competente ou quando haja urgência ou perigo na demora»* – podem

[52] A este propósito poderá ser consultado o Parecer do Conselho Consultivo da Procuradoria Geral da República de 28 de Agosto de 2000, disponível em www.ministeriopublico.pt.
[53] Não deverá confundir-se a apreensão de «*dados informáticos*» - que seguirá o regime dos artigos 16.º e 17.º da Lei do Cibercrime - com a apreensão de «*sistemas informáticos*» (telemóveis, computadores, pen drive, CD Rom, etc…) – que seguirá o regime das apreensões do Código de Processo Penal.
[54] A **finalidade** destes meios de obtenção de prova não é a recolha de dados, mas sim a sua **preservação**, como resulta das expressões «*receio de que possam perder-se, alterar-se ou deixar de estar disponíveis»* (cfr. artigo 12.º, n.º 1) e «*preservação*» (cfr. artigo 13.º, n.º 1), sendo que o período fixado não poderá ir além dos três meses, embora prorrogável até ao prazo de um ano (cfr. artigo 12.º, n.º 5).

determinar a **preservação expedita de dados, revelação expedita de dados** a determinadas entidades e cidadãos, funcionando esta preservação como medida cautelar para a conservação dos dados, pelo que aplicar-se-á mesmo que se tratem de dados de tráfego ou de conteúdo, pois a finalidade é salvaguardá-los e não aceder aos mesmos.

Já a **injunção para apresentação ou para concessão de acesso a dados informáticos** pode ser dirigida tanto a «*entidades públicas ou privadas, que faculte aos utilizadores dos seus serviços a possibilidade de comunicar por meio de um sistema informático ou outra entidade que trate ou armazene dados informáticos*» (em face da definição do artigo 2.º, alínea d), como a qualquer pessoa que tenha «*disponibilidade ou controlo desses dados*» (cfr. artigo 12.º, n.º 1, e 4, bem como artigo 14.º, n.º 1, da Lei do Cibercrime)[55].

Esta injunção tem em vista a obtenção de dados de base e não contende com a privacidade do(s) titular(es), podendo ser comunicados a pedido de qualquer autoridade judiciária, e, na fase de inquérito, a pedido do Ministério Público (cfr. artigos 53.º, n.º 1 e n.º 2, alínea b), 262.º e 263.º, todos do Código de Processo Penal).

O incumprimento da ordem determinada à luz do artigo 14.º da Lei do Cibercrime por parte do possuidor dos dados é sancionado, constituindo crime de desobediência simples, punível com pena de prisão até um ano ou de multa até 120 (cento e vinte) dias.

No que respeita à **pesquisa informática** a que se refere o artigo 15.º do diploma em apreço, cumpre relevar que não obstante a terminologia utilizada pelo legislador, a verdade é que esta «pesquisa» traduz-se numa verdadeira busca, embora adaptada ao ambiente digital, tal com resulta da remissão do n.º 6 deste preceito, para obtenção de «*dados informáticos específicos e determinados, armazenados num determinado sistema informático*».

O Magistrado do Ministério Público pode determinar, por despacho, a sua realização e, sempre que possível, deverá presidir à mesma. A título excepcional e nos casos previstos no artigo 15.º, n.º 3, da Lei do Cibercrime, poderão os órgãos de polícia criminal proceder à pesquisa de dados informáticos sem a prévia autorização da autoridade judiciária, desde que observem o previsto nos n.ºs 3 e 4, deste artigo 15.º.

Julgamos que, no despacho que determina a pesquisa de dados informáticos, deverá ser logo determinada a correspondente apreensão de dados, por tal se afigurar pertinente para a produção de prova.

Para a realização das pesquisas, não se afigura essencial que os dados se encontrem armazenados no dispositivo informático objecto da pesquisa, podendo estar armazenado numa "nuvem", sendo esta acessível a partir dos referidos dispositivos. É esta a razão que subjaz à expressão «*parte diferente do sistema pesquisado, mas que tais dados são*

[55] Apenas não poderá ser dirigida a suspeito ou arguido no processo nesse processo e quanto a sistemas informáticos utilizados para o exercício da advocacia, actividade médica, bancária ou profissão de jornalista (cfr. artigo 14.º, n.ºs 5 e 6), prevenindo-se, desta forma, a auto-incriminação do visado ou uma actuação processual desleal, que pusesse em causa o princípio da presunção da inocência. Mas este meio de prova afigura-se muito relevante porquanto **ocorrerá sem o conhecimento do titular dos dados.**

legitimamente acessíveis a partir do sistema inicial» vertida no artigo 15.º, n.º 5, da Lei do Cibercrime.

A apreensão de correio electrónico e registos de natureza semelhante, tal como previsto no artigo 17.º da Lei do Cibercrime, poderá contender com o direito de inviolabilidade das comunicações.

Como salienta Costa Andrade[56] «*…depois de recebido, lido e guardado no computador do destinatário, um e-mail deixa de pertencer à área de tutela das telecomunicações*», assim, passa a ser um ficheiro digital, sujeitando-se ao regime correspondente àquele a que ficam sujeitos os documentos que o visado cria e arquiva no seu computador.

Contudo, entendemos que o legislador na Lei do Cibercrime pretendeu proteger a privacidade do visado, porquanto estabeleceu a remissão para o regime de apreensão de correspondência previsto no artigo 179.º do Código de Processo Penal.

Assim, para prosseguir-se com a apreensão do correio, tais apreensões deverão ser objecto de despacho judicial, sob pena de nulidade expressa, cabendo ao juiz que autorizar a diligência, a primeira tomada de conhecimento do conteúdo da correspondência apreendida, o que constitui um acto da competência exclusiva do Juiz de Instrução Criminal (cfr. artigo 268.º, n.º 1, alínea d), do Código de Processo Penal). Entendemos que a sua violação constitui a nulidade da prova, remetendo para o regime da proibição da prova.

O **artigo 18.º da Lei do Cibercrime** será aplicável quando estiver em causa a **intercepção de comunicações**.

É o critério da actualidade dos dados, bem como da sua classificação, que distingue os meios de prova previstos nos artigos 12.º a 17.º do previsto no artigo 18.º, todos da Lei do Cibercrime, porquanto[57]:

«***a)*** *No caso do artigo 17.º estamos a tratar de dados de tráfego e de conteúdo de correio electrónico, armazenados;*

b) *No caso do artigo 18.º falamos de interceptar dados de tráfego e de conteúdo;*

c) *No caso dos artigos 12.º a 16.º – e na competência do M.P. – é possível pesquisar e apreender dados de base e de tráfego armazenados* (…)».

Nos dois primeiros casos é necessária a intervenção de Juiz, no ***terceiro da entidade judiciária que presidir à fase processual****. Neste último caso será sempre necessária a intervenção judicial se forem encontrados dados a inserir na previsão do artigo 16.º, n.ºs. 3 e 6.*»[58]

[56] ANDRADE, Manuel da Costa, Bruscamente no Verão Passado, *a Reforma do Código de Processo Penal*, Coimbra Editora, 2009, pág. 157.
[57] Neste sentido já se pronunciaram os Acórdãos do Tribunal da Relação de Évora, de 06.01.2015, no proc. n.º 6793/11.2TDLSB-A.E1, de 20.01.2015, no proc. n.º 648/14.6GCFAR-A.E1, sendo Relator João Gomes de Sousa, ambos acessíveis em www.dgsi.pt.

Com efeito, estando em causa a intercepção de comunicações é possível distinguir dois regimes processuais:

1) Quanto aos crimes previstos na Lei do Cibercrime (cfr. artigo 18.º, n.º 1, alínea a)); ou

2) Quanto aos crimes cometidos por meio de um sistema informático ou em relação aos quais seja necessário proceder à recolha de prova em suporte electrónico, desde que estes se encontrem previstos no artigo 187.º do Código de Processo Penal (cfr. artigo 18.º, n.º 1, alínea b)).

Nos termos *supra* referidos, a remissão para o Código de Processo Penal opera no caso dos crimes previstos no artigo 18.º, n.º 1, alínea b), e já não nos referidos na alínea a) do mesmo preceito legal. Mais acresce que, em face do artigo 18.º, n.º 4, são aplicáveis subsidiariamente, e desde que não contrariem a Lei do Cibercrime, os artigos 187.º, 188.º e 190.º do Código de Processo Penal[59].

Assim, o crime de burla informática e nas comunicações permitirá a **intercepção de comunicações** apenas quando em causa estiver uma burla informática e nas comunicações **na sua forma agravada** (cfr. artigo 221.º, n.º 5, do Código Penal), pois em face da remissão operada para o artigo 187.º do Código de Processo Penal, apenas este contemplará uma moldura penal «…*com pena de prisão superior, no seu máximo, a 3 anos».*

Por último, o artigo 19.º, n.º 1, alínea b), da Lei do Cibercrime prevê, de forma expressa, a aplicação da Lei n.º 101/2001, de 25 de Agosto (que aprovou o regime jurídico das acções encobertas para fins de prevenção e investigação criminal) à burla informática e nas comunicações, desta forma alargando o elenco de crimes previstos no artigo 2.º desse diploma legal, devendo sempre ter-se em especial atenção o prazo de setenta e duas horas a que se refere o respectivo artigo 3.º, n.º 3.

2.2.2. Protocolos de Colaboração

Resultando, à partida, da notícia de crime a utilização de meios informáticos, impõe-se a descoberta da localização geográfica a partir da qual teve origem a conduta criminal, o que, geralmente, se obtém pela identificação do endereço IP de onde partiu a comunicação. Nem sempre o endereço de IP conduzirá à localização do agente, mas pelo menos tal será uma diligência que relevará aquando do planeamento da investigação.

Assim, será através de operadoras que prestam serviços de *Internet*[60], ou fornecedores de serviço internacionais – como o *Facebook (abrangendo* o *Instagram), a* Microsoft, a Google

[58] *In* Acórdão do Tribunal da Relação de Évora, de 06.01.2015, no proc. n.º 6793/11.2TDLSB-A.E1.
[59] O artigo 189.º do Código de Processo Penal nunca será aplicável a crimes informáticos, seja qual for o catálogo aplicável.
[60] Constituem um «Fornecedor de serviço» na acepção do artigo 2.º, alínea d), da Lei n.º 109/2009, de 15 de Setembro (Lei do Cibercrime).

(abrangendo o *Blogger* e o *YouTube*) – que logrará obter-se tal informação, e dados a ela associados, devendo acautelar-se os pedidos que se revelem pertinentes aquando da prolação do primeiro despacho, os quais deverão ser assinados pelo Magistrado do Ministério Público titular do inquérito.

Em 9 de Julho de 2012 a Procuradoria-Geral da República assinou um protocolo de cooperação com operadores de comunicações, no âmbito da investigação da cibercriminalidade e da obtenção de prova digital, estabelecendo a Circular n.º 12/2012, da Procuradoria-Geral da República, que os contactos com as operadoras nacionais operam através dos formulários aprovados, remetidos na forma ali prevista.

Os pedidos aos fornecedores de serviços internacionais identificados assentam na cooperação informal, sem recurso a cartas rogatórias, sendo que a *Microsoft*, a *Google* (abrangendo o *Blogge*r e o *YouTube*) e a *Facebook* (abrangendo o *Instagram*), em geral aceitam remeter ao Ministério Público dados referentes à identificação do titular da conta (nome, morada e endereço IP a partir do qual a conta foi aberta), que existem enquanto a conta estiver activa e sendo que, no caso de pedido de informação sobre concretos acessos à conta, a identificação do endereço IP a partir do qual foi feito o acesso, apenas é guardada por 90 dias.[61] A título excepcional e quando haja perigo para a vida ou a integridade física grave, a generalidade dos fornecedores de serviço estrangeiros (incluindo o *TWITTER* e a *YAHOO)* disponibilizam canais mais expeditos[62].

2.2.3. Código de Processo Penal

Quanto aos meios de obtenção de prova previstos no Código de Processo Penal julgamos de particular importância as **buscas**, pois, podendo ser determinadas pelo Ministério Público (ao abrigo do disposto nos artigos 1.º, alínea b); 174.º, n.ºs 1, 2 e 3; 176.º; 178.º e 267.º, todos do Código de Processo Penal), deverá ser assegurado, desde logo, no despacho que as determina, a apreensão e a pesquisa nos suportes informáticos/ficheiros que vierem a ser apreendidos, tendo em consideração que a apreensão dos dados informáticos deverá ser determinada pelo artigo 16.º da Lei do Cibercrime e a apreensão dos sistemas informáticos (como computadores, *tablets*, telemóveis, consolas de jogos, discos externos, cartões de memória, CD Rom, *pen drive*, DVDs) pelo artigo 178.º do Código de Processo Penal.

Em conformidade entendemos que no mandado de busca, ou na promoção do mesmo, deverá ser previsto:

I) Autorização para pesquisa de dados informáticos e para a sua apreensão, de acordo com o artigo 15.º, n.ºs 1 e 2, e do artigo 16.º, n.º 1, ambos da Lei do Cibercrime, especificando-se a

[61] De acordo com a Nota prática n.º 2/2013 do Gabinete de Cibercrime da Procuradoria-Geral da República, acessível em: http://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/nota_pratica_3_isp_eua.pdf.
[62] Este tipo de comunicação deverá ser realizado através do contacto 24/7 da Polícia Judiciária, nos termos do artigo 21.º da Cibercrime – contacto24.7@pj.pt – Nota prática n.º 2/2013, pontos 11 e 12.

forma de apreensão pretendida (de entre as previstas no n.º 7 do artigo 16.º do mesmo diploma legal);

II) Concretização do tipo de dados pretendidos (ficheiros de texto, de imagem, de som, de vídeo, de áudio e vídeo, bases de dados, agenda, registos de acesso e de contactos, correio electrónico, SMSs, MMs, outras comunicações);

III) Querendo-se aceder ao conteúdo do *email* ou de outras comunicações de natureza semelhante, o mandado deverá prever também autorizar a sua apreensão, de acordo e nos termos do disposto no artigo 17.º da Lei do Cibercrime[63].

Afigura-se merecedor de destaque o facto de ser possível a **emissão, pelo Ministério Público, bem como pelos órgãos de polícia criminal, de mandados fora de flagrante delito**, quando estiver em investigação o crime de burla informática e nas comunicações (agravado) [64], pois tal é o que resulta das disposições conjugadas dos artigos 257.º e 202.º, n.º 1, alínea d), ambos do Código de Processo Penal, prevendo-se desde logo que, em face da competência encontrar-se reservada na Polícia Judiciária, os respectivos mandados emitidos pelo Ministério Público venham a ser cumpridos por este órgão de polícia criminal, com observância das formalidades legais previstas nos artigos 258.º e 259.º, ambos do Código de Processo Penal.

Em face da especificidade do crime de burla informática e nas comunicações, assumem-se como essenciais à investigação as **perícias e exames**, previstos respectivamente nos artigos 151.º e seguintes e 171.º do Código de Processo Penal.

Assim, por despacho, o Ministério Público deverá ordenar a realização da perícia informática, ao abrigo do disposto nos artigos 151.º, 152.º, n.º 1, 153.º e 154.º, do Código de Processo Penal, com a correspondente nomeação do(s) perito(s)[65] e elaboração dos quesitos, para o que será absolutamente aconselhável o apoio de um perito com conhecimentos especiais, podendo o Magistrado solicitá-lo ao Gabinete do Cibercrime da PGR, tendo em consideração os protocolos celebrados com entidades nestas áreas de criminalidade.

2.2.4. Primeiro Despacho

Tendo em consideração as especificidades do crime em apreço, concretamente o respectivo enquadramento da política criminal, delegação de competências e estratégia de investigação, propomos o seguinte despacho inicial[66]:

[63] Realizadas em todas as dependências e espaços fechados, sótãos, garagens, e respectivos anexos, com arrobamento de portas se necessário, caixas de correio.
[64] O que será relevante para o crime de burla informática e nas comunicações na sua forma agravada, prevista no artigo 221.º, n.º 5, alínea a), pois o da alínea b) encontrará acolhimento no artigo 202.º, n.º 1, alínea a), do Código de Processo Penal.
[65] Os que forem indicados pela Polícia Judiciária.
[66] Inspirado no primeiro despacho proferido no âmbito do proc. n.º XXXX/14.5PFLRS, Loures – 7.ª Secção DIAP. Da notícia do crime resultava, desde logo, informação sobre operações bancárias fraudulentas, pelo que considerou-se solicitar *ab initio* as respectivas informações.

I. Os factos denunciados nos presentes autos são susceptíveis de, abstractamente, integrar a prática de, pelo menos, um crime de burla informática e nas comunicações, previsto e punido pelo artigo 221.º, n.º [.] do Código Penal.

De acordo com o artigo 3.º, alínea g), da Lei n.º 96/2017, de 23 de Agosto, a qual define os objectivos, prioridades e orientações de política criminal para o biénio de 2017 -2019, Directiva 1/2017, ponto I, alínea f), este será um inquérito de ***investigação prioritária****.*

Anote *na capa e informaticamente.*

*

II. Remeta *os formulários que lhe entrego em mão, preenchidos de acordo com as instruções constantes da Circular n.º 12/2012 da Procuradoria-Geral da República, às seguintes operadoras de telecomunicações:*

– MEO - Serviços de Comunicações e Multimédia, S.A. e
– Vodafone Portugal Comunicações Pessoais, S.A..

Consulte e obtenha *através da plataforma NOS Comunicações, S.A. os elementos supra referidos.*

Preencha o formulário se necessário.

Prazo*: 30 dias.*

Aguarde pela informação pelo prazo de 30 dias, findos os quais, nada vindo, insista.

*

III. *Nos termos do artigo 270.º, n.º 1, do Código de Processo Penal, artigo 7.º, n.º 3, alínea l) da Lei n.º 49/2008, de 27 de Agosto do Ponto II da Circular da Procuradoria-Geral da República n.º 6/2002,* ***delego na Polícia Judiciária*** *a competência para proceder a diligências de inquérito nestes autos.* **(…)**

Remeta os autos e organize translado.

Aguarde 60 dias pela conclusão das investigações.

Comunique*.*

Após o decurso do prazo conferido, solicite informação acerca do estado do inquérito, a ser prestada em 10 dias.

*

IV*. Não obstante aquela delegação, importa, desde já, nos termos do disposto no artigo 79.º, n.º 2, alínea e), do Decreto-Lei n.º 298/92, de 31 de Dezembro, bem como dos artigos 53.º, n.º 1*

e n.º 2, alínea b), 262.º e 263.º, todos do Código de Processo Penal, ***oficiar o BANCO*** *[.] com sede na [.] com cópia de fls. [.] para em* ***10 (dez) dias*** *informar nos autos:*

i. *Informação detalhada da movimentação bancária de [.] €, realizada no dia [.] da conta bancária com o IBAN [.] para a conta bancária n.º [.], designadamente quanto à origem do referido acesso à conta bancária de origem e das respectivas transacções fraudulentas (endereços de IP e grupo data/hora ou localização do ATM onde foi efectuada a transferência);*

ii. *Identificação completa do titular da conta bancária beneficiária da transferência;*

iii. *Localização geográfica da agência respeitante à conta bancária beneficiária;*

iv. *Data da criação da conta bancária beneficiária;*

v. *Cópia da ficha de assinaturas e todos os elementos de identificação sobre os titulares da conta bancária identificada;*

vi. *Saldo médio da conta bancária beneficiária até à data da transferência.*

Aguarde por 20 dias.

Após, insista. *(Local, data, ass.)*

2.2.5. Constituição como arguido

O Ministério Público tem ampla margem de decisão sobre o momento do interrogatório do arguido, podendo escolher, de acordo com o planeamento da investigação, o momento que se afigure mais adequado para o efeito[67].

No Acórdão de Uniformização de Jurisprudência n.º 1/2006 fixou-se que «*A falta de interrogatório como arguido, no inquérito, de pessoa determinada contra quem o mesmo corre, sendo possível a notificação, constitui a nulidade prevista no artigo 120.º, n.º 2, alínea d), do Código de Processo Penal*.»[68], pelo que, a título de nota que, caso não seja possível apurar o paradeiro do(s) suspeito(s) mas cuja identidade se encontra perfeitamente determinada, e reunidos os indícios suficientes de que foi aquele agente que praticou o crime, deverá o Magistrado do Ministério Público deduzir a acusação, na qual deverá salvaguardar a notificação ao arguido por contacto pessoal, solicitando ao órgão de polícia criminal competente, no acto da notificação, a constituição na qualidade de arguido e respectiva

[67] *In* Código de Processo Penal Comentado, 2016, 2.ª Edição revista, pág. 922.
[68] *In* Acórdão de Uniformização de Jurisprudência n.º 1/2006, de 2 de Janeiro, de 02.01.2006, acessível em www.dgsi.pt.

prestação de Termo de Identidade e Residência (TIR), com a entrega de duplicados legais, nos termos do disposto no artigo 58.º, n.º 4, do Código de Processo Penal.

Podendo haver responsabilidade penal das pessoas colectivas, deverão estas ser constituídas arguidas se o Ministério Público considerar que as mesmas são susceptíveis de vir a ser responsabilizadas. De acordo com o disposto no artigo 25.º do Código de Processo Civil (aplicável *ex vi* do artigo 4.º do Código de Processo Penal) as pessoas colectivas são representadas por quem a lei, os estatutos ou o pacto social designarem e, considerando a Circular 4/2011, de 10-10-2011 da Procuradoria-Geral da República «*os Magistrados e Agentes do Ministério Público deverão instruir o órgão de polícia criminal, no qual deleguem competência para a investigação ou a realização de diligências, no sentido de* ***procederem à sua constituição como arguida, através dos seus actuais representantes legais***»[69] (itálico e destaque nossos).

2.2.6. Medidas de Coacção Aplicáveis

Entendemos que se afiguraria relevante uma breve referência às medidas de coacção, concretamente à possibilidade de aplicação da prisão preventiva ao crime de burla informática e nas comunicações, porquanto, em face das disposições conjugadas do artigo 221.º do Código Penal e do artigo 202.º do Código de Processo Penal, afigura-se possível a sua aplicação quando o crime reveste a forma agravada, desde que se verifiquem as demais condições de aplicação, mas que, tendo em conta o âmbito do presente Guia, não se irão apreciar.

2.3. Encerramento do Inquérito

Findo o inquérito, ou seja, realizadas as diligências de investigação tidas por pertinentes para apurar a existência do crime, determinar os seus agentes e a sua responsabilidade (artigo 262.º, n.º 1, do Código de Processo Penal), o Magistrado do Ministério Público depara-se com as seguintes possibilidades de decisão:

– Arquivamento (artigo 277.º, n.ºs 1 e 2, do Código de Processo Penal);

– Suspensão provisória do processo (artigo 281.º do Código de Processo Penal);

– Requerimento para aplicação de pena em processo sumaríssimo (artigo 392.º do Código de Processo Penal) e, por fim,

– Acusação (artigo 283.º do Código de Processo Penal).

[69] Sociedades civis - representadas pelos administradores (cfr. artigo 996.º, n.º 1, do Código Civil); Sociedades em nome colectivo - representadas pelos gerentes (cfr. artigo 192.º, do Código das Sociedades Comerciais); Sociedades por quotas - representadas pelos gerentes (cfr. artigo 260.º, do Código das Sociedades Comerciais); Sociedades anónimas -representadas pelos seus administradores (cfr. artigo 408.º, do Código das Sociedades Comerciais) e ainda representadas por quem estiver munido de mandato do representante legal (cfr. 252.º, n.º 6, 391.º, n.º 7, do Código das Sociedades Comerciais).

2.3.1. Arquivamento [70]

Optámos por não abordar no presente guia os diversos fundamentos que subjazem ao despacho de arquivamento a proferir pelo Ministério Público, nos termos do disposto no artigo 227.º, n.ºs 1 e 2, do Código de Processo Penal, mas apenas aqueles que, em face da especialidade das especificidades do crime de burla informática e nas comunicações se afiguram mais relevantes.

2.3.1.1. Por Desistência de Queixa

Tratando-se o presente ilícito de crime de natureza semipública, o mesmo admite a desistência de queixa por parte do ofendido até à publicação da sentença da 1.ª instância (cfr. artigo 116.º, n.º 2, do Código Penal).

Com efeito, ocorrendo tal desistência na fase de inquérito, cabe ao Ministério Público homologar a desistência de queixa, notificando, para tanto, o arguido, nos termos do artigo 51.º, n.º 3, do Código de Processo Penal, para que o mesmo se pronuncie quanto à desistência de queixa apresentada, com a advertência de que, em caso de o arguido nada dizer quanto à mesma, a sua falta de resposta valerá como não oposição. Em consequência, nos termos do artigo 51.º, n.º 2, 1.ª parte do Código de Processo Penal, cessa a intervenção do Ministério Público, pelo que deverá determinar-se o arquivamento dos autos por inadmissibilidade legal do procedimento criminal, nos termos do disposto no artigo 277.º, n.º 1, do Código de Processo Penal.

2.3.1.2. Por Extinção do Procedimento Criminal

Em face da remissão do n.º 6 do artigo 221.º do Código Penal, deverá ser apreciado o artigo 206.º do Código Penal, o qual assume diferentes contornos consoante estejamos, por um lado, perante crimes patrimoniais na sua forma agravada, tal como resulta do respectivo n.º 1, e, por outro lado, perante crimes cuja restituição e reparação é efectuada dentro de um determinado limite temporal, como resulta do n.º 2[71].

Significa que, o n.º 1 do artigo 206.º do Código Penal terá aplicação quando estão em causa certos crimes patrimoniais que, pela sua natureza, os respectivos ofendidos não poderiam desistir do procedimento mesmo que os seus interesses viessem ficar repostos e dissessem respeito a direitos disponíveis.

Como salienta Paulo Pinto de Albuquerque «*A reforma do Código Penal de 2007 acrescentou uma norma fundamental: o* ***acordo entre o ofendido e o arguido*** (…) *A ratio da disposição legal é esta: na generalidade dos casos de crime contra o património o ofendido fica satisfeito*

[70] Nos termos e para os efeitos do disposto na Circular da Procuradoria-Geral da República n.º 8/2008, de 23.05.2008, deverá consignar-se a data da prescrição.
[71] Em face do tema proposto, de prática e gestão processual, apenas abordaremos o n.º 1, do artigo 206.º do Código Penal, por a mesma encerrar uma condição de procedibilidade que poderá verificar-se também na fase de inquérito, o que vai ao encontro do objectivo do presente guia.

com a reparação do dano que lhe foi causado o a restituição da coisa sua, dando de bom grado a sua concordância para a extinção da responsabilidade criminal (…) *Esta faculdade do ofendido resultante da natureza semipública de alguns crimes contra o património estava, contudo, vedada nos casos dos crimes públicos* (…) *O legislador decidiu, e bem, alterar este estado de coisas, permitindo que também em relação aos crimes públicos a satisfação do interesse do ofendido possa fazer cessar a responsabilidade criminal. Destarte, é também uma nova categoria processual de crimes que nasce: os crimes públicos cuja procedibilidade depende da vontade do ofendido* (…)»[72].

Com efeito, a extinção do procedimento criminal operará, de acordo com o artigo 206.º, n.º 1, e artigo 221.º, n.º 6, ambos do Código Penal, mediante o acordo do(s) ofendido(s) e mediante a restituição da coisa ou reparação integral dos prejuízos causados[73].

Das considerações aduzidas *supra* resulta que o artigo 206.º, n.º 1, do Código Penal apenas terá aplicação quando o crime de burla informática e nas comunicações assumir a forma agravada, pois tal é o que decorre das disposições conjugadas do n.º 1, do artigo 206.º e n.º 6, do artigo 221.º, ambos do Código Penal.

Como consequência da sua verificação, deverá o Ministério Público proceder ao arquivamento do inquérito por inadmissibilidade legal do procedimento criminal, por extinção da responsabilidade criminal, nos termos do disposto no artigo 206.º, n.º 1, e 277.º, n.º 1, do Código de Processo Penal.

2.3.2. Instrumentos de Oportunidade e Consenso

Terminado o inquérito o Ministério Público deverá, caso tenha recolhido indícios suficientes da prática de um crime de quem foi o seu autor, equacionar soluções em alternativa à acusação[74], sendo neste contexto que surge a suspensão provisória do processo e, bem assim, o processo sumaríssimo.

A moldura prevista para o crime de burla informática e nas comunicações – seja na modalidade simples prevista no artigo 221.º, n.ºs 1 e 2, seja na modalidade prevista no n.º 5, alínea a), do Código Penal – permite a possibilidade de aplicação do **instituto da suspensão provisória do processo**, pelo que, caso o Ministério Público considere não aplicar, os motivos deverão resultar e ficar consignados em despacho fundamentado. Pelo contrário, apurando que os agentes (pessoas singulares ou colectivas) reúnem as condições necessárias para lhes ser aplicado o referido instituto o Ministério Público, cremos que, atendendo ao enriquecimento e/ou benefício que da actuação criminosa pode aportar para o seu agente,

[72] ALBUQUERQUE, Paulo Pinto de, *in* Comentário do Código Penal à luz da Constituição da República Portuguesa e da Convenção Europeia dos Direitos do Homem, 3.ª Edição actualizada, Universidade Católica Editora, Novembro de 2015, págs. 816 e 817, ponto 9 e 10.
[73] A reparação a que se refere o preceito legal em anotação deverá ser integral, não podendo ser considerada para tais efeitos, a transacção das partes sobre o pedido de indemnização civil deduzido, tendo em vista o pagamento em prestações da indemnização acordada (*in* Acórdão do Tribunal da Relação do Porto, de 08.03.2017, proferido no proc. n.º 1397/4.0TDPRT.P1, Relator Castela Rio, acessível em wwww.dgsi.pt).
[74] Em cumprimento da Directiva 1/2014, da Procuradoria-Geral da República, de 15.1.2014.

deverá ser equacionada pelo Magistrado do Ministério Público – além de outras que se afigurem adequadas, proporcionais e suficientes – a obrigação de indemnizar o lesado e ainda a injunção de entrega de certa quantia ao Estado ou a instituição privada de solidariedade social e a de prestação de serviço de interesse público.

Cumpre dar especial relevo ao facto de que, havendo concurso efectivo de crimes, por exemplo entre o crime de burla informática e de falsidade informática (como *supra* defendido) a aplicação deste instituto não ficará prejudicada, porquanto a pena de cada um dos crimes que integra o concurso não excede a medida prevista[75], continuando a verificar-se as mesmas razões de política criminal.

Já quanto ao processo sumaríssimo – enquanto forma de processo especial com vista a uma solução consensual motivada por razões de simplificação, eficácia e de economia processual[76] – já não será aplicável em caso de concurso de crimes, mesmo no exemplo referido anteriormente, pois «*Em caso de concurso de crimes, a pena a tomar em consideração é a aplicável ao concurso, que não pode exceder os 5 anos de prisão.*»[77] (itálico e sublinhado nossos).

Na ponderação da sua aplicação, o Magistrado do Ministério Público deverá levar em conta que a burla informática é um crime essencialmente contra o património e que o seu grau de ilicitude ajuíza-se pelo valor do prejuízo infligido ao ofendido. Acresce que para a apreciação do dolo deverá levar-se em conta o nível da sofisticação da actuação do agente, que poderá revelar o planeamento, a reflexão sobre os meios utilizados.

Havendo responsabilidade penal de pessoa colectiva[78], a medida concreta da pena de multa deverá ser fixada em dias, de acordo com os critérios estabelecidos no n.º 1, do artigo 71.º, do Código Penal (tal como resulta do artigo 90.º-B, n.º 4), tendo em consideração a culpa e as exigências de prevenção, definindo-se cada um dos critérios, tomando como referência a pessoa colectiva[79] (n.º 5 do artigo 90.º-B)[80].

2.3.3. Acusação

O corpo da acusação deverá integrar todos os elementos necessários à verificação do crime de burla informática e nas comunicações, sendo que deverá incluir:

– A delimitação temporal e geográfica;

[75] O que é salientado pela Directiva 1/2014, da Procuradoria-Geral da República, de 15.1.2014.
[76] PEREIRA, Rui Sousa e SILVA, David Ramalho *in Os processos especiais no direito processual português*, O Direito, ano 147.º (2015), IV, pág. 835.
[77] *In* Directiva 1/2016, da Procuradoria-Geral da República.
[78] BRANDÃO, Nuno, *O Regime Sancionatório das Pessoas Colectivas na Revisão do Código Penal, in Revista do CEJ, 1.º Semestre, 2008, N.º 8 (Especial): Jornadas sobre a Revisão do Código Penal, pp. 41-54,* pág. 5, ponto 3.3.
[79] Sempre tendo presente que «*a perigosidade criminal de uma pessoa colectiva é distinta e manifesta-se de modo diferente da perigosidade criminal de uma pessoa física*».
[80] No despacho, o Ministério Público deverá consignar que ao abrigo do Ponto VI, n.º 3, da Circular n.º 6/2002, de 11 de Março de 2002, da Procuradoria-Geral da República foi requerida a aplicação de pena de multa em processo sumaríssimo.

– A descrição da conduta do agente de forma a apreciar-se qual a modalidade típica a que respeita;

– O resultado como necessário dessa conduta;

– O valor do prejuízo provocado na vítima;

– O nível da sofisticação e resolução subjectiva;

– O enriquecimento ou benefício ilegítimos;

– A actuação de forma livre, consciente e voluntária, bem como a consciência da punição e qualificação jurídica.

Para responsabilização das pessoas colectivas encontram-se previstas penas acessórias, designadamente os artigos 90.º-A a 90.º-M, do Código Penal.

IV. Hiperligações e referências bibliográficas

Hiperligações

Cibercrime
Relatórios Anuais de Segurança Interna
Statista

Referências bibliográficas

ANDRADE, Manuel da Costa, Bruscamente no Verão Passado, *a Reforma do Código de Processo Penal*, Coimbra Editora, 2009, pág. 157.

ALBUQUERQUE, Paulo Pinto de, *in Comentário do Código Penal à luz da Constituição da República Portuguesa e da Convenção Europeia dos Direitos do Homem*, 3.ª Edição actualizada, Universidade Católica Editora, Novembro de 2015, pág. 860.

ASCENSÃO, José de Oliveira, *Estudos sobre o Direito da Internet e da Sociedade de Informação*, Almedina, Abril de 2001, pág. 216 e 2017.

AZEVEDO, Ana Helena França*, Burlas Informáticas: Modos de Manifestação*, Tese de Mestrado em Direito e Informática, Universidade do Minho, Janeiro de 2016, pág. 39.

BRANDÃO, Nuno, *O Regime Sancionatório das Pessoas Colectivas na Revisão do Código Penal, in Revista do CEJ, 1º Semestre, 2008 N.º 8 (Especial): Jornadas sobre a Revisão do Código Penal, pp. 41-54,* pág. 5.

COSTA, Almeida, *in Comentário Conimbricense do Código Penal*, Tomo II, 1999, pág. 328.

MONIZ, Helena, FARIA COSTA, José de, *Algumas reflexões sobre a criminalidade informática em Portugal*, *in* BFDUC, Vol. LXXIII, 1997, págs. 323-324;

PEREIRA, Rui Sousa e SILVA, David Ramalho *in Os processos especiais no direito processual português*, O Direito, ano 147.º (2015), IV, pág. 835

RAMOS, Armando Dias, A Prova Digital em Processo Penal, Chiado Editora, 1.ª ed. Novembro 2014, pág. 86.

ROCHA, Manuel António Lopes, *A Revisão do Código Penal Soluções de Neocriminalização, Jornadas de Direito Criminal,* Conferências proferidas na Aula Magna da Reitoria da Universidade de Lisboa, em 3 e 4 de Julho de 1995, Lisboa 1996, página 92.

SANTOS, Rita Coelho (*O Tratamento Jurídico-Penal da Transferência de Fundos Monetários Através da Manipulação Ilícita dos Sistemas Informáticos*, Studia Jurídica, n.º 82, Coimbra Editora, 2005, pág. 261 – 288.

SANTOS, Manuel Simas, LEAL-HENRIQUES, Manuel, *Código Penal Anotado*, Volume III, 4.ª Edição, Reis dos Livros, pág. 1007.

VENÂNCIO, Pedro Dias, *Breve Introdução da Questão da Investigação e Meios de Prova na Criminalidade Informática*, Verbo Jurídico, Dezembro de 2006, pág. 11, e *Comentário das Leis Penais Extravagantes,* volume 1, 1.ª Edição, Universidade Católica Editora Novembro de 2010, pág. 511.

CENTRO
DE ESTUDOS
JUDICIÁRIOS

4.

O crime de abuso de cartão de garantia ou de crédito. Enquadramento jurídico, prática e gestão processual

Maria José Clara Sousa

CENTRO
DE ESTUDOS
JUDICIÁRIOS

4. O CRIME DE ABUSO DE CARTÃO DE GARANTIA OU DE CRÉDITO –ENQUADRAMENTO JURÍDICO, PRÁTICA E GESTÃO PROCESSUAL

Maria José Clara Sousa

I. Introdução

O presente trabalho versa sobre o crime de abuso de cartão de garantia ou de crédito previsto no artigo 225.º do Código Penal, que foi introduzido pela reforma de 1995, como forma de proteger o património da entidade emissora do cartão da utilização não autorizada de cartões de crédito e de garantia. Na excursão feita são revisitados os conceitos de cartão de crédito e de cartão de garantia, essenciais para a boa compreensão de espírito da norma e são apresentadas algumas das posições doutrinárias mais relevantes acerca do tipo legal em estudo. É feita referência a alguma jurisprudência resultante de pesquisa efetuada *on line* e uma análise a alguns inquéritos tramitados no Departamento de Investigação e Ação Penal de Santarém – Secção do Cartaxo. Para concluir, é feita uma análise crítica (mas que se pretende construtiva) acerca da aplicabilidade do artigo 225.º do Código Penal aos dias de hoje.

II. Objetivos

O trabalho elaborado tem por objetivo principal contribuir para a discussão acerca do âmbito de aplicação do artigo 225.º do Código Penal na atualidade, face ao aparecimento de novas realidades no contexto bancário, no que toca aos cartões bancários (recarregáveis, duais, conta ordenado) e à implementação de novos mecanismos de segurança para a utilização dos cartões (chip e pin).

O presente trabalho destina-se aos meus colegas Auditores de Justiça do 32.º Curso de Formação de Magistrados para os Tribunais Judiciais, vertente Magistratura do Ministério

Público, respetivos Coordenadores Regionais, Magistrados em funções junto dos Tribunais e ao Centro de Estudos Judiciários.

III. Resumo

A abordagem ao crime de abuso de cartão de garantia ou de crédito começa com uma alusão histórica aos motivos que estão na origem da criação deste artigo, conforme consta das atas da revisão do Código Penal de 1995 e menção às principais diferenças entre o artigo 225.º do Código Penal Português e o seu homónimo no Código Penal Alemão. Logo a seguir, é abordado o conceito de cartão de garantia de cheque e de cartão de crédito. São enunciadas as linhas mestras do tipo de crime e respetivo âmbito de aplicação, com base na doutrina mais relevante e segue-se para uma vertente mais prática, no capítulo da gestão processual. É feita uma breve referência à jurisprudência nacional, após o que se segue a apresentação de alguns inquéritos tramitados no DIAP de Santarém – Secção do Cartaxo. E por fim, é apresentada uma análise crítica seguida de conclusão.

1. O crime de abuso de cartão de garantia ou de crédito

1.1. A revisão do Código Penal de 1995

1.1.1. A diferença entre o crime de abuso de cartão de garantia ou de crédito no Código Penal Português e no Código Penal Alemão

O Decreto-Lei n.º 48/95, de 15 de março introduziu profundas alterações na configuração dos crimes patrimoniais do Código Penal[1], levando a cabo uma reforma que implementou o crime de abuso de cartão de garantia ou de crédito, inserindo-o no Capítulo III "Crimes contra o património em geral", do Título III "Crimes contra o património", do Código Penal Português.

A introdução do artigo 225.º no Código Penal teve como justificação, o facto de não existir previsão legal no Código Penal que punisse a utilização não autorizada de cartões de crédito ou de garantia, nem a sua utilização, para além do limite acordado.

Os elementos integradores da comissão da reforma do Código Penal entendiam que a prática de tais abusos, não se encontrava abrangida pelo crime de burla, pelo que, inspirados no Código Penal Alemão, introduziram o artigo 225.º no Código Penal. Apesar de ter sido inspirado na norma análoga do Código Penal Alemão, a redação do artigo sofreu algumas alterações, em relação a seu homónimo, já que, na versão alemã, o crime de abuso do uso do cartão de crédito só pode ser cometido por quem seja o titular legítimo do cartão[2],

[1] DANTAS, A. Leones, Jornadas de Direito Criminal Revisão do Código Penal, alterações ao Sistema Sancionatório e Parte Especial, Lisboa, 1998, Centro de Estudos Judiciários, pp. 516 a 518.
[2] Como ensina o insigne Professor Paulo Pinto de Albuquerque, em Comentário do Código Penal à luz da Constituição da República Portuguesa e da Convenção Europeia dos Direitos do Homem, Lisboa, 3.ª Edição, Universidade Católica Editora, 2015, p. 872, "O StGB alemão foi introduzido em 1986 (§ 266.º b) Missbrauch von

nomeadamente, por utilização para além dos limites de crédito concedido pela entidade bancária ou instituição financeira. Na norma do Código Penal Alemão só o detentor legítimo do cartão tem a possibilidade de levar o emitente a fazer um pagamento, em seu próprio prejuízo ou em prejuízo de terceiro. Na realidade, naquele código, o que está em causa é a violação, pelo detentor do cartão, dos termos do contrato celebrado e subjacente à emissão do cartão.[3]

Na previsão introduzida no Código Penal português o crime pode ser cometido por qualquer um.

1.1.2. Conceito de cartão de crédito e cartão de garantia e exclusões do âmbito de proteção da norma

Como refere Miguez Garcia, "o cartão de garantia (cartão de garantia de cheque) funciona como garantia de pagamento de um cheque até determinado montante[4], independentemente da existência de provisão[5].

Por sua vez o cartão de crédito é qualquer instrumento de pagamento, para uso eletrónico, ou não, que seja emitido por uma instituição de crédito ou por uma sociedade financeira que possibilite ao seu detentor a utilização de crédito outorgado pela emitente, em especial para a aquisição de bens ou serviços (Aviso do Banco de Portugal n.º 11/2001). O cartão desempenha, no fundo, uma dupla função de meio de pagamento e de concessão de crédito. O cartão de crédito integra-se num sistema que compreende três partes, a entidade emissora, geralmente um grupo de bancos, o titular do cartão de crédito e um universo de comerciantes aderentes.

Como refere Miguez Garcia[6], "quando se faz uma compra, a pessoa legitimada para usar o cartão (Visa, American Express, Master Card, entre outros) aceita pagar ao emitente assinando a fatura do comerciante, de onde constam os elementos do cartão e a indicação do

---

Schen-und Kraditkarten) e também no StG Suíço artigo 148.º Check-und Kreditkartenmissbrauch) introduzido em 1994, o crime foi tratado como sendo um crime específico, pois apenas pode ser cometido pelo titular do cartão."

[3] DANTAS, A. Leones (Jornadas de Direito Criminal Revisão do Código Penal, alterações ao Sistema Sancionatório e Parte Especial, Lisboa, 1998, Centro de Estudos Judiciários, p. 517) refere a este propósito que, "O alargamento do âmbito deste tipo introduzido pelo legislador português poderá ter desfigurado a consistência estrutural daquele tipo de crime e talvez de forma desnecessária. Com efeito, nas situações de utilização do cartão por quem dele não seja titular, recaia afinal o prejuízo sobre o emitente ou sobre terceiro, sempre estaríamos perante um normal crime de burla, em que a utilização do cartão mais não foi do que o instrumento da indução em erro do terceiro. Acresce que quer nos cartões de crédito, quer nos meros cartões de garantia a utilização do cartão envolve por norma outros ilícitos, nomeadamente a falsificação, seja do cheque garantido, seja do título de pagamento, nos cartões de crédito. As normas gerais relativas à burla e à falsificação de documentos estabeleciam a tutela penal suficiente para tal uso."

[4] J.M. Damião da Cunha, citando Joana de Vasconcelos, RDES, 1992, pp. 346 e ss. para definir "cartão de garantia (ou mais corretamente o cartão de garantia de cheques) não é em si mesmo um meio autónomo de pagamento, antes funciona em associação com outro meio de pagamento – o cheque – caucionando a sua utilização", in DIAS, Jorge de Figueiredo, Comentário Conimbricense do Código Penal, parte especial Tomo II, artigos 202.º a 307.º 1999, Coimbra Editora, p. 376.

[5] Barreiros, António José, Crimes contra o património, Lusíada, 1996, p. 216.

[6] O Direito penal passo a passo, p. 272, ob. cit.

quantitativo a pagar[7]. (…) Nos meses em que o cartão tenha sido utilizado é remetida ao titular, para conferência, a nota indicativa das compras efetuadas, seguindo-se o débito em conta. Para o comércio, uma transação com cartão de crédito é mais segura do que outras formas de pagamento, por ex.: o cheque, uma vez que o banco emissor aceita pagar ao vendedor ou prestador de serviços a fatura conferida, deduzindo-lhe o que é devido pelo serviço prestado (*discount rate*). Ao titular do cartão de crédito competirá efetuar pontualmente os pagamentos ou conseguir o correspondente crédito bancário suportando os juros e as despesas."

Estes dois tipos de cartões têm em comum é o fato de ambos concederem crédito, o cartão de garantia constitui uma garantia de pagamento de um cheque até um determinado montante, acabando desta forma por também conceder crédito ao seu titular.

É unânime na doutrina que, está excluído do âmbito de proteção do tipo incriminador da norma do 225.º do CP, os abusos cometidos através da utilização de um cartão de uso corrente, como um cartão de débito, que tenha uma finalidade diversa da do cartão de crédito propriamente dito.

Assim, o Professor J. M. Damião da Cunha defende que o cartão de débito, não está considerado no crime de abuso de cartão de garantia ou de crédito, por ser um cartão de pagamento imediato e encontrar-se associado a uma conta bancária que é imediatamente movimentada; pelo que o seu uso (ao contrário do cartão de crédito) está limitado pelas disponibilidades monetárias do titular.

Por sua vez, o Professor Pinto de Albuquerque, entende que não está, incluído no tipo de crime, o cartão de crédito e débito (chamado cartão dual) quando o cartão seja utilizado como cartão de débito, com um código secreto (o PIN) por exemplo, para levantamento de somas de dinheiro[8].

Discutível é a situação nos cartões de crédito baseados num sistema bilateral (relação exclusiva entre emitente e titular do cartão), que era a forma original do cartão de crédito, pelo qual, a entidade emitente concede crédito ao titular para cada um dos seus estabelecimentos filiais. Embora este tipo de cartão seja, correntemente, denominado de crédito, de facto, constitui uma forma exclusiva de concessão de crédito, em regra, a sua titularidade, não confere a possibilidade de levar o emitente a efetuar um pagamento, pelo que, não cabe no âmbito de proteção da norma do 225.º do Código Penal.

Problema especial é o da utilização abusiva de cartão em sistemas automatizados de pagamento. No âmbito da discussão sobre este crime na comissão revisora, Lopes Rocha manifestou dúvidas quanto à utilização do cartão de crédito como instrumento que possibilite levantamento de moeda através de sistema informatizado.

[7] Acrescenta o mesmo autor, que "O vendedor tem meios de verificar se o cartão é válido e se o titular dispõe de crédito suficiente para pagar o preço". – o comerciante segue determinados procedimentos de segurança fornecidos pelo banco, porém tais procedimentos, serão, quanto a nós, meramente preventivos.
[8] Contra este entendimento e defendendo uma aplicação analógica do tipo de crime previsto no artigo 225.º do Código Penal vide Maia Gonçalves 2007: 829, e Sá Pereira e Alexandra Lafayette, 2008: 559.

Dada a redação prevista neste artigo 225.º do CP, parece que este tipo de conduta não pode ser abrangida por este crime: por um lado, no caso de utilização por terceiro, a utilização abusiva não resulta apenas da posse do cartão, mas também do conhecimento do código secreto que permite movimentar a conta do titular (que é o único prejudicado); por outro lado, esta hipótese não é sequer configurável no caso de ser o próprio titular a utilizar o cartão, pois o levantamento está limitado, por princípio, ao montante disponível na conta bancária ou ao *plafond* do cartão de crédito[9].

Este caso de utilização abusiva de cartão em sistemas automatizados de pagamentos deve, portanto, ter um tratamento penal diferente dos que atrás ficaram referidos. Eventualmente, poderá ocorrer um crime de furto, ou um outro qualquer crime, referido à informática (previsto no âmbito da criminalidade informática)[10].

O tipo não inclui o cartão de moeda eletrónica que o titular carrega com um determinado valor em dinheiro eletrónico incorporado no cartão. Quando este cartão é subtraído ao seu titular e utlizado por um terceiro sem autorização, o terceiro é punido pelos crimes de furto e burla informática.

A par de outros autores, Miguez Garcia, entende que, "o código a mais da incriminação prevista no 225.º, equipara o cartão de garantia ou de crédito a moeda [artigo 267.º, n.º 1 alínea c)] pondo-os em paralelo com os bilhetes ou frações da lotaria nacional. Protege-se o cartão tanto da contrafação como da falsificação parcial e da sua posterior colocação em circulação, por aplicação dos arts. 262.º a 266.º. Quando o cartão, apesar de ser "de crédito", puder servir para outros fins, nomeadamente, levantamentos de quantias de conta provisionada, a respetiva utilização para subtração ilegítima de dinheiro não corresponderá a este crime, mas ao crime de furto ou de burla informática. A utilização ilícita pode também fazer-se por meio de cartões de crédito falsos nos POS "point of sale" ou "point of service", que pode ser uma loja num centro comercial ou qualquer outro lugar onde a transação ocorra, mas que algumas vezes designa o terminal de pagamento por sistema eletrónico num restaurante, num hotel, num casino, etc."

Aqui chegados importa analisar o tipo de crime.

[9] J. M. Damião da Cunha, in Comentário Conimbricense do Código Penal, p. 788: "Também no caso do Código Penal alemão, estes casos não são considerados, dado que o que o tipo legal pune é a utilização abusiva do cartão no quadro da sua função específica. No caso de levantamento de quantias não se trata de usar o cartão como garantia ou instrumento de crédito, mas como chave para acesso a uma conta". – salvo o devido respeito, não concordamos com esta posição porquanto, o levantamento efetuado com cartão de crédito pode ser um levantamento a crédito e disponibiliza, de imediato, ao seu titular, um determinado montante em dinheiro, independentemente da conta estar aprovisionada.

[10] Diferentemente, GONÇALVES, Maia, Código Penal Português, página 728, defende que "Em nosso entendimento, contrariamente ao que sustenta o Prof. J. M. Damião da Cunha, ob. cit., p. 379, a utilização abusiva de cartão em sistemas automatizados de pagamento pode ser subsumível à previsão deste artigo. É que o agente pode ter tido conhecimento do número secreto (PIN) que possibilita a utilização do cartão que está em seu poder, porque o descobriu, porque forçou o titular a revelá-lo, ou por qualquer outro processo. Não se trata de hipóteses académicas, mas de casos que têm sucedido com preocupante frequência, como tem sido revelados pelos meios de comunicação social, alguns já submetidos a julgamento, v.g. o chamado caso do banco multibanco."

1.1.3. Do Tipo de Crime

Escalpelizando a norma do artigo 225.º do Código Penal, chegamos aos seguintes **elementos do tipo objetivo** do crime:

– A utilização de um cartão de garantia de cheque ou de crédito (usar e ter na sua posse);

– Ter a possibilidade de levar o emitente a fazer um pagamento; e

– Provocar um prejuízo no emitente do cartão ou a terceiro.

Tendo em conta os elementos do tipo objetivo, concluímos que, o crime de abuso de cartão de crédito ou de garantia é um **crime comum**, já que pode ser praticado por qualquer pessoa[11].
Por outro lado, o facto do título da posse ser legítimo ou ilegítimo, é irrelevante, já que pode ser responsabilizado pelo abuso, quer o titular do cartão, quer qualquer outra pessoa que legítima ou ilegitimamente o possua.

O tipo subjetivo do crime implica **o dolo**, pelo menos, o **dolo** eventual[12], que tem de abranger o abuso e o prejuízo patrimonial. Não é necessário que o agente (em especial, quando esteja em causa um portador não titular) individualize a pessoa que vai sofrer o prejuízo patrimonial, já tudo depende das regras contratuais acordadas entre a entidade emissora e o titular do cartão.

Não é possível a punição a título de negligência, por força da interpretação conjugada dos art.º 225.º, n.º 1 e 13.º, ambos do Código Penal.

A **tentativa** é punível (art.º 225.º, n.º 1, do Código Penal), o que se justifica pelo facto de o regime de punição deste crime ser idêntico ao do crime de burla. Atendendo aos esquemas de segurança que são inerentes ao uso destes cartões será usual situações em que o agente possa usar o catão de crédito sem que, porém consiga obter o resultado (prejuízo patrimonial) o que configura uma tentativa impossível.

São também aplicáveis as regras da **desistência** relevante, nos termos dos artigos 24.º e 25.º do Código Penal.

O Professor José Manuel Damião da Cunha[13] concebe duas formas de **erro**, a primeira, erro sobre os elementos típicos do crime e a segunda, erro quanto à possibilidade de compensar ou regularizar um débito. No primeiro caso, se o agente, titular do cartão representar falsamente

[11] Em sentido contrário ver Barreiros, José António, Crimes contra o património, 1996, p. 214.
[12] Jorge Figueiredo Dias, Comentário Conimbricense do Código Penal, Parte Geral e Especial Tomo II, Coimbra Editora, p. 380.
[13] DIAS, Jorge de Figueiredo, Comentário Conimbricense do Código Penal, parte especial Tomo II, artigos 202.º a 307.º 1999, Coimbra Editora, p. 380, ob. cit.

a "cobertura" quanto ao pagamento, **faltará o elemento típico "abuso"**[14], enquanto que no erro quanto à possibilidade de compensar ou regularizar um débito eventualmente, faltará **o dolo** quanto ao prejuízo patrimonial (sendo certo, porém, que, neste caso, não serão suficientes para excluir o dolo, meras suposições ou expectativas vagas na regularização do débito).

No que concerne às **causas de justificação**, J. M. Damião da Cunha[15], entende serem de aplicar as regras gerais das causas de justificação, em especial o direito de necessidade. Deve, no entanto, ter-se presente a existência de acordo do titular do cartão para uma utilização por um não titular, e quanto às regras contratuais definidas. No caso de atuação em acordo com o titular do cartão, embora tal conduta possa ser contrária às regras do contrato de emissão do cartão, este acordo poderá ser penalmente relevante, conquanto não haja outro prejudicado com esse facto.

O mesmo autor, indica como **causas de exclusão da culpa**, a atuação com base num estado de necessidade desculpante.

Também será de considerar o **consentimento** do lesado, nos casos em que seja feito um levantamento com o consentimento da entidade emitente, mesmo depois de ultrapassado/atingido o *plafond* acordado, ou, nos casos em que o cartão sirva para garantir um valor diverso para mais relativamente ao acordado, igualmente com o consentimento da entidade bancária – tal sucede com clientes mais antigos, fidelizados, *private banking*.

Não há crime quando o titular do cartão consinta na utilização do cartão por terceira pessoa e esta o utilize de acordo com as instruções do titular.

O **bem jurídico protegido** pelo tipo de crime é o património da entidade emissora do cartão de crédito e pode ser também, o património do titular do cartão, nas situações em que o cartão seja utlizado por pessoa diferente do seu titular[16].

Desta forma, o **ofendido** pode ser a pessoa que suporta o prejuízo decorrente da utilização do cartão de crédito ou de garantia, normalmente a entidade que emitiu o cartão, mas também pode ser o titular do cartão, isto é da conta[17], nas situações em que o cartão é utilizado por terceiro.

De entre os casos de utilização do cartão por terceiro, temos as situações de utilização consentida e a não consentida[18]. As situações de utilização do cartão por pessoa diferente do

[14] Seria o caso de o agente, titular do cartão de crédito utilizar o cartão convicto que não tinha atingido o *plafond* acordado, ou utilizar o cartão convicto que a máquina ATM rejeitaria o cartão no caso da validade se encontrar ultrapassada, quer no caso de não ter *plafond* disponível
[15] DIAS, Jorge de Figueiredo, Comentário Conimbricense do Código Penal, parte especial Tomo II, artigos 202.º a 307.º 1999, Coimbra Editora, p. 380, ob. cit.
[16] Costa Andrade, Actas n.º 39.
[17] Vide Professor Costa Andrade, *in* Actas e Projecto da Comissão de Revisão, Código Penal, p. 451.
[18] Assim, entende Miguez Garcia *in* o Direito Penal passo a passo – crime contra o património, Coimbra, Almedina, 2011, p. 271, que, a utilização do cartão furtado encontra-se abrangida por este artigo remetendo para as atas, p. 450.

seu titular, não consentida, será sempre uma utilização ilegítima (furto, perda, com recurso à falsificação de assinatura na fatura, do cartão, no caso de este não estar assinado, e eventualmente, mera apresentação do cartão fazendo-se passar por outra pessoa).

Ora, neste casos a possibilidade de levar o emitente (por ex. Banco) a fazer um pagamento depende dos termos do contrato celebrado entre o emitente e o titular do cartão, na parte que define as condições em que este se compromete a comunicar o extravio. Daí não se poder concluir que existe sempre a possibilidade do emitente se ver obrigado a fazer o pagamento[19].

O crime de abuso de cartão de crédito ou de garantia é um **crime de dano**, quanto ao grau de lesão do bem jurídico protegido, e **um crime material** ou **de resultado** quanto à forma de consumação do ataque objeto da ação, que apenas se verifica com o empobrecimento a saída das coisas ou valores da esfera de disponibilidade fáctica do legítimo titular.

Portanto coloca-se a questão da imputação objetiva do resultado à ação.

O **agente do crime** pode ser qualquer pessoa, pois, o crime de abuso de cartão de garantia ou de crédito pode ser praticado por qualquer pessoa. Esta extensão justifica-se tendo em conta o bem jurídico protegido pelo tipo de crime e a forma como se consubstancia a infração (o abuso da garantia da entidade emissora)[20].

O **objeto da ação** são o cartão de garantia ou de crédito. O cartão há de ser emitido por uma instituição de crédito ou por uma sociedade financeira por forma a possibilitar ao seu detentor a utilização de crédito, nos termos constantes das condições do contrato outorgado.

A **ação típica** consiste em o agente abusar da possibilidade de levar o emitente a fazer um pagamento, por qualquer forma, inclusivamente, por transferência bancária.

O abuso afere-se relativamente à função dita normal que deve de ser desempenhada por um cartão de garantia ou de crédito e da qual possa emergir para a entidade que emite o cartão, ou mesmo para o seu titular (se pensarmos no crime cometido por alguém que não é titular do cartão) um dever de pagamento. O que em princípio, apenas será possível se o sistema estiver *off line*, o que sucede, sempre que há atualizações de software, que ocorrem, por norma, durante a noite, ou, quando é feito um pagamento durante um voo, sempre que ocorrer uma falha de comunicação e o sistema fique *off line*.

A qualificação da conduta como abusiva depende do possuidor do cartão ser, ou não, o titular do mesmo. Se for este o caso, o abuso significa violação das regras contratualmente impostas

[19] Leones Dantas (Jornadas de Direito Criminal, A revisão do Código Penal, alterações ao sistema sancionatório e Parte especial, Lisboa, 1998, Centro de Estudos Judiciários, pp. 517-518), conforme referido, defende que "nas situação de utilização do cartão por quem dele não seja titular, recaia afinal o prejuízo sobre o emitente ou sobre terceiro, sempre estaríamos perante um normal crime de burla, em que a utilização do cartão mais não foi do que o instrumento da indução em erro. Acresce que quer nos cartões de crédito, quer os meros cartões de garantia a utilização do cartão envolve por norma outros ilícitos, nomeadamente a falsificação, seja do cheque garantido, seja do título de pagamento, nos cartões de crédito. As normas gerais relativas à burla e à falsificação de documentos estabeleciam tutela penal suficiente para tal uso."
[20] Vide Miguez Garcia, em Código Penal - parte geral e especial, p. 1001.

aquando da emissão do cartão e aceites pelo seu titular – a chamada relação interna. Pode dar-se também quando o titular do cartão atua em relação a um terceiro (um estabelecimento comercial, por exemplo) violando as regras contratuais do emitente e criando um dever de pagamento a esta entidade bancária. Pode dar-se abuso em virtude do titular ultrapassar o valor do crédito concedido, ou, o prazo de validade ter cessado[21]. Assim pune-se a utilização abusiva do cartão de garantia ou de crédito por quem dele seja titular legítimo, mas também a utilização por quem não seja titular.[22] No caso do abuso levado a cabo por um terceiro não titular do cartão, a coberto, por exemplo de relações familiares, a apreciação do abuso deve seguir as mesmas regras a que o titular do cartão está sujeito[23].

O crime fica consumado com a saída do dinheiro ou disponibilidade financeira do património do lesado.

1.2. Natureza do crime

O crime de abuso de cartão de garantia ou de crédito reveste natureza **semi-pública** e **particular** nos casos do artigo 207.º do Código Penal.

A remissão feita para o artigo 207.º do Código Penal justifica-se quando a vítima seja o titular do cartão de crédito ou de garantia, mas parece que deve também ser aplicável o mesmo princípio, quando o lesado seja a entidade emitente, ou, eventualmente, o comerciante, se o agente tiver uma das qualidades previstas na alínea a) do artigo 207.º do Código Penal (cônjuge, ascendente, descendente, adotante, adotado, parente ou afim até ao 2.º grau da vítima, ou com ela viver em condições análogas às dos cônjuges), caso o titular assuma, ou seja, obrigado contratualmente, a assumir, a responsabilidade pelo pagamento. Esta solução é compreensível, uma vez que, tal como já se disse, deverá tratar-se de situações em que o terceiro (embora ligado ao titular, por laço familiar ou análogo) atua com base numa relação de confiança; esta situação corresponde a uma violação das obrigações contratuais – a não

[21] DANTAS, A. Leones, p. 516, referia que "Pune-se a utilização abusiva do cartão de garantia ou de crédito por quem dele seja titular legítimo, mas também a utilização por que não seja titular. Não se mostra contudo, fácil determinar o conteúdo efetivo da previsão desta norma. Na verdade, a emissão de um cartão de garantia ou de crédito cria a possibilidade em abstrato levar o emitente a fazer um pagamento, pelo que deixa de fazer qualquer sentido fazer-se apelo a tal possibilidade na estrutura do tipo, uma vez que ela é parte integrante do contrato que está subjacente à emissão daquele tipo de cartões. Por outro lado, deixa também de fazer sentido fazer-se apelo ao abuso dessa possibilidade por quem não seja titular legítimo do cartão, porque relativamente a esse tipo de detentores, qualquer uso é ilegítimo, nunca se colocando a questão do uso legítimo daquela possibilidade. Acresce que relativamente aos cartões detidos por quem não seja titular, a possibilidade de levar o emitente a fazer o pagamento depende dos termos do contrato, celebrado entre o emitente e o titular do cartão que define as condições em que este se obriga a comunicar o extravio. Não se pode, assim, afirmar que exista sempre a possibilidade de o emitente se ver obrigado a fazer um pagamento, pelo que existirão situações de utilização abusiva do cartão já não ter, de facto, tal potencialidade. As dificuldades de interpretação desta norma têm origem no circunstancialismo que rodeou a sua aprovação no âmbito da comissão revisora e fundamentalmente das suas fontes."

[22] A. Leones Dantas, ob. cit., p. 516.

[23] Vide neste sentido, Dias, Jorge Figueiredo, *in* Comentário Conimbricense do Código Penal, página 378: "Embora tal prática possa constituir uma violação às regras do contrato de emissão, ela é, para efeitos penais irrelevante, na medida em que, por um lado dificilmente se pode falar em abuso, e, por outro, não há de facto prejuízo patrimonial. Deve, no entanto, referir-se que, neste caso, pode eventualmente questionar-se se não se verificará antes um crime de infidelidade. Em regra, porém, deverá verificar-se a apresentação do presente tipo legal, exceto, eventualmente, se se verificar uma atuação no interesse do titular do cartão."

cedência de cartão a qualquer outra pessoa – que tem como sanção ser o próprio titular a suportar as quantias em dívida. No caso da alínea b) deste artigo 207.º (valor diminuto) parece que o lesado pode ser qualquer uma das entidades acima referidas.

O crime tem dois escalões de qualificação conforme o prejuízo for de valor elevado ou de valor consideravelmente elevado, e nesses casos, o crime qualificado assume natureza de crime **público.**

Sendo um crime comum, é possível o cometimento do crime em conjunto por vários agentes e assim, será aplicável o regime da **comparticipação**. São os casos do crime ser cometido pelo titular do cartão de crédito ou de garantia e um terceiro com ele conluiado, cometimento do crime em conjunto com o comerciante com intenção de defraudar o património da entidade emissora do cartão, e existência de mais do que um cartão para uma mesma conta em que os diversos titulares agem mancomunados.

1.3. Relação com outros crimes – o concurso

O concurso de normas consiste na subsunção formal dos factos a uma pluralidade de tipos criminais, sendo a aplicação de um desses tipos incriminadores suficiente para punir os factos.

Para Paulo Pinto de Albuquerque e M. Miguez Garcia existe uma relação de concurso aparente (especialidade) entre o crime de abuso de cartão de garantia ou de crédito e os crimes de burla e burla informática.[24]

Já para J. M. Damião Cunha[25] "O problema fundamental, quanto ao concurso de crimes será a relação que se verifica com o crime de burla p. e p. no artigo 217.º do Código Penal sobretudo atendendo a que existirão muitas situações em que se pode verificar o cometimento dos dois crimes. A razão para a criação deste crime, está diretamente ligada à dificuldade em afirmar o crime de burla, face a factos, em que a conduta mereceria exatamente o mesmo tratamento. Uma vez que a redação típica do artigo 225.º do Código Penal é menos exigente do que a do crime de burla (que foi precisamente uma das razões para a criação deste mesmo crime), parece claro – a despeito da identidade do regime punitivo – que toda a conduta abusiva de utilização de cartões de crédito ou de garantia deve, em princípio, ser subsumida ao presente artigo 225.º que, neste sentido, constitui uma *lex specialis* em relação ao crime de burla."

Por esta via se resolvem problemas como os da relevância do erro ou fraude ou da conexão entre a conduta fraudulenta e o prejuízo patrimonial.

[24] ROCHA, Manuel António Lopes, Soluções de Neocriminalização, p. 97, "(…) um dos meios típicos para a prática da burla informática é a utilização não autorizada de dados (…) que para Romeo Casabona abarca, entre outras condutas, a utilização de cartões de crédito em caixas automáticas, tanto por um terceiro contra a vontade do titular, como a utilização abusiva por parte deste, ou seja, ultrapassando o limite da disponibilidade monetária concedida (…) Poderão verificar-se, por isso, situações reais de concurso de normas, a resolver eventualmente pelos critérios do concurso legal ou aparente."

[25] *In* DIAS, Jorge de Figueiredo, Comentário Conimbricense do Código Penal, parte especial, Tomo II, artigos 202.º a 307.º 1999, Coimbra Editora, p. 381.

Não cabe, evidentemente, dentro do âmbito do presente normativo toda e qualquer conduta, que possa causar prejuízo patrimonial para um terceiro, assente numa utilização abusiva de um cartão, mas que não resulte da específica função do cartão. Nestes casos, a eventual punibilidade a subsistir, deverá verificar-se pelo crime de burla.

Também pode haver concurso com o crime de emissão de cheque sem provisão (artigo 11.º do Decreto-Lei n.º 454/91, de 28 de Dezembro), crime também sujeito ao regime punitivo do crime de burla. Neste caso, importante é a sua ligação com o abuso de cartão de garantia de cheques, naturalmente, quando praticado pelo titular do cartão. Haverá, assim, que distinguir entre a emissão de cheque sem cobertura, nomeadamente a que ultrapassa o valor da garantia assumida pelo banco (um caso de emissão de cheque sem cobertura) e a emissão de cheque com valor, em princípio, dentro da garantia assumida pelo banco, mas tendo esta sido já ultrapassada (só nesta segunda hipótese se pode referir o crime de abuso de cartão de garantia).

Pode ainda eventualmente verificar-se concurso com crime de falsificação ou uso de documento alheio, sempre que o terceiro, não titular do cartão, ao utilizar o cartão de crédito assine a fatura ou o próprio cartão.

1.4. Punição

O crime de abuso de cartão de crédito ou de garantia é punido, tal como o crime de burla com pena de prisão até 3 anos ou com pena de multa.

Assim, se o valor do prejuízo for de **valor elevado** o crime tem como punição o limite máximo de 5 anos e a multa um limite de 600 dias [n.º 5, alínea a)].

A noção de **valor elevado** é dada pela alínea a) do art.º 202.º do Código Penal, que o define como o valor que excede 50 unidades de conta no momento da prática do facto, ou seja 5.100 euros [n.º 5, alínea b)].

Caso o prejuízo seja de valor **consideravelmente elevado** o agente pode ser punido com uma pena de prisão de 2 a 8 anos, não lhe podendo ser aplicada uma simples pena de multa.

A noção de **valor consideravelmente** elevado é dada pela alínea b) do artigo 202.º do Código Penal, que refere que é aquele que exceder 200 unidades de conta avaliada no momento, ou seja, 20.400 euros.

São aplicáveis a este crime as regras especiais do artigo 206.º do Código Penal quanto à reparação.

1.5. Direito de queixa

No caso em que o crime depender de **queixa** (artigo 49.º do CPP) tem legitimidade para apresentar queixa o ofendido, considerando-se como tal, o titular dos interesses que a lei quis proteger com a incriminação, nos termos do disposto no artigo 113.º do Código Penal.

Desta forma, **tem legitimidade para apresentar queixa** a pessoa prejudicada pelo abuso do cartão, que pode ser a entidade bancária, o titular do cartão (caso lhe tenha sido furtado ou utilizado por terceiro) ou o comerciante.
O **direito de queixa** extingue-se decorridos seis meses contar da data em que o titular tiver tido conhecimento do facto e dos seus autores, ou, a partir da morte do ofendido, ou da data em que ele se tiver tornado incapaz, conforme disposto no artigo 115.º do Código Penal.

O direito de queixa não poderá ser exercido se o seu titular a ele tiver expressamente renunciado ou se tiver praticado factos de onde seja possível retirar que renunciou à mesma.

Sempre que se verificar alguma das circunstâncias previstas no artigo 207.º do Código Penal, o crime dependerá **de acusação particular**, e revestindo natureza de crime particular, nesse caso é necessário que, os ofendidos se queixem, se constituam assistentes e deduzam acusação particular, no prazo legal (artigo 68.º, n.º 2, 246.º, n.º 4, do Código de Processo Penal).

Nas hipóteses em que o crime revesta natureza semi-pública e particular[26],o crime admite **desistência** até à publicação da sentença em primeira instância, desde que, o arguido não se oponha, devendo ser notificado nos termos e para os efeitos do disposto no artigo 51.º, n.º 3, do Código de Processo Penal, conforme se retira do disposto nos artigos 116.º e 117.º do Código Penal.

Nesses casos, se o conhecimento da desistência tiver lugar durante o inquérito, deverá ser o Ministério Público a homologar a desistência apresentada, conforme se infere do artigo 51.º, n.º 2, do Código de Processo Penal.

1.6. Prescrição

O procedimento criminal extingue-se, por prescrição, quando desde o seu início e ressalvado o tempo de suspensão, tiver de corrido o prazo normal de prescrição acrescido de metade (artigo 121.º, n.º 3, do Código Penal).

Para o crime em apreço, o prazo de prescrição previsto é de, cinco anos sobre a prática do crime, no caso do n.º 1, do artigo 225.º do Código Penal e de dez anos sobre a prática do crime, no caso do n.º 5 alíneas a) e b) do artigo 225.º do Código Penal, conforme previsto no artigo 113.º do Código Penal.

[26] Conforme estatuição do n.º 3 do art.º 225.º CP "o procedimento criminal depende de queixa". Em determinado circunstancialismo pode mesmo exigir-se acusação particular para desencadear procedimento criminal, nomeadamente, para os casos em que o abuso tem um valor diminuto, um valor inferior à unidade de conta avaliada ao momento da prática do facto lesivo.

1.7. Gestão Processual

1.7.1. O Inquérito

Compete especialmente ao Ministério Público exercer a ação penal orientada pelo princípio da legalidade, dirigir a investigação criminal, ainda quando realizada por outras entidades; e promover e realizar ações de prevenção criminal, tudo nos termos do disposto no artigo 3.º, n.º 1, alíneas c), h) e i), do Estatuto do Ministério Público. A direção do inquérito cabe ao Ministério Público, nos termos do disposto nos artigos 53.º, n.º 2, e artigo 263.º, n.º 1, do CPP.

Assim, o Ministério Público tem legitimidade para promover o processo penal com as restrições constantes dos artigos 49.º a 52.º do Código Penal.

Sendo o **crime público**, bastará, para que o Ministério Público possa despoletar a investigação que seja feita uma denúncia (artigo 262.º, n.º 2, CPP).

No caso de ser **semi-público** é preciso que o ofendido se queixe, artigo 49.º do CPP. Caso o crime revista natureza **particular**, findo o inquérito, o Ministério Público notificará o assistente para que este deduza, em 10 dias, acusação particular, indicando se, no seu entender, foram ou não colhidos indícios suficientes da verificação de crime e bem assim de quem foram os seus agentes. O Ministério Público poderá, nos cinco dias posteriores, à apresentação da acusação particular, acusar pelos mesmos factos, por parte deles ou por outros que não importem uma alteração substancial daqueles.

O **inquérito** compreende o conjunto de diligências que visam investigar a existência de um crime, determinar os seus agentes e a responsabilização deles e descobrir e recolher as provas em ordem à decisão sobre a acusação.

A competência do Ministério Público para o inquérito afere-se, nos termos das disposições conjugadas dos artigos 264.º do CPP e 7.º do Código Penal. Deste modo, o facto considera-se praticado, tanto no lugar em que, total ou parcialmente e sob qualquer forma de comparticipação, o agente atuou ou deveria de ter atuado, como aquele em que, o resultado típico compreendido no elemento do tipo se tiver produzido. No caso do crime previsto no artigo 225.º do Código Penal, é competente o Ministério Público do local onde se consumar o crime[27].

Assim é competente para o inquérito, o Ministério Público do local do cometimento do crime (loja ou ATM onde tiver sido utilizado o cartão) ou, desconhecendo-se, o do lugar onde o

[27] A Procuradora-Geral Distrital foi chamada a intervir na resolução de um conflito de competência opondo Magistrados do DIAP de Lisboa ao da Comarca do Funchal, no inquérito com o NUIPC 561/11.9 S7LSB, no qual estavam em causa atos suscetíveis de integrar a prática de um crime de burla informática, p. e p. no artigo 221.º do Código Penal, e, dependendo da forma de atuação do agente, de um crime de falsificação de moeda, p. e p. pelos artigos 262.º, n.º 1, e 267,º, n.º 1, al. c), do mesmo diploma, ou um crime de acesso ilegítimo, p. e p. no artigo 6.º da Lei 109/2009, de 15/09 (Lei do Cibercrime). Face ao desconhecimento do local onde o agente tinha atuado, atribuiu-se a competência ao Ministério Público do local onde se situava a agência da conta bancária fraudulentamente debitada, pese embora a queixa tenha sido feita em Lisboa; para consulta em http://www.pgdlisboa.pt/docpgd/doc_mostra_doc.php?nid=165&doc=files/doc_0165.html.

resultado se tiver produzido (balcão onde esteja sedeada a conta bancária onde se deu o empobrecimento). O critério supletivo quando não é conhecido o local onde o crime foi cometido, é o do local onde primeiro tiver havido notícia do crime. Sempre sem prejuízo de, em caso de urgência ou perigo na demora, o Ministério Público poder proceder aos atos de inquérito que julgue necessários (detenção, interrogatório, aquisição e conservação dos meios de prova), nos termos do artigo 264.º, n.º 4, do C.P.P.

Recebida a notícia do crime ou a queixa, o Ministério Público, se não for caso de arquivamento nos termos do artigo 277.º, n.º 1 ou 2, do C.P.P., dará início ao inquérito, artigo 267.º, do C.P.P. A investigação pode ser delegada em órgão de polícia criminal competente, nomeadamente, na Guarda Nacional Republicana ou Policia de Segurança Pública, nos termos do disposto no artigo 270.º do C.P.P. e do artigo 6.º da Lei n.º 49/2008, de 27 de agosto.

Deve o Ministério Público recolher todos os elementos probatórios possíveis e utilizando todos os meios de prova, com as limitações decorrentes, do artigo 125.º e seguintes do C.P.P. e do artigo 32.º, n.º 8, da Constituição.

O Ministério Público deverá oficiar, com a maior brevidade possível, ao Banco emissor do cartão de crédito, solicitando o envio da listagem de todos os pagamentos efetuados com o cartão de crédito identificado, no período temporal em investigação, com menção das entidades a quem foram efetuados pagamentos com o cartão de crédito e ou de garantia. Deverá, ainda, ser solicitada cópia das fichas de assinatura da conta bancária associada ao cartão de crédito, respetivo extrato bancário. No mesmo ofício, o Ministério Público solicita que o Banco esclareça se, para utilização do cartão em apreço é ou não necessário um código pin, e se existem outros cartões associados à mesma conta bancária.

Tal solicitação feita por despacho do Ministério Público, deverá fazer apelo ao artigo 79.º[28] do Regime Geral das Instituições de Crédito e Sociedade Financeiras (Decreto Lei n.º 298/92, de 31 de Dezembro) que tem sob epígrafe, "exceções ao dever de segredo", e que prevê, na alínea e) do seu n.º 2 que, "os factos e elementos cobertos pelo dever de segredo só podem ser revelados: às autoridades judiciárias, no âmbito de um processo penal".

Nos termos do disposto no artigo 1.º, alínea b), do Código de Processo Penal, o Ministério Público é uma "autoridade judiciária", devendo por isso, a informação solicitada, ser-lhe revelada.

Caso o Ministério Público se aperceba que, foram efetuados carregamentos de telemóvel com o cartão de crédito, deve oficiar a operadora móvel, solicitando, que informe, designadamente, a identidade(s) do(s) utilizador do número de telemóvel detetado no

[28] Com a alteração legislativa operada pela Lei n.º 36/2010, de 2 de setembro, que alterou o artigo 79.º, n.º 2, al. d) do Decreto-Lei n.º 298/92, de 31 de dezembro, deixou de se justificar a intervenção do Tribunal da Relação para efeitos de quebra/levantamento do segredo bancário, uma vez que os Bancos ficaram desobrigados do dever do segredo em relação aos elementos que lhe forem solicitados pelas autoridades judiciárias, no âmbito de um qualquer processo penal, seja qual for o crime que se investigue, ac, Tribunal da Relação de Évora, processo 824/10.0TAABF-A.E1, relator Desembargador Fernando Ribeiro Cardoso, disponível em www.dgsi.pt.

carregamento, no hiato temporal em causa, e bem assim, a identificação de todos os IMEIs onde aquele cartão operou, e quais os cartões que ainda operam no mesmos IMEIs.

Uma vez que a informação solicitada constitui um **dado de base**[29], é da competência do Ministério Público, não carecendo da intervenção do Juiz de Instrução.

Durante o inquérito o Ministério Público pode sempre chegar à conclusão que está em causa a prática de um tipo de crime diferente do inicialmente investigado, devendo ponderar a eventual necessidade de conservar dados, fazendo-o ao abrigo do disposto no artigo 12.º, da Lei do Cibercrime, aplicável em virtude do artigo 11.º, n.º 1, alínea b), da mesma lei.

Em simultâneo e tendo sempre presente a necessidade de imprimir carácter urgente aos pedidos a efetuar, importará averiguar se, no local onde há notícia que o cartão tenha sido utilizado, ou nas suas imediações, existem câmaras de videovigilância[30] que permitam a recolha de imagens com o intuito de identificar o autor da prática dos factos.

Nesse sentido, deverá o órgão de polícia criminal competente a quem tenha sido delegada a investigação, oficiar o proprietário da câmara para que, conserve as imagens e entregue cópia em prazo a estipulado.

Importa ainda, averiguar no mais curto espaço de tempo, junto dos comerciantes que se tenha logrado identificar e aos quais foram adquiridos produtos pagos com o cartão de crédito, se, por hipótese, foram emitidas faturas, e em caso afirmativo solicitar cópia das mesmas.

Em paralelo, poderá ser feito um interrogatório complementar do ofendido em ordem a esclarecer algum elemento necessário e/ou obter mais informações que permitam investigar noutras direções.

A investigação apresenta algumas dificuldades sempre que, o cartão de crédito tenha sido cedido ao terceiro, e este aproveitando-se da posse do mesmo, o utiliza em seu próprio benefício. Será o caso de A que cede o seu cartão de crédito a B, com instruções específicas que este deverá adquirir um determinado bem C, já que A não tem tempo para o fazer. B aproveitando-se da possibilidade de ter o cartão de crédito de A, adquire não só o bem C mas também o bem D, em violação das instruções dadas por A.

[29] Os dados de base são os que dizem respeito à identificação dos clientes de uma determinada operadora, o nome, morada, essenciais para a celebração do contrato, e que incluem os números de telefone, os números do cartão SIM e o IMEI, e estão previstos no artigo 14.º da Lei do Cibercrime e são da competência da autoridade judiciária, neste caso, atenta a fase de inquérito, será o Ministério Público a autoridade competente.

[30] Não constitui crime ("gravações e fotografias ilícitas", cfr. art.º 199.º, do C. Penal) a obtenção de imagens, mesmo sem consentimento do visado, sempre que exista justa causa para tal procedimento, designadamente quando sejam enquadradas em lugares públicos, visem a proteção de interesses públicos, ou hajam ocorrido publicamente. A obtenção de fotogramas através do sistema de videovigilância existente num estabelecimento comercial, para proteção dos seus bens e da integridade física de quem aí se encontre, mesmo que se desconheça se esse sistema foi comunicado à CNPD, não corresponde a qualquer método proibitivo de prova, desde que exista uma justa causa para a sua obtenção, como é o caso de documentar a prática de uma infração criminal, e não diga respeito ao "núcleo duro da vida privada" da pessoa visionada", *in* Ac. do Tribunal da Relação de Coimbra, de 10.10.2012, relator desembargador Elisa Sales, Proc. 19/11.6TAPBL.C1, disponível em www.dgsi.pt. Ver também no mesmo sentido Ac. STJ de 28.09.2011, Processo 22/09.6YGLSB.S2, relator Conselheiro Santos Cabral, disponível em www.dgsi.pt.

Aqui, a investigação passará, necessariamente, por ouvir o ofendido e o suspeito, na recolha de outros elementos junto do banco e dos comerciantes (extratos, talões assinados, imagens de câmaras de videovigilância, faturas assinadas), para, depois do confronto dos elementos recolhidos e com base nas regras da experiência e da normalidade, analisar se foram recolhidos indícios suficientes de se ter verificado o crime e de quem foi o seu agente, para acusar, ou pelo contrário, arquivar o inquérito (artigo 283.º, n.º 1 e 2.º, 277.º, n.º 1 e 2, do Código de Processo Penal).

Verificando-se algumas das circunstância do artigo 58.º do C.P.P., e desde que não ponha em risco a investigação ou os próprios direitos de defesa do suspeito, o Ministério Público procede à constituição de arguido com obediência das formalidades legais previstas nos artigos 58.º, n.ºs 2, 3 e 4, 61.º, e 64.º n.ºs 2, 3 e 4, do C.P.P. devendo o arguido ser interrogado nessa mesma qualidade, cfr. artigos 144-.º e 272.º do C.P.P.

A aplicação das chamadas **medidas de consenso e de oportunidade** deverão de ser ponderadas. O Ministério Público deverá de ponderar a aplicação do instituto da suspensão provisória do processo[31] previsto no artigo 281.º do C.P.P. ou, ou não sendo este aplicável, fazer uso do processo sumaríssimo regulado pelo artigo 392.º do C.P.P.[32].

O Ministério Público, na condução do inquérito deverá ter presente os prazos previstos nos artigos 276.º do CPP.

Findo o inquérito, o Ministério Público, se considerar que foram recolhidos indícios suficientes, de se ter verificado crime e de quem foi o seu agente, deduz acusação sob a forma de processo sumário, se, se verificarem os requisitos do artigo 381.º e seguintes do C.P.P. ou abreviado, nos termos do artigo 391.ºA e seguintes do mesmo diploma. Não sendo possível aplicar nenhuma das referidas formas processuais, o Ministério Público deduz acusação sob a forma de processo comum, artigo 283.º, n.º 1, do C.P.P.

No que concerne à suscetibilidade de aplicação de **medidas de coação**, atentas as molduras penais abstratamente aplicáveis no crime em estudo, além do termo de identidade e residência podem ser aplicadas medidas de coação como a suspensão do exercício de profissão, função, atividade e de direitos (art.º 199.º do C.P.P.).

Deste modo, quando a factualidade apurada consubstancie uma das hipóteses previstas no n.º 5 do artigo 225.º do CP, atenta a moldura penal abstratamente aplicável ser superior a três anos de prisão, e caso se verifiquem os pressupostos do disposto no artigo 204.º do C.P.P., designadamente, fuga ou perigo de fuga, perigo de perturbação do decurso do inquérito ou da instrução do processo, nomeadamente, perigo para a aquisição, conservação ou veracidade da prova, ou perigo de continuação da atividade criminosa ou perturbação da ordem e tranquilidade públicas, é admissível a aplicação da medida de coação de proibição e imposição de condutas, obrigação de permanência na habitação e

[31] Diretiva n.º 1/2014, da Procuradoria-Geral da República, Diretiva n.º 1/2015, da Procuradoria-Geral da República e Instrução n.º 1/2018, da Procuradoria-Geral da República.
[32] Diretiva n.º 1/2016, da Procuradoria-Geral da República.

prisão preventiva, atento o disposto no artigo 200.º, 201.º e 202.º, n.º 1, alínea a), do C.P.P.

1.8. Jurisprudência

O acórdão do Supremo Tribunal de Justiça, de 12.04.2008, que teve como relator o Juiz Conselheiro Pires da Graça, proferido no âmbito do processo 8P3552, disponível para consulta em www.dgsi.pt.

Neste acórdão, "A arguida foi julgada pelo 1.º Juízo Criminal do Tribunal Judicial de e condenada pela prática de vários crimes, entre eles, um crime de abuso de cartão de crédito, previsto e punível pelo artigo 225.º, n.º 1, do Código Penal." (…) "Da factualidade apurada resulta que, a arguida, aproveitando-se do facto de DD, proprietária daquele estabelecimento, estar a atender clientes, retirou da parte interior do balcão a carteira pertença daquela, (…) continha um porta-moedas, (…), bem como os seus documentos pessoais, designadamente o Bilhete de Identidade, a carta de condução, o cartão de contribuinte, (…) ainda um cartão Multibanco do BPN, um cartão de crédito Visa Classic do Banco Santander, com o número (…). 2. Ato contínuo, a arguida abandonou o local, levando com ela a referida carteira e o respetivo conteúdo- 3. Uma vez na posse do referido cartão de crédito do Banco Santander pertencente à ofendida DD, a arguida decidiu utilizá-lo com o fim de adquirir o maior número possível de produtos nos estabelecimentos comerciais da cidade. 4. (…) no estabelecimento de ourivesaria TRIOURO, que estava aberto ao público, onde efetuou pelas 11h28 compras no valor de € 680, procedendo ao respetivo pagamento com o aludido cartão de crédito, apondo no final uma rubrica pelo seu punho no talão de compra, como se fosse a titular daquele cartão. 5. De seguida, e ainda na mesma Rua, a arguida entrou no estabelecimento de sapataria CHARLES, também aberto ao público, onde, pelas 11h56, foi atendida pela funcionária XX e onde efetuou compras no valor de € 146,16, após o que procedeu ao respetivo pagamento com o mesmo cartão de crédito do Banco Santander (pertencente a DD), apondo no final uma rubrica pelo seu punho no talão de compra, como se fosse a titular daquele cartão. (…).

A arguida recorreu alegando a existência de um concurso, porém não logrou obter provimento.

Sumário: "I - O Assento n.º 8/2000, de 04-05-2000 (DR 119, Série I-A, de 23-05-2000), fixou jurisprudência no sentido de que «No caso de a conduta do agente preencher as previsões de falsificação e de burla do artigo 256.º, n.º 1, alínea a), e do artigo 217.º, n.º 1, respetivamente, do Código Penal, revisto pelo Decreto-Lei n.º 48/95, de 15 de Março, verifica-se concurso real ou efetivo de crimes.» II - Em tal Assento se considerou: "Parece não suscitar dúvidas de que continuam a ser diferentes os bens jurídicos tutelados pelos artigos 217.º, n.º 1, e 256.º, n.º 1, do Código Penal de 1995. Como se escreveu já no Acórdão deste Supremo de 16 de Junho de 1999, processo n.º 577/99: «Ora, nem no Código Penal de 1982 nem no de 1995 existe qualquer disposição que ressalve o concurso da burla com a falsificação (enquanto meio de realização daquela) do regime geral estatuído no artigo 30.º: 'O número de crimes determina-se pelo número de tipos de crime efetivamente cometidos, ou

pelo número de vezes que o mesmo tipo de crime for preenchido pela conduta do agente.' Logo, sendo distintos os bens jurídicos tutelados pelos tipos legais de crime de burla (o património) e de falsificação de documento (que não será tanto a fé pública dos documentos [...] III - Não havendo razões para alterar tal posição, à mesma se adere, sendo que o mesmo tipo de argumentação é válido para o crime de abuso de cartão de crédito e falsificação, quanto à operação relativa à ativação do cartão e consequente e necessária assinatura do respetivo talão. No que concerne ao crime de furto (do cartão e não só), ele é autónomo em relação aos crimes que se lhe seguem de falsificação e abuso de cartão de crédito, porque relativo a conduta diversa que protege também bem jurídico diferente, no caso a propriedade (e posse), pelo que não pode deixar de se considerar que há concurso real entre os três aludidos crimes. IV - As utilizações abusivas e ilícitas, por terceiro alheio à titularidade do cartão de crédito, dependentes de resolução e ações posteriores ao furto da carteira, assumem autonomia em relação a este. V - Do artigo 206.º, n.º 2, do CP resulta que a pena é especialmente atenuada quando a coisa furtada ou ilegitimamente apropriada for restituída, ou tiver lugar a reparação integral do prejuízo causado, sem dano ilegítimo de terceiro, até ao início da audiência de julgamento em 1.ª instância, e, nos termos do n.º 3, se a restituição ou a reparação forem parciais, a pena pode ser especialmente atenuada."

*

Acórdão do Tribunal da Relação do Porto, de 17.01.2001. proferido no âmbito do processo 10659, que teve por relator o Juiz Desembargador Marques Pereira, disponível para consulta em www.dgsi.pt.

Neste acórdão, Tribunal Judicial da comarca de Vale de Cambra, o Ministério Público requereu o julgamento, em processo comum, com intervenção do tribunal singular, fazendo uso do disposto no artigo 16.º, n.º 3, do CPP, da arguida Lígia..., imputando-lhe a prática, como autora material, de um crime de furto simples p. e p. no artigo 203.º, n.º 1 e de um crime de abuso de cartão de crédito p. e p. no artigo 225.º, n.º 1, ambos do C. Penal. Resultou provado que, "De modo que não foi possível apurar, a arguida apoderou-se da carteira da ofendida, contendo, para além de documentos pessoais como o BI, carta de condução-o, cartão de contribuinte, cartão de beneficiária da SS, cartão de eleitora, cartão jovem, ainda um cartão multibanco emitido pela CGD e um cartão "visa universo", tudo pertencente à ofendida. (…) 4)Apoderou-se dessa carteira, bem como do seu conteúdo, sem a autorização e contra a vontade da ofendida. 5)Uma vez na posse daqueles documentos e cartão de crédito, a arguida decidiu usar este para seu benefício pessoal. 6)E assim, cerca das 13h, do dia 14 de Fevereiro de 1999, a arguida utilizou o cartão "visa universo" pertencente à ofendida, para pagar a quantia de 670$00 de compras, e para retirar 15.000$00 da caixa. 7) O que fez numa das caixas daquele hipermercado, onde a arguida estava a operar, sem a autorização e contra a vontade da ofendida. 8)Por essa via, a arguida viu o seu património acrescido daquele montante, no qual a ofendida ficou prejudicada. 9)Somente alguns dias mais tarde, 18 de Fevereiro, é que a ofendida veio a apurar da transação efetuada com o referido cartão, bem como a identidade do agente que a efetuara. 10) Esta, confrontada com tal facto, devolveu nessa data, à ofendida a carteira e todos os documentos, bem como lhe entregou a quantia de 16.000$00 para a ressarcir." Veio a arguido recorrer com base em erro notório na apreciação da prova, muito embora não tivesse obtido provimento, a Relação alterou a qualificação jurídico-penal dos

factos provados, em causa, condenam a arguida..., como autora material de um crime de abuso de cartão de crédito previsto e punido no artigo 225.º, n.º 1, do Código Penal, na pena determinada na sentença recorrida, isto é, na pena de 70 (setenta) dias de multa, à taxa diária de 700$00 (setecentos escudos), o que se traduz na quantia de 49.000$00 (quarenta e nove mil escudos)."

Sumário: "Integra um crime de abuso de cartão de crédito previsto e punido pelo artigo 225 n.1 do Código Penal, a conduta do arguido que utilizou um cartão de crédito da ofendida, sem o acordo desta, para, com ele, fazer um pagamento e retirar dinheiro de uma caixa do estabelecimento comercial em que trabalhava, causando assim prejuízo patrimonial à titular do cartão, e tendo agido livre e conscientemente, sabendo da ilicitude da sua conduta."

*

Acórdão do Tribunal da Relação de Coimbra, de 03.04.2009, que teve como relator a Juíza Desembargadora Elisa Sales, Proferido no processo n.º 1313/07.6GBAGD.C1., disponível para consulta em www.dgsi.pt.

Neste processo, o arguido foi condenado pela "prática, como autor material e em concurso efetivo, de um crime de furto p. e p. pelo artigo 203.º, n.º 1, e de um crime de abuso de cartão de crédito, na forma continuada, p. e p. pelos artigos 225.º, n.º 1 e 30.º, n.º 2, todos do Código Penal, nas penas parcelares de 160 e 240 dias de multa e, em cúmulo jurídico, na pena única de 300 dias de multa, à taxa diária de € 11,00, perfazendo o total de € 3.300,00, ou subsidiariamente, na pena de 200 dias de prisão. Apurou-se que, o arguido se apoderou de um cartão de pontos da Galp, um cartão Multibanco e o cartão de crédito Visa Gold com o n.º 4…. da queixosa, o intuito de utilizar os mesmos em levantamentos bancários e aquisição de produtos."

Sumário: "I. - Para além da prova direta do facto, a apreciação do tribunal pode assentar em prova indireta ou indiciária, a qual se faz valer através de presunções. II. - No recurso a presunções simples ou naturais (artigo 349.º do Cód. Civil), parte-se de um facto conhecido (base da presunção), para concluir presuntivamente pela existência de um facto desconhecido (facto presumido), servindo-se para o efeito dos conhecimentos e das regras da experiência da vida, dos juízos correntes de probabilidade, e dos princípios da lógica. III. - "As presunções simples ou naturais são, assim, meios lógicos de apreciação das provas; são meios de convicção. Cedem perante a simples dúvida sobre a exatidão no caso concreto."

*

Acórdão da Relação de Guimarães, proferido no processo 102/09.8GEBRG.G2 e que teve por relatora a Juíza Desembargadora Maria Luísa Arantes. Datado de 24.04.2014, disponível para consulta em www.dgsi.pt.

O acórdão versa sobre a proteção de dados e proibição de prova. Neste acórdão os arguidos vinham acusados pelo tribunal coletivo, Vara de Competência Mista do Tribunal Judicial de Braga, além do mais, pela prática de um crime de furto qualificado p. e p. pelo artigo 204.º, n.º 1, al. b), do C. Penal, na pena de um ano de prisão; pela prática de um crime de burla

informática p. e p. pelo artigo 221.º, n.º 1, do C.Penal, na pena de oito meses de prisão; pela prática de um crime de abuso de cartão de garantia p. e p. pelo artigo 225.º, n.º 1, do C. Penal, na pena de nove meses de prisão. Em cúmulo jurídico, o arguido André foi condenado na pena única de vinte meses de prisão efetiva.

"No dia 15 de Junho de 2009, entre as 13 e as 16 horas, o arguido André N..., agindo de comum acordo com o Albano M... e com a Maria S... e no prossecução de um plano delineado por todos decidiram assaltar o veículo de matrícula 21-34-..., Peugeot, modelo 206, propriedade de Alexandre M..., que se encontrava estacionado na Rua T..., nesta cidade de Braga. 2. Para o efeito, por forma não apurada o arguido, o Albano e a Maria S... abriram as portas do referido veículo e daí retiraram e fizeram seus: um GPS marca Tom Tom, no valor de 100 euros; uma bolsa de senhora tira colo, de marca Cavalinho, em couro de cor castanha e bege, no valor de 80€, uma carteira porta documentos, da mesma cor e marcas, no valor de 50€, contendo documentos pessoais da esposa do proprietário do veiculo Florbela M..., nomeadamente BI, cartão contribuinte, cartão eleitor, dois cartões multibanco em nome da mesma, um de crédito e outro de débito, de uma conta do BES, uma porta-moedas, (…) 100€ em notas e moedas do BCE. Na posse do cartão de crédito n.º 3389..., na referida ATM após introduzirem o cartão do ofendido, digitaram o código e levantaram as quantias de 200€ e 200€ de que se apropriaram. Em seguida dirigiram-se ao centro comercial B.... 6. Uma vez aí deslocaram-se à loja Worten Mobile onde adquiriram os telemóveis com os IMEI`S 354208031935..., 352965037646... e 354850029279..., Nokia E71, Sony Ericson w595 e Nokia 5610, respetivamente, pelo valor de 364,00€, 249,90€ e 159,90€. 7. Para pagamento dos referidos telemóveis introduziram o cartão de crédito n.º 3389... e o respetivo código no terminal de pagamento automático. 8. Deslocaram-se depois à loja NIKE, onde adquiriram, peças de vestuário e sapatilhas para todos, no valor de 254,75€ e 440,75€. 9. Para pagamento de tais peças introduziram o cartão de crédito n.º 3389... e o respetivo código no terminal de pagamento automático da referida loja. 10. Depois na loja LEVI`S (…) adquiriram roupa, no valor de 427,00€. Para pagamento de tais peças introduziram o cartão de crédito n.º 3389... e o respetivo código no terminal de pagamento automático da referida loja. 11. O arguido atuou do modo descrito em conjugação de esforços com o Albano e a Maria S... e em execução de plano prévio antes por eles delineado, no propósito concretizado de se introduzir no interior do veículo automóvel, e apoderar-se dos objetos acima referidos, assim os retirando da disponibilidade do seu proprietário, sendo certo que sabia que os mesmos lhe não pertenciam. 12. Sabia o arguido que o cartão de crédito não lhe pertencia e que não tinha autorização do seu proprietário para o utilizar e, apesar disso, não se coibiu das suas condutas, utilizando o referido cartão, efetuando levantamentos e pagamentos contra a vontade do seu legítimo dono, causando-lhe, desta forma, prejuízo. 13. Agiu, ainda, o arguido com o propósito concretizado de obter um enriquecimento ilegítimo, causando prejuízo patrimonial, interferindo no resultado de tratamento de dados acedendo ao programa informático das máquinas ATM, utilizando dados do titular sem a respetiva e necessária autorização e intervindo também de forma não autorizada no processamento desse sistema, já que, acedeu a tal programa através do código PIN do cartão de débito que obteve da forma descrita. 14. Ao assim agir, bem sabia o arguido que as suas condutas eram proibidas, não se abstendo, todavia, de as prosseguir."

Sumário: "I – O direito à imagem está tutelado criminalmente, mas apenas na medida em que não esteja coberto por uma causa de justificação da ilicitude. II – Não constituem provas ilegais, podendo ser valoradas pelo tribunal, a gravação de imagens por particulares em locais públicos, ou acessíveis ao público, nem os fotogramas oriundos dessas gravações, se se destinarem a documentar uma infração criminal e não disserem respeito ao «núcleo duro da vida privada» da pessoa visionada (onde se inclui a intimidade, a sexualidade, a saúde e a vida particular e familiar mais restrita)."

1.9. O crime nos nossos Tribunais

Foram localizados os seguintes processos na Procuradoria do Juízo de competência genérica do Cartaxo e no Departamento de investigação e ação penal de Santarém, secção do Cartaxo:
Processo 1: Processo n.º ---/12.0PACTX, que tramitou nos Serviços do Ministério Público da Comarca do Cartaxo, o ofendido apresentou queixa na PSP, contra desconhecidos alegando que, após consulta do extrato de conta constatou que foram efetuadas várias transações com o seu cartão de crédito, que nunca saiu da sua posse, a partir de Los Angeles. Efetuadas as diligências com vista à obtenção de prova, foi o processo arquivado nos termos do disposto no artigo 277, n.º 2 do C.P.P.

Comentário: Aparentemente e com base na parca factualidade carreada para os autos, estariam em causa fatos suscetíveis de consubstanciar um crime de burla informática, p. e p. artigo 221.º do Código Penal.

Processo 2: Processo n.º ---/13.0PACTX, estava em causa a utilização de dados do um cartão de crédito por desconhecidos, que, de forma não concretamente apurada conseguiram realizar movimentos/transações *on line*, no montante total de € 697,11, efetuados com cartão de crédito, a partir de Londres, entre outros. À semelhança do processo anterior, o cartão de crédito nunca saiu da posse do seu titular. A qualificação dos factos foi alterada mais tarde, passando a tramitar como inquérito relativo ao crime de burla informática. O ofendido foi ressarcido parcialmente pelo banco, e desistiu da queixa, tendo o processo sido arquivado nos termos do artigo 277.º, n.º 1, do Código Processo Penal.

Comentário: concordamos com a alteração efetuada à qualificação jurídica.

Processo 3: Processo n.º ---/15.0PBBJA, no âmbito do qual foi apresentada queixa porquanto foram efetuados levantamentos, com recurso a um cartão de crédito furtado, numa caixa ATM, entre os dias 01.05.2014 e 07.04.2015, no valor total de € 540,05. Feitas diligências de prova foi possível apurar que o cartão de crédito nunca tinha chegado à pose do seu titular, assim como, o respetivo código pin, já que foi retirado da caixa do correio do queixoso; foi possível identificar a autora dos factos, através do cruzamento da informação constante do extrato da conta, fornecido pela entidade emissora do cartão de crédito, no qual constava um carregamento de um cartão de telemóvel, com os dados fornecidos pela operadora de telecomunicações. A titular do processo fez uso do instituto da suspensão provisória do processo (281.º do C.P.C.) tendo considerado que, estava em causa a prática dos crimes de

apropriação ilegítima de coisa achada p. e p. pelos artigos 209.º do C.P., crime de violação de correspondência p. e p. pelo artigo 194.º do C.P. e um crime de abuso de cartão de crédito, p. e p. pelo artigo 225.º do Código Penal.

Comentário: atenta a posição assumida pela maioria dos autores, a factualidade descrita (caso o levantamento tenha sido feito a crédito) consubstanciaria, a par de outros, um crime de abuso de cartão de crédito.

1.10. Conclusão

O crime de abuso de cartão de garantia ou de crédito foi pensado para colmatar a lacuna existente no crime geral de burla em relação à conduta do titular do cartão de crédito ou de garantia que o utiliza, intencionalmente, para além do montante contratualmente estipulado.

O núcleo essencial de proteção da norma do artigo 225.º do C.P. é o património da entidade emissora do cartão de crédito, porém o artigo está também pensado para os casos de utilização por terceiro não autorizada, por exemplo, no caso de furto, situação em que protege o património do seu titular.

Nos dias de hoje, todos os cartões novos estão equipados com um *chip* e são utilizados através da marcação de código pin, sendo poucos ou inexistentes os cartões de crédito utilizados com recurso a banda magnética e com assinatura da fatura, que representavam à data em que o artigo foi redigido, um maior risco. Da mesma forma, no caso das compras feitas *on line*, os cartões são utilizados através da marcação dos três algarismos de segurança.

Assim, a utilização dos cartões de crédito é, agora, feita de uma forma mais segura, apenas se concebendo uma utilização abusiva dos cartões de crédito durante os períodos em que o sistema esteja *off line*.

Da mesma forma, o cheque caiu em desuso e com ele o cartão de garantia, sendo que, grande parte dos pagamentos efetuados nos dias de hoje é feita através de cartão ou transferência bancária.

O grosso da utilização dos cartões de crédito é feita através de pagamentos *on line*, em *sites* na internet e nas caixas ATM e POS, sendo que, no primeiro caso, temos para nós que, estamos perante um crime de burla informática; já no segundo caso, conforme se viu, alguns autores (Maia Gonçalves e Alexandre Lafayette) consideram que a utilização do cartão de crédito para levantar dinheiro, numa caixa ATM, com utilização de PIN se subsume à norma do artigo 225.º do C.P., desde que, o cartão de crédito seja utilizado com o seu propósito normal, de conceder crédito.

Outros autores (Damião da Cunha e Miguez Garcia) consideram que, se a utilização do cartão de crédito for feita com recurso à marcação de pin e ou sistema informático, já consubstancia um crime de burla informática.

Fazer depender a subsunção dos factos à norma incriminadora do artigo 225.º do C.P. da forma como o cartão de crédito é utilizado, parece-nos uma opção dúbia; cremos também que, a especialidade do crime de abuso de cartão de garantia ou de crédito em relação aos crimes de burla e burla informática deixou de fazer sentido, atenta a quantidade e diversidade de cartões existentes atualmente e bem assim, o facto de a sua utilização implicar, necessariamente, a utilização e transmissão de dados informáticos.

No que concerne à tramitação do processo, a par da errónea tipificação dos inquéritos, assistimos a um grande número de desistências/arquivamentos. Em regra, o queixoso tem pouca ou nenhuma informação acerca do local e demais circunstâncias onde ocorreram os abusos – apenas sabe o que vem mencionado no seu extrato. Na generalidade destes processos, a vítima/denunciante tem uma postura pouco cooperante com a investigação. Sendo que, muitas das vezes, o cartão já foi cancelado e o seguro ativado – a verdadeira motivação da queixa.

Por outro lado, consideramos que, no limite, a utilização fraudulenta destes cartões (crédito/garantia de cheque) pelo seu titular, em violação do acordo celebrado entre o titular do cartão e a entidade emissora do mesmo, deveria, ser resolvida em sede de ação emergente de responsabilidade civil contratual, por se tratar de um incumprimento. A tipificação de um incumprimento contratual como delito criminal, configura no limite uma prisão por dívidas, cuja constitucionalidade, é quanto a nós, suscetível de ser posta em causa[33].

Referências bibliográficas

ALBUQUERQUE, Paulo Pinto de, "Comentário do Código Penal à luz da Constituição da República Portuguesa e da Convenção Europeia dos Direitos do Homem, Lisboa, 3.ª Edição, Universidade Católica Editora, 2015, pp. 871-873.

BARREIROS, José António, Crimes contra o património, 1996, Universidade Lusíada, Lisboa, pp. 214-217.

DANTAS, A. Leones, Jornadas de Direito Criminal, A revisão do Código Penal, alterações ao sistema sancionatório e Parte especial, Lisboa, 1998, Centro de Estudos Judiciários, pp. 516 a 518.

DIAS, Jorge de Figueiredo, Comentário Conimbricense do Código Penal, Parte especial Tomo II, artigos 202.º a 307.º, Coimbra Editora, 1999, pp. 373-383.
GARCIA, M. Miguez, RIO, J. M. CASTELA, Código Penal, Parte Geral e Especial com Notas e Comentários, Coimbra, 2.ª Edição, Almedina, 2015, pp. 998-1002.

[33] Vide Casabona, Delitos Cometidos Com La Utilización de Tarjetas de Crédito, 1991, Nuevo Foro Penal.

GARCIA, M. Miguez, O Direito Penal Passo a Passo – Elementos da parte especial, 2.º volume, com os crimes contra o património, os crimes de falsificação e os crimes de perigo comum contra a segurança das comunicações, Coimbra, Almedina, 2011, pp. 271-273.

GONÇALVES, M. Maia, Código Penal Português Anotado e Comentado e Legislação complementar, 14.ª Edição, Coimbra, Almedina, 2001, pp. 727 a 728.

LEAL-HENRIQUES, Manuel de Oliveira, SANTOS, Manuel José Carrilho de Simas, Código Penal Anotado, (art.º 131.º a 386.º), II Volume, 3.ª Edição, Porto, Rei dos Livros, 2000, pp. 948-952.

ROCHA, Manuel António Lopes da, Jornadas de Direito Criminal, A revisão do Código Penal, soluções de neocriminalização, Centro de Estudos Judiciários, pp. 95.-97.

Ministério da Justiça, Código Penal Atas e Projeto da Comissão de Revisão, Rei dos Livros, pp. 450-451.

CASABONA, Carlos Maria Romeo, "Delitos cometidos con la utilización de tarjetas de crédito", Poder Judicial, número Especial IX, 1991, pp. 109-124.

5.
O crime de abuso de cartão de garantia ou de crédito. Enquadramento jurídico, prática e gestão processual

Nuno Filipe de Sousa Gonçalves

CENTRO
DE ESTUDOS
JUDICIÁRIOS

5. CRIME DE ABUSO DE CARTÃO DE GARANTIA OU DE CRÉDITO. ENQUADRAMENTO JURÍDICO, PRÁTICA E GESTÃO PROCESSUAL

Nuno Filipe de Sousa Gonçalves

I. Introdução

O primeiro cartão de crédito a ser emitido em Portugal remonta ao ano de 1970, sendo que, nessa altura, os cartões apenas podiam ser usados para crédito e, regra geral, em ocasiões especiais como uma viagem, uma ida ao restaurante ou compras em alguns estabelecimentos.

Volvidos quase 50 anos, os cartões de crédito não só se popularizaram, encontrando-se acessíveis a um elevado número de pessoas, como também são fortemente utilizados para pagamento de bens e serviços.

Ao mesmo tempo, conforme a Internet e os sistemas informáticos foram evoluindo e alargando cada vez mais o seu âmbito de utilização, ao ponto de se tornarem essenciais ao bom funcionamento da sociedade moderna, também aumentou o risco de fraude associado ao uso dos cartões de crédito.

Partindo deste contexto, é preciso ter presente que, num primeiro momento, para utilizar o cartão de crédito requeria-se um terminal de pagamento manual, vulgarmente designado de "*ferro de engomar*", no qual era colocado o cartão e um impresso. Após esta operação uma parte amovível da máquina pressionava o cartão, de molde a que os dados do cartão ficassem gravados num talão, que era passado em triplicado, sendo o original para o comerciante, uma

cópia para a entidade emitente do cartão e outro para o titular do cartão: este talão era assinado pelo titular do cartão, devendo o comerciante compará-la com a assinatura colocada no verso do cartão.
Numa fase posterior, o cartão passou a possuir uma banda magnética para ser inserido num terminal de pagamento automático, através do qual era permitido a leitura dos dados inseridos nessa banda magnética. Neste terminal é inserido o montante da operação, sendo emitido um talão, em duplicado, que é assinado pelo titular do cartão, conferindo assim autenticidade ao acto, sendo depois transmitidas para a entidade emitente ou gestora do sistema as operações realizadas.

Mais tarde, para obviar à insegurança dos cartões de crédito, foram neles introduzidos *chips* que permitem armazenar mais informação que uma barra magnética, nomeadamente a identificação do titular, o seu histórico, o limite de crédito, passando a ser necessário ainda a introdução de um PIN pelo titular para desta forma validar a operação em substituição da assinatura. Assim, os terminais de pagamentos automáticos passam a estar em constante comunicação com o emitente do cartão, sendo este quem, em último lugar, depois de confirmar dos dados e o saldo associado ao cartão, vai autorizar o pagamento.

Portanto, o legislador em 1995 quando introduziu o crime de abuso de cartão de garantia ou de crédito no Código Penal Português, apesar que compreender a importância que aqueles cartões representavam para a economia (em especial o cartão de crédito, pois o cartão de garantia nunca teve grande adesão), ainda estava no meio deste processo de evolução e segurança de cartões de crédito.

Isto significa, que o legislador naquela altura estava longe de imaginar que a utilização dos cartões não iria depender mais da assinatura do titular para realizar transacções, mas antes da introdução de um código PIN num sistema informático (os terminais automáticos de pagamento POS). O que sucede hoje em dia de forma quase exclusiva.

Por isso, apesar da consagração legal do crime de abuso de cartão de garantia e de crédito em 1995, a verdade é que aquele tipo legal de crime nunca teve grande aplicabilidade, somente em casos residuais, sendo que nos últimos anos parece ter desaparecido por completo dos tribunais.

II. Objectivos

O presente trabalho visa compreender o contexto em que surge o crime de abuso de cartão de crédito e de garantia no Código Penal Português, enumerando e apreciando os seus elementos típicos e outras características associadas ao tipo legal, e procurar saber se actualmente ainda se mantém as mesmas condições que levaram à criação daquele tipo legal de crime, sendo aqui importante analisar várias outras situações de utilização indevida do cartão e o concurso de crimes, para assim concluir se o crime em causa se deve manter ou se pelo contrário deve ser revogado. Não descurando em fornecer, dentro do possível, alguns elementos não

exaustivos do que deve ser feito em termos de gestão processual na investigação deste tipo legal de crime.

III. Resumo

O crime de abuso de cartão de abuso de cartão de garantia ou de crédito foi introduzido em 1995 no Código Penal Português, sendo que a sua tipificação não foi pacífica, suscitando naquela alguma controvérsia.

O bem jurídico pela incriminação é o património de outra pessoa, onde é possível que sejam afectados diversos patrimónios, dependendo da qualidade do agente perante o cartão.

O tipo objectivo consiste na conduta de alguém que abuse da possibilidade, que lhe é conferida pela posse de cartão de garantia ou de crédito, de levar o emitente a fazer um pagamento causando desta forma um prejuízo. Por seu lado, o tipo subjectivo supõe a verificação do agente, em qualquer uma das suas modalidades.

Para que se possa afirmar que o agente verdadeiramente cometeu um crime, é necessário ainda a verificação do preenchimento dos pressupostos da ilicitude e da culpa, pois, para que um facto seja punível, para além de ser necessariamente típico, terá que ser ainda ilícito e culposo.

Este crime é punido com pena de prisão até 3 anos ou com pena de multa, prevendo ainda o tipo a agravação da conduta em função do valor, com pena de prisão de 2 a 8 anos.

Por regra é um crime de natureza semi-pública, mas, em função de certas qualidades do agente ou da agravação, pode ter igualmente natureza particular ou pública.

A tentativa é punível.

Na determinação da responsabilidade criminal dos agentes podem ocorrer situações de anulação ou concurso (aparente ou real) de crimes, sempre que o agente com a sua conduta cometa uma pluralidade de crimes ou aquela possa aparentemente preencher vários tipos legais de crime. Situações que são muitos frequentes, quando está em causa a utilização indevida do cartão.

A investigação deste tipo de criminalidade reclama, assim como as restantes investigações criminais, uma racionalização eficaz e eficiente dos meios. Eficaz no sentido de atingir o objectivo pretendido, e eficiente no sentido de atingir um objectivo definido da melhor forma possível. Todavia, esta tem a particularidade de, logo no primeiro momento, identificar o modo como cartão foi utilizado.

1. Consagração legal

O crime de abuso de cartão de garantia ou de crédito foi introduzido no Código Penal Português na revisão operada pelo Decreto-Lei n.º 48/95, de 15 de Março - como um exemplo claro do movimento de neocriminalização presente no Código Penal -, dispondo, desde então, o artigo 225.º, n.º 1, que: "Quem, abusando da possibilidade, conferida pela posse de cartão de garantia ou de crédito, de levar o emitente a fazer um pagamento, causar prejuízo a este ou a terceiro é punido com pena de prisão até 3 anos ou com pena de multa".

Este tipo legal de crime tem por fonte próxima o § 266.ºb do Código Penal Alemão (*Missbrauch von Schech- und Kreditkarten*), introduzido no ano de 1986, pela Segunda Lei de Combate ao Crime Económico, mas afasta-se daquele no que respeita ao universo de potenciais agentes activos.

Com efeito, o tipo legal Alemão sanciona apenas condutas de abuso praticadas por titulares do cartão (crime específico/próprio), enquanto do tipo legal Português além de abranger a eventual responsabilidade daqueles alarga a responsabilização criminal a todos os terceiros que, por qualquer título, usem um cartão de garantia ou de crédito alheio e sem autorização do seu titular (crime comum)[1].

A introdução do crime de abuso de cartão de garantia ou de crédito no Código Penal em 1995 não foi pacífica, suscitando alguma controvérsia no âmbito da Comissão Revisora (assim como também sucedeu no Direito Alemão), quer quanto à dignidade penal da conduta, quer quanto ao seu enquadramento legal[2].

A incriminação surgiu da proposta do Conselheiro Sousa e Brito com o objectivo de sanar uma lacuna de punibilidade do crime geral de burla (com o qual encontra o seu paralelismo), pois, não existia até então um claro enquadramento criminal de certos casos, nomeadamente os que se prendem com a utilização não autorizada de cartões de crédito[3].

Como refere Damião da Cunha, «[d]e facto, pode ser difícil a afirmação do *crime de burla* (tendo por vítima a entidade emitente do cartão), sobretudo porque poderá ser difícil, se não impossível, a verificação do erro ou da astúcia, como, por outro lado, a actuação abusiva se dirigirá contra um terceiro (um comerciante associado) e não directamente face à entidade emitente, o que pode colocar dificuldades na determinação da conexão entre o acto de "burla" e o prejuízo patrimonial (cf. artigo 217.º)»[4].

Todavia, como bem refere Paulo Pinto de Albuquerque, o legislador nacional ao conformar o crime de abuso de cartão de garantia e de crédito como um crime comum, cria problemas de concurso aparente de normas, porquanto, as condutas de utilização por terceiro do cartão de

[1] Neste sentido, Damião da Cunha, Comentário Conimbricense do Código Penal, Parte Especial, Tomo II, Jorge de Figueiredo Dias [Dir.], Coimbra Editora, 1999, p. 373, e Paulo Pinto de Albuquerque, Comentário do Código Penal à luz..., Universidade Católica Editora, 2008, p. 620.
[2] Veja-se as Actas n.ºs 39, 47, 48 e 52 da Comissão de Revisão, in Ministério da Justiça, Código Penal, Actas e Projecto da Comissão de Revisão, Rei dos Livros, 1993.
[3] Neste sentido, Sousa e Brito, Acta n.º 39 da Comissão de Revisão, *op. cit.*, 1993, p. 450.
[4] *Op. cit.*, 1999, p. 374.

garantia ou de crédito não autorizadas já se encontram tuteladas pela incriminação geral da burla (quando o enganado é uma pessoa) ou pela burla informática (quando se verifica manipulação informática)[5].

Assim como refere Almeida Costa, «quando ocorra o emprego de processos informáticos, pode verificar-se uma de duas hipóteses. A primeira consistirá em o agente induzir outra pessoa num erro que a leva, através de uma operação informática, a causar prejuízo patrimoniais próprios ou alheios, detecta-se aqui o *duplo nexo de imputação objectiva* característico do modelo tradicional de burla e, portanto, o preenchimento do tipo legal do artigo 217.º, desde que satisfeitos os demais requisitos da figura. A segunda traduzir-se-á no facto de o sujeito activo produzir o dano patrimonial mediante a interferência *directa* num sistema informático, deparando-se com um *iter criminis* que não apresenta, de permeio, a intervenção de uma pessoa em estado de erro e, por conseguinte, *não* comporta o referido "duplo nexo de imputação objectiva". Só esta última alternativa integra o delito de burla informática do n.º 1 do art.º 221.º»[6].

Também A. Leones Dantas entende que crime de abuso de cartão de garantia ou de crédito, tal como foi introduzido no Código Penal Português, cria sérias dificuldades de interpretação quando alarga o âmbito de aplicação daquele crime a terceiros e não só apenas ao seu titular, ao contrário do que sucede no correspondente crime previsto no Código Penal Alemão.

Segundo este Autor, a consagração do tipo legal de crime em causa, enquanto crime comum, «poderá ter desvirtuado a consistência estrutural daquele tipo de crime e talvez de forma desnecessária. Com efeito, nas situações de utilização do cartão por quem dele não seja titular, recaia afinal o prejuízo sobre o emitente ou sobre terceiro, sempre estaríamos num normal crime de burla, em que a utilização do cartão mais não foi do que o instrumento da indução em erro do terceiro»[7].

Também assim, José António Barreiros defende a posição que, tal como no Direito Alemão, estamos perante um crime próprio e não face a um crime que possa ser cometido por qualquer pessoa no qual o agente do crime apenas pode ser o legitimo titular e possuidor de um cartão de crédito ou de garantia, estando, desta forma, excluídas do tipo legal as pessoas que tenham obtido a posse de tais cartões por forma ilegítima[8].

Mas não parece ser o caso, pois, a própria Comissão Revisora expressamente considerou o crime de abuso de cartão de garantia ou de crédito como um crime comum, justificando esta extensão a qualquer pessoa face ao bem jurídico protegido (património da entidade emissora

[5] *Op. cit.*, 2008, p. 620, baseando-se em Trechsel e Bk-Fiolka.
[6] *In* Comentário Conimbricense do Código Penal, Parte Especial, Tomo II, Jorge de Figueiredo Dias [Dir.], Coimbra Editora, 1999, p. 330. Ou seja, no crime de burla informática o prejuízo patrimonial é consequência adequada da conduta do agente sem mediação do ofendido ou da pessoa enganada, o que se afasta da estrutura tradicional do crime de burla (simples).
[7] A. Leones Dantas, A Revisão do Código Penal e os Crimes Patrimoniais, in "Jornadas de Direito Criminal, Revisão do Código Penal", Centro de Estudos Judiciários, 1998, pp. 517 e 518.
[8] José António Barreiro, Crimes Contra o Património, Universidade Lusíada Editora, 1996, p. 214.

do cartão) e a forma como se consubstancia a infracção (abuso da garantia da entidade emissora)[9].

Todavia, em nossa opinião, para obviar às dificuldades interpretativas suscitadas quanto ao agente do crime, o legislador poderia ter sido mais claro neste sentido se a norma em causa previsse a "detenção de cartão" em vez de "posse de cartão".

Portanto, tendo em conta os princípios a seguir na interpretação da lei, previstos no art.º 9.º do Código Civil, e também tendo em conta o pensamento legislativo que levou à criação do tipo legal de crime em análise, uma vez ocorrendo correspondência deste com a letra da lei, independentemente do resultado, inclusive pela aplicação das regras do concurso de crime, não pode atribuir-se a este crime outra natureza senão a de crime comum.

2. O bem jurídico protegido

O bem jurídico protegido pela incriminação é o património de outra pessoa, em regra, o património do emitente do cartão de garantia ou de crédito atingido pelo facto criminoso, seja ele uma instituição de crédito ou uma sociedade financeira[10]. Com efeito, é esse, quem, normalmente, pagando, sofre um prejuízo, desencadeado pelo abuso do utilizador, ao servir-se, de modo ilegítimo, da "possibilidade de levar o emissor a fazer um pagamento"[11].

Todavia, outros patrimónios podem ser lesados, especialmente nos casos em que a utilização do cartão não é feita pelo titular do cartão mas por outra pessoa[12].

Assim, o titular do cartão ao abusar da posse atinge os interesses pecuniários da entidade emissora, mas se o cartão for utilizado por um terceiro o prejudicado pode ser tanto a entidade emissora, como o próprio titular do cartão ou até mesmo o comerciante integrado na rede. O crime consuma-se logo que um deles sofra um prejuízo com o abuso[13].

E como refere Damião da Cunha, a protecção da confiança no tráfico com cartões deste tipo (modos de pagamento não pecuniário) não é protegido pela incriminação, mesmo que secundariamente esteja presente, pois, quanto muito apenas logra um *efeito protectivo reflexo*[14].

Como se observa, no crime de abuso de cartão de garantia ou de crédito é assim essencial a ocorrência de um prejuízo patrimonial, sendo um crime de dano quanto ao grau de lesão do

[9] Neste sentido, Sousa e Brito, Acta n.º 39 da Comissão de Revisão, *op. cit.*, 1993, p. 450.
[10] *Idem ibidem*.
[11] Neste sentido, Victor de Sá Pereira e Alexandre Lafayette, Código Penal Anotado e Comentado, *Quid Juris*, 2008, p. 598.
[12] Neste sentido, Costa Andrade, Acta n.º 39 da Comissão de Revisão, *op. cit.*, 1993, p. 451.
[13] Neste sentido, M. Miguez Garcia, O Direito penal – Passo a Passo, Vol. II, 2.º Ed., Almedina, 2015, p. 275.
[14] *Op. cit.*, 1999, p. 375.

bem jurídico, e um crime de resultado quanto à forma de consumação do ataque ao objecto da acção[15].

O património, por seu lado, abrange o conjunto das "*situações*" e "*posições*" com valor económico, detidas por uma pessoa e protegidas pela ordem jurídica ou, pelo menos, cujo exercício não é desaprovado pela ordem jurídica[16].

Património será, neste contexto, «a capacidade económica do sujeito de direito, derivada do seu domínio sobre objectos que a ordem jurídica reconhece como elemento autónomo do tráfico económico (...) Com maior rigor, património será "o complexo de relações jurídicas encabeçadas por um sujeito que tem por último *coisas* dotadas de *utilidade*, isto é, de capacidade de satisfazer necessidades humanas, *materiais* ou *espirituais*"» (concepção mista de património ou jurídico económica)[17].

Quanto ao prejuízo patrimonial, enquanto requisito da consumação do delito, adoptando a opinião actualmente dominante, este consiste num conceito objectivo-individual e de acordo com o qual «deverá determinar-se através da aplicação de critérios objectivos de natureza económica à concreta situação patrimonial da vítima, concluindo-se pela existência de um dano sempre que se observe uma diminuição do valor económico por referência à posição em que o lesado se encontraria se o agente não houvesse realizado a sua conduta»[18].

Todavia, como afirmam alguns autores, a diminuição do valor económico não necessita de se exprimir num valor pecuniário certo, sendo suficiente que a lesão típica do bem jurídico se produza com o ataque a todas ou algumas faculdades inerentes à situação de domínio, prescindindo de considerações económicas.

[15] Neste sentido, Paulo Pinto de Albuquerque, *op. cit.*, 2008, p. 620.
[16] Para um melhor estudo sobre a discussão em torno do conceito jurídico-penal de património, veja-se M. Miguez Garcia, *op. cit.*, 2015, pp. 12 a 18.
[17] M. Miguez Garcia, *op. cit.*, 2015, pp. 13 e 14, citando Faria Costa.
[18] Neste sentido, Almeida Costa, *op. cit.*, 1999, p. 285.

3. Elementos do tipo legal de crime

3.1. Elementos objectivos

O tipo objectivo consiste na conduta de alguém que abuse da possibilidade, que lhe é conferida pela posse de cartão de garantia ou de crédito, de levar o emitente a fazer um pagamento, causando deste modo um prejuízo para o emitente ou para um terceiro.

São, pois, elementos do tipo objectivo:

– "Posse" de um cartão de garantia ou de crédito;

– Abusar da possibilidade de levar o emitente a fazer um pagamento; e,

– Causar prejuízo ao emitente ou a terceiro.

3.1.1. "Posse" de um cartão de garantia e de crédito

A "posse" no tipo legal de crime em análise afigura-se como um elemento do tipo que identifica o autor da acção (aquele que possui), referindo-se a um exercício do poder de facto em sentido jurídico-penal do cartão próprio ou alheio, e não à "posse" como conceito do direito civil[19]. Sendo certo que a utilização de cartão furtado também se encontra abrangida pela incriminação[20].

O cartão de garantia (ou cartão de garantia de cheques) é aquele que se destina «a garantir, até um determinado montante, cheques que foram validados por um comerciante, quer com base num cartão emitido ao titular do cheque ou através de uma base de dados central, à qual os comerciantes têm acesso. Os cheques validados são garantidos pela entidade emissora do cartão de garantia, o banco sacado ou pelo operador do sistema»[21].

A sua função é a de facilitar a aceitação do cheque no comércio, mediante a garantia por parte do emitente de que aquele será pago, independentemente de ter ou não provisão, ou seja, tem uma função de garantia de pagamento.

O cartão de crédito, por sua vez, é aquele que permite ao seu titular «adquirir bens e serviços cujo pagamento é assegurado pela actuação intermediadora do emissor que se substitui junto do comerciante, e cujo reembolso pelo titular é diferido, podendo eventualmente ser escalonado em prestações mensais mediante o pagamento de juros»[22].

[19] Neste sentido, Pedro Sá Machado, Os "crimes de detenção" e a "detenção-de-uma-coisa-móvel" no direito penal português: problemas conceptuais, dogmáticos e político-criminais, Tese de Mestrado, Faculdade de Direito da Universidade de Coimbra, 2015, p. 23.
[20] Neste sentido, Sousa e Brito, Acta n.º 39 da Comissão Revisora, *op. cit.*, 1993, p. 450.
[21] Noção dada pelo Banco de Portugal na sua página de Internet: https://www.bportugal.pt/glossario/c.
[22] Joana de Vasconcelos, *apud.* Damião da Cunha, *op. cit.*, 1999, pp. 375 e 376.

Em regra, a utilização do cartão de crédito integra-se num sistema tripartido, que compreende três partes, assente numa relação triangular entre o emitente, o titular e o comerciante aderente que tem um terminal de pagamento (em regra automático, mas que pode ser manual), e tem a dupla função de servir como meio de pagamento e de concessão de crédito.

Nesta circunstância são celebrados dois contratos distintos, embora paralelos, o contrato de compra e venda do bem, ou contrato de prestação de serviços, e o contrato de crédito associado, o que determina a constituição de uma conexão entre ambos – contratos coligados.

Sem perder aquela dupla função de servir como meio de pagamento e de concessão de crédito, pode ainda existir um sistema quadripartido de utilização de cartões. Tal como o próprio nome prenuncia, existem quatro intervenientes que asseguram a transacção: o titular, o comerciante, o banco emissor que assegura a relação com o titular do cartão bancário e o banco adquirente, entidade licenciada da marca do sistema de pagamentos com cartão que é responsável pelas transacções realizadas junto do comerciante[23].

O sistema quadripartido distingue-se do sistema tripartido, em que existe uma única entidade financeira responsável em exclusivo pela emissão de cartões e contratualização da marca do cartão junto dos comerciantes numa determinada área geográfica (sendo um exemplo clássico a marca "American Express").

Quanto aos cartões de crédito baseados num sistema bilateral, ou seja, numa relação exclusiva entre o emitente e o titular do cartão, em que a entidade emitente concede crédito ao titular para cada um dos seus estabelecimentos filiais, «[e]mbora este tipo de cartão seja correntemente denominado de crédito, de facto constitui uma forma exclusiva de concessão de crédito e, em regra, a sua titularidade não confere a possibilidade de levar o emitente a efectuar um pagamento, pelo que não cabe no âmbito deste crime»[24].

Para além da dupla função de servir como meio de pagamento e de concessão de crédito, os cartões de crédito podem ainda assumir várias outras funções (cartão *dual*), tais como:

– Adiantamento de dinheiro (*cash advance*), ou seja, a possibilidade conferida ao titular de levantar dinheiro em caixas automáticos ou aos balcões dos bancos que disponham dessa funcionalidade, e mediante o pagamento de juros;

– Débito directo em conta, que permite ao seu titular levantar dinheiro em caixas automáticos (ATM) ou pagar directamente compras com fundos da sua conta numa instituição de crédito depositária.

A incriminação em causa só prevê a protecção penal ao cartão de crédito quando este é usado na sua função típica de servir como meio de pagamento e de concessão de crédito.

[23] Note-se que o banco emissor pode ter a função de adquirente, assim como o adquirente pode também ser emissor de cartões.
[24] Damião da Cunha, *op. cit.*, 1999, p. 379.

Por outro lado, adiantando um pouco aquilo que se vai concluir mais à frente, o cartão que esta norma prevê, não é o cartão que usualmente é utilizado nos dias de hoje. Com efeito, o legislador configurou a existência deste cartão na sua forma mais simples, sem os actuais mecanismos de segurança contra fraude, e sem que houvesse comunicação instantânea entre o terminal de pagamento do comerciante e o sistema informático da entidade emitente.

Portanto, o legislador de 1995, quando previu a criminalização desta conduta, configurou-a ainda nos seguintes termos: quando se faz uma compra, o titular aceita pagar ao emitente assinando a factura do comerciante, onde constam os elementos do cartão e a indicação do quantitativo a pagar, tendo o comerciante apenas verificado previamente se o cartão era válido e se o titular dispõe de crédito suficiente para pagar o preço. Não havendo naquele momento uma prévia autorização para pagamento por parte do emitente do cartão no acto da compra, sendo antes a assinatura do titular que valida a transacção.

3.1.2. Abusar da possibilidade de levar o emitente a fazer um pagamento

O pagamento não significa apenas o pagamento em moeda, mas toda e qualquer forma de pagamento, como, *v.g.* o pagamento efectuado através de transferência bancária, e tem que resultar da possibilidade conferida pela posse do cartão, independentemente de qualquer relação jurídico-civil válida que fundamente a obrigação de pagamento, bastando, para o efeito, que o possuidor crie a aparência jurídica para gerar possibilidade de levar o emitente a fazer o pagamento[25].

Isto significa, pois, que aquele pagamento tem de resultar, directa e imediatamente, da função típica do cartão de garantia ou de crédito, pois é esta função que permite criar a referida aparência jurídica perante terceiros.

Assim, não faz parte do tipo objectivo do crime a utilização abusiva de cartões em sistemas automáticos que possibilite o pagamento de compras ou levantamento de dinheiro a débito, como é o caso dos casos das ATMs (caixas automáticas), pois, por um lado, no caso de utilização por terceiro, a utilização abusiva não resulta apenas da posse do cartão, mas também do conhecimento do código secreto que permite movimentar a conta do titular, sendo esta conduta prevista no crime de burla informática; por outro lado, esta hipótese não é configurável no caso de ser o próprio titular a utilizar o cartão, pois o levantamento está limitado, por princípio, ao montante disponível na conta bancária[26].

Em qualquer destes casos, faltará sempre a função de garantia ou de concessão de crédito dos cartões em causa.

Quando o tipo legal refere "abusando da possibilidade", esta conduta tanto pode ser levada a cabo pelo titular do cartão ou de qualquer outra pessoa, pelo que o abuso tem que ser apreciado de forma diferente, dependendo da qualidade da pessoa que utiliza o cartão.

[25] *Ibem idibem*, p. 377.
[26] Neste sentido, veja-se Damião da Cunha, *op. cit.*, 1999, p. 379.

No caso de a conduta ser realizada pelo titular do cartão, o abuso significa a violação das regras impostas ao nível do contrato que o titular celebrou com a entidade emitente, em que «a determinação do abuso por parte do titular tem de ser aferida em função das condições do contrato subjacente à emissão do cartão de garantia ou de crédito, pelo que dependerá, nomeadamente, do montante de crédito cujo pagamento a entidade emitente assegure»[27].

No caso de o agente não ser o titular do cartão o conceito de abuso não pode ser entendido como a "violação das regras impostas". Com efeito, em princípio, não sendo o agente titular do cartão, este também não tem direito ao uso do mesmo.

Nestes casos, pode haver abuso do cartão de crédito ou de garantia «quando um terceiro utiliza o cartão à revelia da vontade do respectivo titular, quer por ter desrespeitado as suas instruções, quer por lhe ter furtado o cartão, quer ainda por ter encontrado o cartão perdido o cartão pelo titular»[28].
Nos casos em que a utilização do cartão se baseia numa relação de confiança entre o titular e o não titular do cartão, p. ex., um familiar, a apreciação do abuso deve seguir as mesmas regras que o titular está sujeito[29].

Importante, em todo o caso, é que o abuso se refira à função normal do cartão e que, portanto, possa levar a entidade emitente a fazer um pagamento.

3.1.3. Causar prejuízo ao emitente ou a terceiro

Como já analisamos, ao contrário do que se passa no direito alemão, onde o prejuízo tem de se verificar na esfera da entidade emitente, aqui o universo dos potenciais lesados não é determinado no tipo, podendo este prejuízo vir a ocorrer no património do emitente como no património de um terceiro, pois tudo depende do agente do crime.

Sendo o agente o titular do cartão que abusa da posse daquele, em princípio o prejuízo vai ocorrer no património do emitente do cartão.

Todavia, não sendo o agente titular do cartão, então as pessoas prejudicadas podem ser: o emitente do cartão, o titular do cartão ou o comerciante que esteja associado à rede de utilização do cartão. Podendo nestes casos, inclusivamente, haver uma repartição do risco no caso de utilização abusiva por terceiro, dependendo das obrigações contratualmente estabelecidas, em especial no que concerne às comunicações ou notificações[30].

[27] *Idem ibidem*, p. 377.
[28] Paulo Pinto de Albuquerque, *op. cit.*, 2008, p. 621.
[29] Neste sentido, Damião da Cunha, *op. cit.*, 2009, p. 378.
[30] Neste sentido, Damião da Cunha, *op. cit.*, 2009, pp. 378 e 379, e M. Miguez Garcia e J.M. Castela Rio, *op. cit.*, 2015, pp. 1001 e 1002.

Cumpre recordar, no entanto, que este é um crime material ou de resultado, em que o tipo legal apenas se consome quando se verifica saída de disponibilidades financeiras do património do lesado.

3.2. Elemento subjectivo

O presente tipo legal supõe a verificação do dolo no agente, em qualquer uma das suas modalidades (cfr. art.º 14.º do Código Penal).

Isto significa, que «não é necessário que o agente (em especial, quando esteja em causa um portador não titular) individualize a pessoa que haja de sofrer o prejuízo patrimonial, pois, como se referiu, a definição do patrimonialmente prejudicado depende das regras contratuais»[31].

Por outro lado, não é exigido ao agente a intenção de causar prejuízo e, consequentemente, uma vantagem económica[32], ao contrário do que sucede com a maioria dos crimes contra o património, bastando, para o efeito, aferir se o dolo do agente, ao utilizar o cartão, abrange o abuso e o prejuízo patrimonial.

Todavia, tendo em conta a dignidade penal da conduta levada a cabo pelo titular do cartão, a mera violação das regras impostas pelo titular do cartão deve ser reconduzida ao incumprimento contratual, tutelado pela lei civil, e apenas ser considerado para efeitos penais os casos de abuso em que o titular do cartão excede o crédito que lhe foi atribuído com a consciência de que não tem condições financeiras para ressarcir a entidade emitente ou sabendo que o prazo de validade do cartão está ultrapassado e, assim, pretende subtrair-se ao pagamento[33]. Intenção que esteve em discussão na Comissão de Revisão, mas que por não se pretender fazer o paralelismo com o crime de burla não chegou a ser transposto para o texto final do artigo[34].

Este crime não é punível a título de negligência, por força das disposições conjugadas dos art.ºs 13.º e 225.º do Código Penal.

Caso o agente actue em eventuais estados de erro sobre os elementos típicos, *v.g.* representando falsamente a cobertura quanto ao pagamento, parece que faltará o elemento

[31] *Idem ibidem*, p. 380.
[32] Possibilidade que chegou a ser ponderada, mas que foi posteriormente abandonada – cfr. Actas n.ºs 48 e 52 da Comissão de Revisão, *op. cit.*, 1993, pp. 520 e 541.
[33] Neste sentido, veja-se Claudia Pecorella, *Il nuovo diritto penale delle "carte di pagamento"*, *in* Revista Italiana de Diritto e ProceduraPenale, 1, 1993, p. 240, e M. Miguez Garcia e J.M. Castela Rio, Código Penal – Parte Geral e Especial, Almedina, 2015, pp. 1001 e 1002.
[34] Actas n.ºs 48 e 52 da Comissão de Revisão, *op. cit.*, 1993, p. 520 e 541. Tendo chegado a ser, inclusivamente, proposto a alteração da redacção para: "*Quem com intenção de obter para si ou para terceiro enriquecimento ilegítimo, abusar da possibilidade, que lhe é conferida pela posse de cartão, ..., de levar o emitente ... causar prejuízo a este ou a outra pessoa*". Todavia, entendendo Sousa e Brito que o paralelismo deste crime se devia fazer com o crime de infidelidade e não com o crime de burla, a sua redacção, acabou por ser: "*Quem, abusando ... causar prejuízo ...*"

típico "abuso", ou no erro quanto à possibilidade de compensar ou regularizar um débito, eventualmente faltará o dolo quanto ao prejuízo patrimonial[35].

4. Causas de exclusão da ilicitude e da culpa

Para que se possa afirmar que o agente verdadeiramente cometeu um crime, é necessário a verificação do preenchimento dos pressupostos da ilicitude e da culpa, ou seja, para que um facto seja punível, para além de ser necessariamente típico, terá que ser ainda ilícito e culposo.

Quer isto dizer e, desde logo, no que ao pressuposto da ilicitude concerne (que consiste na desconformidade da conduta com o direito ou lesão de interesses juridicamente protegidos) ser necessário verificar se existe alguma causa de justificação ou de exclusão da ilicitude, de forma a afirmarmos se estamos (ou não) perante um crime.

Isto porque, «o direito penal, como qualquer ramo do direito, existe para se aplicar às concretas situações da vida social. E estas situações ou casos concretos podem apresentar-se como relativamente simples ou como realmente complexas (…) quer isto significar que um facto que, em princípio, i. é, em abstracto, constitui um tipo de ilícito, pode, em concreto, por força das circunstâncias em que é praticado, transformar-se num facto justificado, aprovado pela ordem jurídica e, portanto, não ilícito»[36].

Por seu lado, a culpa, enquanto elemento do crime, assenta na capacidade do agente em avaliar a ilicitude no momento da prática do facto ou de se determinar de acordo com essa avaliação, e traduz-se num juízo de censurabilidade dirigido ao agente por ter actuado daquela forma.

Assim, para que haja crime é necessário que a conduta que constitui um tipo de ilícito (seja activo ou omissivo, doloso ou negligente) possa ser censurada, ético-pessoalmente, ao seu autor a título de culpa[37]. Tal exigência, portanto, não é mais do que a concretização do princípio *nulla poena sine culpa,* que estabelece que não pode haver sanção criminal sem culpa e que a medida da pena não pode nunca ultrapassar a medida da culpa (artigo 13.º e artigo 40.º, n.º 2, do Código Penal)[38].

Sobre o tema Damião da Cunha afirma serem de aplicar as regras gerais das causas de justificação, incluindo o direito de necessidade, bem como hipóteses de actuação com base num estado de necessidade desculpante[39].

[35] Damião da Cunha, *op. cit.*, 2009, p. 380.
[36] Américo Taipa de Carvalho, Direito Penal - Parte Geral - Questões Fundamentais – Teoria Geral do Crime, Coimbra Editora, 2.ª ed, 2014, pp. 256 e 257.
[37] *Idem ibidem*, p. 260.
[38] Sobre a fundamentação da culpa jurídico-penal, veja-se Jorge de Figueiredo Dias, Direito Penal, Parte Geral, Tomo I, 2.ª ed, Coimbra Editora, 2007, pp. 510 a 559.
[39] *Op. cit.*, 2009, p. 380.

5. A pena e o regime punitivo

Nos termos do disposto no n.º 1 do art.º 225.º do Código Penal, o crime de abuso de cartão de garantia ou de crédito é punido com pena de prisão até 3 anos ou com pena de multa.

No entanto, este artigo prevê no seu n.º 5 duas situações de agravação em função do valor do prejuízo. No primeiro caso, se o prejuízo for de valor elevado (cfr. art.º 202.º, al.ª a), do Código Penal), o crime passa a ser punido com pena de prisão até 5 anos ou com pena de multa até 600 dias. No segundo caso, se o prejuízo for de valor consideravelmente elevado (cfr. art.º 202.º, al.ª a), do Código Penal), o crime é punível com pena de prisão de 2 a 8 anos.

Nos termos do n.º 4 do artigo em causa, é também aplicável a este crime o regime da reparação previsto no art.º 206.º do Código Penal.

Assim, extingue-se a responsabilidade criminal, mediante a concordância do ofendido e do arguido, sem dano ilegítimo de terceiro, até à publicação da sentença da 1.ª instância, desde que tenha havido reparação integral do prejuízo causado (cfr. n.º 1 do referido art.º 206.º). E, se a reparação for apenas parcial, a pena pode ser especialmente atenuada, nos termos do disposto no art.º 73.º do Código Penal (cfr. n.º 3 do referido art.º 206.º).

Deve notar-se, no entanto, que estando em causa a actuação pelo titular ou por pessoas, a qualquer título, legitimadas a usar o cartão, deverão ter-se em atenção as regras contratuais próprias estabelecidas no contrato de emissão. Pois, nestes casos pode haver situações em que a própria entidade emissora crie mecanismos de reparação contratualmente estabelecidos que podem afastar a responsabilidade por este crime[40].

6. Natureza do crime

O n.º 3 do art.º 255.º do Código Penal estabelece que o procedimento criminal depende de queixa quando o crime é simples nos termos do n.º 1 do mesmo artigo.

Isto significa que apenas assiste legitimidade ao Ministério Público para prosseguir com o procedimento criminal se o ofendido/lesado apresentar queixa, conforme estabelece o art.º 49.º, n.º 1, do Código do Processo Penal. Na ausência desta manifestação de vontade, o Ministério Público não pode avançar com o procedimento criminal (cfr. art.º 48.º do Código do Processo Penal).

Por força da remissão nos n.ºs 4 e 6 do citado art.º 255.º para o art.º 207.º do Código Penal, pode o mesmo procedimento criminal depender de acusação particular.

Isto significa que apenas assiste legitimidade ao Ministério Público para prosseguir com o procedimento criminal se o ofendido/lesado apresentar queixa, se constitua assistente e

[40] Neste sentido, Damião da Cunha, *op. cit.*, 1999, p. 382.

deduza acusação particular, conforme estabelece o art.º 50.º, n.º 1, do Código do Processo Penal.

Nos termos daquela remissão, "o procedimento criminal depende de acusação particular se: *a)* O agente for cônjuge, ascendente, descendente, adoptante, adoptado, parente ou afim até ao 2.º grau da vítima, ou com ela viver em condições análogas às dos cônjuges; ou *b)* A coisa furtada ou ilegitimamente apropriada for de valor diminuto e destinada a utilização imediata e indispensável à satisfação de uma necessidade do agente ou de outra pessoa mencionada na alínea a)".

A referência ao art.º 207.º justifica-se principalmente quando o ofendido/lesado for o titular do cartão; mas é também aplicável a outros possíveis ofendidos/lesados da prática do crime (a entidade emitente do cartão ou, eventualmente, o comerciante), se o agente tiver uma das qualidades previstas na al.ª a) do art.º 207.º ou se verificar a situação prevista na al.ª b) do artigo[41].

O titular do direito de queixa é, em regra, o ofendido, considerando-se como tal o titular dos interesses protegidos pela incriminação, isto é, o portador do bem jurídico protegido, segundo o disposto no n.º 1 do art.º 113 do Código Penal. No crime em apreço têm legitimidade para apresentar queixa os lesados pela conduta abusiva, ou seja, o titular do cartão, o emitente do cartão ou o comerciante, consoante os casos.

Todavia, nos casos em que o crime é qualificado em razão do valor nos termos do n.º 5 do art.º 225.º, do Código Penal, este reveste natureza pública, o que significa que não é necessário queixa por parte do titular, dispondo o Ministério Público de legitimidade para prosseguir a acção penal, nos termos do disposto no art.º 48º do Código de Processo Penal, a partir do momento em que adquire a notícia do crime nos termos do disposto nos art.ºs 241.º e ss. do mesmo diploma.

7. A tentativa

Nos termos do disposto no n.º 2 do art.º 255.º do Código Penal, a tentativa é punível.

Há tentativa quando o agente pratica actos de execução de um crime que decidiu cometer, sem que este chegue a consumar-se. A definição legal da tentativa encontra-se no art.º 22.º Código Penal, enquanto o n.º 1 do art.º 23.º Código Penal estatui quando e o n.º 2 como a tentativa é punível.

Assim, tendo em atenção os eventuais sistemas de segurança que são inerentes ao uso de cartões de garantia ou de crédito, é possível que possam ocorrer situações em que o agente

[41] «Poder-se-á dizer da previsão do artigo207.º, al. b), do CP que ela se propõe uma finalidade que como que complementa a justificação do facto assente no direito de necessidade ou no estado de necessidade desculpante, destinando-se a dar um tratamento benévolo aos casos em que, embora sem os pressupostos de facto e de direito para neles se enquadrarem, estão próximos destas figuras jurídicas» - Ac. do STJ de 25/10/2007, proc. n.º 06P1946, relatado por Souto de Moura, disponível na página de Internet em www.dgsi.pt.

use abusivamente o cartão sem conseguir a produção do resultado, por motivos alheios à sua vontade, ficando-se pela tentativa.

A tentativa será punível com a pena aplicável ao crime consumado, mas especialmente atenuada nos termos do disposto nos art.ºs 72.º e 73.º Código Penal. Nestes casos, não existe apenas uma possibilidade de atenuação por parte do juiz, mas antes um dever. A atenuação especial tem que ser feita sempre que se verifique a tentativa punível.

8. A utilização indevida do cartão (de crédito) e o concurso de crimes

Hoje em dia a utilização de cartões de crédito está massificada (já não tanto quanto aos cartões de garantia) e é uma das formas mais comuns de pagamento para compras de bens e serviços, sendo igualmente cada mais frequentes acções criminosas que têm por objecto a sua utilização.

Assim, depois de analisado os elementos que compõem o crime de abuso de cartão de garantia ou de crédito, impõe-se agora realizar uma pequena abordagem às diversas condutas criminosas susceptíveis de incidir sobre o cartão de crédito, de forma distinguir as situações, nem sempre claras, em que se verifica um concurso aparente de normas.

Portanto, na determinação da responsabilidade criminal dos agentes podem ocorrer situações de anulação ou concurso (aparente ou real) de crimes, sempre que o agente com a sua conduta cometa uma pluralidade de crimes ou aquela possa aparentemente preencher vários tipos legais de crime. Situações que são muitos frequentes quando está em causa a utilização indevida do cartão.

A teoria do concurso permite distinguir os casos nos quais as normas em concurso requerem uma aplicação conjunta, das situações em que o conteúdo da conduta é absorvido por uma única das normas[42].

Assim, no "*concurso real/efectivo ou concurso de crimes*" existe uma situação em que o agente comete efectivamente vários crimes e ele é responsável por todos eles, ao passo que no "*concurso aparente ou concurso de normas*" existe uma situação em que o agente aparentemente preenche com a sua conduta vários crimes, mas na verdade é um só crime.

O art.º 30.º, n.º 1, do Código Penal vai ao encontro dessas realidades, dispondo que o número de crime determina-se pelo número de tipos efectivamente cometidos (concurso real), ou pelo número de vezes que o mesmo crime for cometido (concurso aparente).

[42] Citando M. Miguez Garcia, O Risco de Comer uma Sopa e Outros Casos de Direito Penal, Almedina, 2012, p. 734: «a teoria do concurso tem como ponto de partida clarificar a seguinte questão: quais as opções, no seio do direito penal, quando uma e a mesma pessoa – seja com uma só acção, seja com várias acções – viola vários tipos de crime ou viola o mesmo tipo de crime várias vezes de modo ilícito e culposo, podendo ser em qualquer modalidade de autoria ou de comparticipação».

O Código Penal não dispõe de directrizes sobre a resolução das situações de concurso real ou aparente de crimes, remetendo, assim, para a doutrina que vem resolvendo o concurso aparente através da relação de *especialidade*[43], de *subsidiariedade*[44] ou de *consumpção*[45] entre os crimes, onde uma das normas prevalecerá sobre as outras[46].

8.1. Falsificação ou clonagem do cartão

A clonagem de cartões (ou também conhecido por "*Skimming*") consiste em regravar os dados (informáticos) dos cartões noutros cartões que contenham banda magnética, para que depois sejam utilizados na rede automática que gere os cartões como se fossem verdadeiros.

Esta operação é usualmente realizada através de mecanismos sofisticados que podem ser colocados nas fendas das caixas de multibanco (ATM) ou mesmo em locais de prestação de serviços (v.g. lojas e restaurantes) - os chamados *point of sale* (POS) -, que recolhem e gravam as informações constantes nas respectivas bandas magnéticas dos cartões, incluindo o código PIN, sendo depois utilizados para realizar as mais diversas operações comerciais, nomeadamente compras em terminais de pagamentos ou compras *on line*, como também podem ser ainda utilizados para fazer levantamentos de dinheiro na modalidade de *cash advance*.

Não raras vezes, esses "cartões" falsificados podem também ser vendidos *on line,* normalmente em *sites* especializados para a prática de condutas criminosas, localizados na *deep web*[47].

A captura da informação existente na banda magnética de cartão de crédito constitui a prática do crime de falsidade informática, p. e p. pelo art.º 3.º, n.ºs 1 e 2, da Lei n.º 109/2009, de 15 de Setembro (Lei do Cibercrime), que diz: "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

[43] Verifica-se quando duas normas se encontram numa relação de género e espécie, ou seja, quando duas normas têm os mesmos elementos típicos, mas uma delas apresenta ainda outros elementos distintivos que a particularizam.
[44] Casos em que a norma vê a sua aplicabilidade condicionada pela não aplicabilidade de outra norma, só se aplicando a norma subsidiária quando a outra não se aplique. A norma prevalecente condiciona de certo modo o funcionamento daquela que lhe é subsidiária.
[45] Quando a norma tem uma discrição típica suficientemente ampla que abranja os elementos da discrição típica da outra norma.
[46] Para um estudo mais aprofundado sobre o concurso de normas, veja-se Germano Marques da Silva, Direito Penal Português, Parte Geral I, Editorial Verbo, 1997, pp. 305 a 321.
[47] Caso paradigmático desta nova realidade pode ser resumido na acção encoberta liderada pelo Federal Bureau of Investigation (FBI) dos Estados Unidos, na "Operação DarkMarket", que contou com colaboração dos órgãos policiais da Alemanha, Reino Unido, Turquia e de outros países, e que culminou no fecho da página da *DarkMarket* em 04/10/ 2008, localizado na *deep weeb*, e levou à detenção de 59 pessoas espalhadas por vários locais do mundo, tendo impedido que mais 70 milhões de dólares fossem retirados das contas das vítimas. O *DarkMarket* era um *site* alojado na "parte escondida" da Internet onde ladrões de identidade podiam comprar e vender números de cartões de crédito e credenciais de login (nomes de utilizador, senhas) subtraídos das vítimas – principalmente através do método de *phishing* –, identidades falsas e ferramentas para fazer cartões de crédito falsos. Este *site* tinha no seu auge 2500 utilizadores.

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"[48].
A falsificação de cartão em si mesmo, ou seja, o fabrico de cartão de crédito falso com inserção de banda magnética clonada de um cartão verdadeiro, constitui a prática do crime de contrafacção de moeda falsa, p. e p. pelas disposições conjugadas dos art.ºs 262.º, n.º 1 e 267.º, n.º 1, al.ª a), do Código Penal, que dizem: " 1 - Quem praticar contrafacção de moeda, com intenção de a pôr em circulação como legítima, é punido com pena de prisão de três a doze anos", e "1 - Para efeitos do disposto nos artigos 262.º a 266.º, são equiparados a moeda: (...) c) Os cartões de garantia ou de crédito"[49].

Já a utilização destes "cartões" falsificados por pessoas não autorizadas, com a introdução do código PIN ou com a introdução do numero de cartão de crédito em transacções *on line*, constitui a prática do crime de burla informática, p. e p. pelo art.º 221.º, n.º 1, do Código Penal, que diz: "*1 - Quem, com intenção de obter para si ou para terceiro enriquecimento ilegítimo, causar a outra pessoa prejuízo patrimonial, interferindo no resultado de tratamento de dados ou mediante estruturação incorrecta de programa informático, utilização incorrecta ou incompleta de dados, utilização de dados sem autorização ou intervenção por qualquer outro modo não autorizada no processamento, é punido com pena de prisão até 3 anos ou com pena de multa*"[50].

Esta forma de utilização do cartão constitui a prática do crime de burla informática, porquanto, «a burla informática, na construção típica e na correspondente execução vinculada, há-de consistir sempre em um comportamento que constitua um artifício, engano ou erro consciente, não por modo de afectação directa em relação a uma pessoa (como na burla - artigo 217.º do CP), mas por intermediação da manipulação de um sistema de dados ou de tratamento informático, ou de equivalente utilização abusiva de dados»[51].

Para além do mais, resulta da intenção da Comissão de Revisão excluir da previsão legal do crime de abuso de cartão de garantia ou de crédito a utilização destes em sistemas automatizados de pagamento, por esta conduta já estar incluída no crime de burla informática[52].

Existe assim, nestes casos, um concurso efectivo entre os crimes de falsidade informática, contrafacção de moeda falsa e de burla informática, no caso em que o agente da burla informática seja também aquele que captura os dados do cartão e procede à falsificação do

[48] Assim decidiu, o Ac. do TRP de 17.04.2014, proc. n.º 2013/13.3JAPRT.P1, relatado por Coelho Vieira, disponível na página da Internet em www.dgsi.pt.
[49] *Idem ibidem*.
[50] Para um estudo aprofundado sobre o crime de burla informática nesta matéria, veja-se Ana Helena França Azevedo, Burlas Informáticas: Modos de Manifestação, Tese de Mestrado, Escola de Direito da Universidade do Minho, 2016.
[51] Neste sentido, Ac. do STJ de 05.11.2008, proc. n.º 08P2817, relatado por Henriques Gaspar, disponível na página de Internet em www.dgsi.pt.
[52] Acta n.º 39 da Comissão de Revisão, *op. cit.*, 1993, p. 451.

cartão[53], estando aquele em concurso aparente com o crime de abuso de cartão de garantia ou de crédito.

Por seu lado, sendo os cartões de crédito equiparados a moeda equiparado pelo art.º 267.º, n.º 1, al.ª c), do Código Penal, a venda destes "cartões" falsificados constitui a prática do crime de passagem de moeda falsa de concerto com o falsificador, p. e p. pelo art.º 264.º do Código Penal, que diz: "*1 - Nas penas indicadas nos artigos 262.º e 263.º incorre quem, concertando-se com o agente dos factos neles descritos, passar ou puser em circulação por qualquer modo, incluindo a exposição à venda, as ditas moedas*"[54].

Aos quais pode acrescer ainda o crime de falsificação de documento, nos termos do disposto no art.º 256.º, n.º 1, al.ª c), do Código Penal, quando haja lugar à utilização do cartão "falso" com recurso à assinatura em talão de pagamento por terceiro não autorizado, como se fosse o seu legítimo titular[55]. Com efeito, em certos terminais automáticos de pagamento, para além da introdução do código PIN, é ainda emitido um talão com os dados da operação que deve ser assinado pelo apresentante do cartão e corresponder ao seu titular.

8.2. Detenção ilegítima do cartão

Situação frequente consiste também na detenção ilegítima do cartão de crédito alheio e obtenção do código PIN, por meio de apropriação, subtracção ou constrangimento a que lhe seja entregue, incluindo através do uso de violência, e na utilização posterior desse cartão para realizar as mais diversas operações comerciais e financeiras ou fazer levantamentos de dinheiro na modalidade de *cash advance*, com a introdução do código PIN em sistemas automáticos de pagamento ou com a introdução do numero de cartão de crédito em transacções *on line*.

A jurisprudência tem-se pronunciado, de forma quase unânime no sentido de que estas situações integram a previsão do crime de burla informática, previsto no art.º 221.º do Código Penal, pelos motivos já apresentados no subcapítulo anterior[56].

Acertadamente, cremos, parte da jurisprudência entende ainda a existência nestes casos de concurso real entre o crime de burla informática e os crimes de apropriação ilegítima em caso de acessão ou de coisa achada, furto ou roubo, conforme a situação que levou à sua detenção ilegítima, (previstos, respectivamente, nos art.ºs 209.º, n.ºs 1 e 2, 203.º, n.º 1 e 210.º, n.º 1 do Código Penal), pois, visando aquele crime não só a protecção do património da vítima, mas

[53] Assim decidiram, o Ac. do TRL de 30.06.2011, proc. n.º 189/09.3JASTB.L1-5, relatado por Filomena Lima, o Ac. do TRP de 14.09.2016, proc. n.º 2177/09.0PAVNG.P1, relatado por Ernesto Nascimento, e o Ac. do TRP de 21.11.2011, proc. n.º 1001/11.9JAPRT.P1, relatado por Borges Martins, disponíveis na página de Internet em www.dgsi.pt.
[54] Assim decidiu, o Ac. do STJ de 12.09.2012, proc. n.º 1008/11.6JFLSB-L1.S1, relatado por Armindo Monteiro, disponível na página de Internet em www.dgsi.pt.
[55] Assim decidiu, o Ac. do TRL de 10.07.2012, proc. n.º 7876/10.1JFLSB.L1-5, relatado por Luís Gominho, disponível na página de Internet em www.dgsi.pt.
[56] Assim decidiram, entre muitos outros, o Ac. do STJ de 27.06.2001, proc. n.º 01P1800, relatado por Leal Henriques, e o Ac. do TRG de 18.12.2012, proc. n.º 541/10.GAPTB.G1, relatado por Ana Teixeira, disponíveis na página de Internet em www.dgsi.pt.

também o sigilo e a fiabilidade dos meios informáticos e de telecomunicações, não há consumpção entre os crimes[57].

Quanto ao crime de abuso de cartão de crédito ou de garantia, também aqui este se encontra naquelas situações numa relação de concurso aparente com aqueles crimes.

8.3. Caso prático na jurisprudência[58]

No Tribunal Judicial da Comarca de Vale de Cambra, o Ministério Público deduziu acusação, em processo comum, com intervenção do tribunal singular, fazendo uso do disposto no art.º 16.º, n.º 3, do CPP, contra a arguida, imputando-lhe a prática, como autora material, de um crime de furto simples p. e p. no art.º 203.º, n.º 1 e de um crime de abuso de cartão de crédito p. e p. no art.º 225.º, n.º 1, ambos do Código Penal.

Uma vez realizada a audiência de julgamento foi proferida a sentença, pela qual se decidiu:

a) Condenar a arguida, como autora material, de um crime de furto p. e p. no artigo 203.º, n.º 1, do C. Penal, na redacção do DL 48/95, de 15/03, na pena de 70 dias de multa, à taxa diária de 700$00;

b) Absolver a arguida do crime de abuso de cartão de crédito de que vinha acusada.

A arguida interpôs recurso para o Tribunal da Relação do Porto, pugnando pela absolvição da prática do crime de furto.

Na resposta, o Ministério Público defendeu o não provimento do recurso, devendo ainda a arguida ser condenada pelo crime de abuso de cartão de crédito.

Da matéria de facto dada como provada, resulta o seguinte:

«**1)** No período compreendido entre as 20h e as 22h do dia 13 de Fevereiro de 1999, a ofendida Maria... esteve a trabalhar, como operadora de caixa, nas instalações do hipermercado "M...", sitas no Lugar de..., ..., Vale de Cambra;

2) A arguida trabalhava como supervisora no mesmo estabelecimento.

3) De modo que não foi possível apurar, a arguida apoderou-se da carteira da ofendida, contendo, para além de documentos pessoais como o BI, carta de condução, cartão de contribuinte, cartão de beneficiária da SS, cartão de eleitora, cartão jovem, ainda um cartão multibanco emitido pela CGD e um cartão "visa universo", tudo pertencente à ofendida.

[57] Neste sentido, entre outros, o Ac. do STJ de 06.10.2005, proc. n.º 05P2253, relatado pro Simas Santos, e o Ac. do TRC de 29.02.2012, proc. n.º 183/10.1GATBU.C1, relatado por Paulo Valério, disponíveis na página de Internet em www.dgsi.pt.
[58] TRP de 08.03.2000, proc. n.º 0010659, relatado por Marques Pereira, disponível na página de Internet em www.dgsi.pt.

4) Apoderou-se dessa carteira, bem como do seu conteúdo, sem a autorização e contra a vontade da ofendida.

5) Uma vez na posse daqueles documentos e cartão de crédito, a arguida decidiu usar este para seu benefício pessoal.

6) E assim, cerca das 13h, do dia 14 de Fevereiro de 1999, a arguida utilizou o cartão "visa universo" pertencente à ofendida, para pagar a quantia de 670$00 de compras, e para retirar 15.000$00 da caixa.

7) O que fez numa das caixas daquele hipermercado, onde a arguida estava a operar, sem a autorização e contra a vontade da ofendida.

8) Por essa via, a arguida viu o seu património acrescido daquele montante, no qual a ofendida ficou prejudicada.

(...)

11) A arguida agiu de forma livre, deliberada e consciente.

12) Sabia que a sua conduta não lhe era permitida e que era punida por lei».
Segundo a apreciação feita em sede de recurso:

«Sustenta-se, na decisão recorrida, que tais factos integram a prática de um crime de furto, porque "a arguida usou (...) um cartão alheio, de uma conta alheia, apropriando-se de dinheiro de outrem, sem conhecimento e contra a vontade do dono, com intenção de o utilizar em proveito próprio ou de terceiro".

Quanto a nós, parece-nos, tal como entende o MP, ocorrer um crime de abuso de cartão de crédito p. e p. no artigo225, n.º 1, do C. Penal (na redacção dada pelo DL n.º 48/95, de 15/03).

Segundo este artigo: 1.Quem, abusando da possibilidade, conferida pela posse de cartão de garantia ou de crédito, de levar o emitente a fazer um pagamento, causar prejuízo a este ou a terceiro é punido com pena de prisão até 3 anos ou com pena de multa.

(...)

Ora, em face dos factos provados, acima relatados, todos os elementos essenciais do mencionado crime (objectivos e subjectivos) se mostram verificados.

Com efeito, tendo utilizado o cartão de crédito da ofendida, sem o acordo desta, para, com ele, fazer um pagamento e retirar dinheiro de uma caixa do estabelecimento comercial em que trabalhava, não há dúvida de que a arguida abusou da possibilidade conferida pela posse do

mesmo cartão de levar o emitente a fazer um pagamento, causando prejuízo patrimonial à própria titular do cartão.

Por outro lado, tendo agido livre e conscientemente, sabendo da ilicitude da sua conduta, está verificado o dolo, que o presente tipo legal supõe (que abrange o abuso e o prejuízo patrimonial).

(...)

Em face do exposto, acordam os Juízes desta Relação em negar provimento ao recurso, mas, alterando a qualificação jurídico-penal dos factos provados, em causa, condenam a arguida..., como autora material de um crime de abuso de cartão de crédito previsto e punido no artigo 225.º, n.º 1, do Código Penal, na pena determinada na sentença recorrida, isto é, na pena de 70 (setenta) dias de multa, à taxa diária de 700$00 (setecentos escudos), o que se traduz na quantia de 49.000$00 (quarenta e nove mil escudos)».

À primeira vista este acórdão não parece ser muito esclarecedor porque é que a conduta da arguida foi subsumida aos elementos típicos do crime de abuso de cartão de garantia ou de crédito, p. e p. pelo art.º 225.º, n.º 1, do Código Penal, e não antes do crime de burla informática, p. e p. pelo art.º 221.º, n.º 1, do Código Penal, afastando-se, assim, das considerações que fizemos nos subcapítulos anteriores.

Todavia, uma leitura mais atenta do acórdão explica essa diferença de tratamento.

Com efeito, não resulta daquele aresto que o cartão de crédito tenha sido usado pela arguida num terminal automático de pagamento mediante a introdução do código PIN, mas sim que aquela assinou o talão emitido pelo comerciante, com a assinatura correspondente à do titular do cartão.

Neste caso, estávamos perante um cartão de crédito simples, ou seja, sem os actuais mecanismos de segurança contra fraude, e sem que houvesse comunicação instantânea entre o terminal de pagamento do comerciante e o sistema informático da entidade emitente, tendo sido assim a suposta assinatura do titular do cartão que validou a transacção, em substituição da introdução de um código PIN.

Desta forma, efectivamente, a lesão do património não se produziu através da intromissão nos sistemas e da utilização em certos termos de meios informáticos, mediante a execução de interferência "no resultado de tratamento de dados ou mediante estruturação incorrecta de programa informático", na "utilização incorrecta ou incompleta de dados", em "utilização de dados sem autorização" ou na "intervenção por qualquer outro modo não autorizada no processamento".

Razão pela qual, não estão preenchidos os elementos típicos previstos no crime de burla informática, e o crime de abuso de cartão de garantia ou de crédito, neste caso, encontra-se

numa relação de concurso aparente com o crime de falsificação de documento, p. e p. pelo art.º 256.º, n.º 1, al.ª c), do Código Penal.

9. O crime continuado

O crime continuado encontra-se previsto no artigo 30.º, n.º 2, do Código Penal, segundo o qual: "2 — Constitui um só crime continuado a realização plúrima do mesmo tipo de crime ou de vários tipos de crime que fundamentalmente protejam o mesmo bem jurídico, executada por forma essencialmente homogénea e no quadro da solicitação de uma mesma situação exterior que diminua consideravelmente a culpa do agente."

Constituem-se assim, como pressupostos da ocorrência de crime continuado:

a) A realização plúrima do mesmo tipo de crime ou de vários tipos que protejam fundamentalmente o mesmo bem jurídico.

b) A homogeneidade da forma de execução.

c) A persistência de uma "situação exterior" que facilita a execução e que diminui consideravelmente a culpa do agente.

Segundo o Acórdão do STJ de 20/10/2010, proc. n.º 78/07.6JAFAR.E2.S1, relatado por Pires da Graça, relativo à utilização de cartões de crédito falsificados em operações de levantamento de dinheiro em caixas multibanco (ATM), e onde se discutia a prática do crime de burla informática, na forma continuada, este afastou essa continuação, dizendo:

«Da matéria de facto provada não resulta, efectivamente, configurada a actuação do arguido no "quadro da solicitação de uma mesma situação exterior", que lhe tenha propiciado e facilitado a repetição das suas acções.

O que se alcança da matéria provada é que o arguido concebeu um esquema para cometer múltiplos crimes e procurou os meios aptos para os levar a cabo, não tendo deparado "com uma situação exterior" que o tenha levado a repetir a sua actuação, por esta se mostrar facilitada (…)

(…) "não é suficiente a utilização de um mesmo cenário ou plano de actuação, ou ainda como no caso dos autos a prática do mesmo tipo de crime, durante um determinado período em que se verifica até uma certa proximidade temporal entre os factos praticados (...) [ou seja] *o facto de se terem passado sensivelmente no mesmo local ou junto da mesma caixa, não é situação exterior que revele uma menor culpa (...)"».*

Apesar do acórdão em causa não se referir em concreto ao crime de abuso de cartão de garantia ou de crédito, a sua fundamentação pode ser perfeitamente transposta para este

crime, atenta a similitude que se apresenta por vezes a utilização abusiva dos cartões de débito e os cartões de crédito.

Portanto, apesar de ser possível haver casos em que estejamos perante um crime de abuso de cartão de garantia ou de crédito na forma continuada, no qual é preciso identificar em concreto a "situação exterior" que facilita a execução e que diminui consideravelmente a culpa do agente, essa verificação perante o caso concreto pode ser difícil, não bastando, como se viu, a utilização de um mesmo cenário ou plano de actuação durante um determinado período em que se verifica até uma certa proximidade temporal entre os factos praticados.

10. Gestão processual

Nos termos do disposto no art.ºs 262.º, n.º 1, e 263.º do Código de Processo Penal, o inquérito é da competência do Ministério Público e compreende o conjunto de diligências que visam investigar a existência de um crime, determinar os seus agentes e a responsabilidade deles e descobrir e recolher provas, em ordem à decisão sobre a acusação, cabendo a este, por regra, praticar os actos e assegurar os meios de prova necessários à realização das referidas finalidades (cfr. art.º 267.º do Código de Processo Penal).

O objectivo da investigação criminal tem por base reunir indícios que permitam concluir pela prática (ou não) de determinados factos que preenchem os tipos legais de crimes. Pretende, portanto, apurar-se que crime ocorreu, quando e onde ocorreu, bem como quem e que circunstâncias o praticou. Porém, além disso, na investigação criminal devem também recolher-se elementos de prova quanto aos factos que determinem a punibilidade ou não e, bem assim, quanto a factos que levem à determinação concreta da medida da pena.

A lei não indica quais os actos de inquérito que devem ser praticados pelo Ministério Público, o que, aliás, seria impossível, para além de uma referência genérica, deixando ao critério deste a escolha de quais os actos necessários à realização da finalidade do inquérito. Isto sem prejuízo de a lei impor a prática de certos actos de inquérito, como é o caso do interrogatório do arguido, nos termos do art.º 272.º do Código de Processo Penal.

Assim, como é referido por Germano Marques da Silva, «competindo a direcção do inquérito ao Ministério Público, não é curial que o Juiz possa intrometer-se na actividade de investigação e recolha de provas, salvo se se tratar de actos necessários à salvaguarda dos direitos fundamentais. A direcção do inquérito pertence ao Ministério Público e só a ele compete decidir quais os actos que entende dever levar a cabo para realizar as finalidades do inquérito. Para a prática de algum desses actos pode necessitar da intervenção do juiz, quer para os consentir quer mesmo para os praticar, mas só por sua promoção podem ter lugar, a menos que se trate de actos necessários à salvaguarda de direitos fundamentais dos requerentes (...) Ora se a lei confia ao Ministério Público a direcção da investigação, permitindo-lhe dispor quais os actos que entenda necessários à realização da finalidade do inquérito, não se

compreenderia que depois submetesse a actividade desenvolvida a fiscalização judicial. O que fica sujeito a fiscalização judicial é a decisão do Ministério Público no termo do inquérito»[59].

Como é sabido, entre nós foi consagrado em processo penal a regra geral da admissibilidade de todas as provas que não forem proibidas por lei, significando assim, em termos muito simples, que todas as provas serão legalmente admissíveis mesmo que não se encontrem tipificadas na lei (provas atípicas), desde que não sejam proibidas por qualquer disposição legal – princípio da legalidade da prova e princípio da inadmissibilidade das provas proibidas (cfr. art.ºs 125.º e 126.º do Código de Processo Penal)[60].

Porque para além da função de realização da justiça por parte do Estado se torna igualmente necessário por parte deste proteger os direitos fundamentais dos intervenientes envolvidos, uma investigação criminal deve ser eficaz e eficiente. Eficaz no sentido de atingir o objectivo pretendido, e eficiente no sentido de atingir um objectivo definido da melhor forma possível.

Portanto, uma investigação eficiente é aquela que é planeada, organizada – se possível temporizada –, por forma a reunir, no mais curto espaço de tempo, toda a prova da existência do crime e de quem são os seus autores[61].

Assim sendo, uma vez recebida a notícia do crime, cumpre desde logo, num primeiro momento, fazer uma análise cuidada do conteúdo do Auto de Notícia/Denuncia/Queixa, tendo em vista:

– Encontrar as omissões de dados e factos fundamentais (localização no tempo e espaço) que podem ser de imediato colmatadas;

– Delimitar o âmbito da investigação, pela selecção dos factos nucleares;

– Decidir qual a prova necessária e os meios de recolha de prova mais adequados para a sua recolha;

– Decidir quem pratica os actos de investigação (Ministério Público ou Órgão de Policia Criminal)[62].

Como é compreensível, não cumpre aqui descrever os vários passos que devem ser tomados durante uma investigação pela prática do crime de abuso de cartão de garantia ou de crédito,

[59] Curso de Processo Penal, Tomo III, 2.ª Ed., Editorial verbo, 2000, pp. 85 e 86.
[60] A investigação criminal enquanto processo de procura e recolha de indícios e de vestígios da prática de infracções penais move-se dentro de um quadro normativo juridicamente complexo entre a prova conseguida e a prova aceite, de modo a prevenir a prática de abusos. A procura e recolha de prova que conduza ao esclarecimento da verdade material em tribunal dos factos ocorridos que consubstanciam a prática de um crime, quer objectivamente, quer subjectivamente, não é mais do que a realização prática das finalidades do Direito Penal na realização da justiça por parte do Estado.
[61] Neste sentido, Maria José Fernandes, Investigação Criminal e Gestão de Inquérito: práticas de optimização de meios (materiais e humanos) e de métodos de trabalho condicionantes do êxito da investigação, in "Gestão processual: agenda, conclusões, serviço urgente e serviço diário, provimentos e ordens", Centro de Estudos Judiciários, 2013, p. 121.
[62] *Idem ibidem*.

porquanto, todas as investigações criminais são dinâmicas, no sentido em que cada caso é um caso, devendo proceder-se à recolha da prova mediante o uso dos meios mais adequados e eficazes previstos na lei, conforme essa necessidade vai sendo reclamada no tempo (processual).

Em todo o caso, existem certos procedimentos comuns que não podem deixar de ser observados na investigação deste tipo de crime.

Assim:

– Deve ter-se acesso ao contrato de concessão ou emissão do cartão de garantia ou de crédito em causa, para, dentro das obrigações contratualmente estabelecidas, se apurar quem suporta o prejuízo no caso de utilização abusiva do cartão e, assim, se apurar quem tem a legitimidade para apresentar queixa no caso do crime revestir natureza semi-pública ou particular;

– Determinar se a utilização abusiva do cartão ocorreu num terminal automático pagamento, mediante a introdução do código PIN, pois neste caso estamos perante um crime de burla informática e não perante o crime de abuso de cartão de garantia ou de crédito;

– Procurar recolher toda a informação sobre a utilização abusiva do cartão, quer junto da entidade emitente, quer junto do comerciante, incluindo qualquer documento que o agente do crime possa ter assinado (v.g. o talão de comprovativo da transacção) e que possa levar à sua cabal identificação;

– Havendo um suspeito, se necessário, solicitar a realização de perícias forenses de escrita manual e recolha de amostras referência; e;

– Procurar obter os dados informáticos gerados pela operação, usando, sempre que necessário, as normas processuais de obtenção de prova digital prevista nos art.ºs 11.º a 17.º da Lei n.º 109/2009, de 15 de Setembro (Lei do Cibercrime), em especial a preservação expedita de dados.

Quanto a este último meio de obtenção de prova, ou seja a *preservação expedita de dados* (cfr. art.º 12.º, da Lei do Cibercrime), ele pode vir a ser muito importante neste tipo de investigação, e traduz-se na ideia que sempre que se afigurar necessário para a prova do crime e no decurso de uma investigação criminal em curso, a obtenção de dados informáticos (cfr. art.º 2.º, al.ª b), da Lei do Cibercrime) específicos armazenados em sistema informático – incluindo dados de tráfego – em relação aos quais haja receio de que possam perder-se, alterar-se ou deixar de estar disponíveis, a autoridade judiciária competente, ordena a quem tenha a disponibilidade ou controlo desses dados, designadamente a fornecedor de serviços, que preserve os dados em causa.

Podendo ainda a preservação expedita de dados ser ordenada pelos órgãos de polícia criminal nos casos previstos no n.º 2 do art.º 12.º da Lei do Cibercrime.

Esta medida destina-se a ser executada primordialmente pelos fornecedores de serviço de Internet, mas também o pode ser qualquer outra pessoa que tenha controlo sobre um sistema informático (cfr. art.º 2.º, al.ª a), da Lei do Cibercrime) onde os dados estejam armazenados.

A ideia principal a reter com a utilização deste meio de prova (assim como os restantes previstos na Lei do Cibercrime) é que o sucesso das investigações da criminalidade associada à informática e às redes de comunicações electrónicas exige, na maior parte dos casos, que as autoridades judiciárias e policiais tenham acesso aos elementos que compõem essas comunicações electrónicas e, por esta razão, os mesmos devem ser conservados previamente para o efeito.

Não se enumera outras diligências possíveis, porquanto, sintomático da pesquisa que fizemos, quer junto de alguns tribunais, quer junto da base de dados da jurisprudência, é o facto de existirem escassos casos em que este tipo legal de crime serviu de base a uma investigação criminal, e mais escassos ainda aqueles que chegaram a ser apreciados em sede de recurso. Não tendo sido encontrado nenhum processo por este crime que tenha sido investigado, julgado ou apreciado em sede de recurso nos últimos anos.

11. Conclusão

Na mesma altura em que foi introduzido o crime de abuso de cartão de garantia ou de crédito no Código Penal Português, foi igualmente introduzido o crime de burla informática, ambos assentes em pressupostos de criminalização diferentes.

Contudo, se em 1995 a criminalização da conduta prevista no crime de abuso de cartão de garantia ou de crédito era de alguma forma justificada, hoje em dia seria difícil encontrar essa justificação, concluindo-se que o crime de burla informática já tutela de forma satisfatória o bem jurídico protegido do património lesado com a utilização abusiva do cartão.

Com efeito, para além do cartão de garantia não ser muito utilizado em transacções (ao contrário do que sucede com os cartões de crédito), é preciso ter a noção que a partir do final da década de 90 do século passado a Internet e os sistemas informáticos dominaram o quotidiano da sociedade hodierna, facultando a comunicação e circulação de informação a nível transnacional, de forma instantânea e de fácil acesso, com custos relativamente baixos.

Esta massificação do uso da Internet provocou grandes benefícios para a actividade bancária e financeira, mas agravou de forma considerável os riscos associados à fraude de cartões, o que levou, por seu lado:

i) Que se abandonasse quase por completo os terminais manuais de pagamento com cartões;

ii) Que se adoptasse de forma generalizada os terminais automáticos de pagamento; e

iii) Que se instituísse fortes mecanismos de segurança, produzidos e desenvolvidos pela informática, para criar uma forma de protecção "física", prévia e eficaz, dos cartões e dos sistemas informáticos em que estes são usados.

A progressiva substituição dos cartões baseados na assinatura (equipadas com uma banda magnética para leitura) por cartões baseados no PIN (conformes á norma EMV), contribuiu para reduzir de modo significativo os abusos de utilização nos terminais de pagamento a nível europeu. Com efeito, no final de 2010, cerca de 90% de todos os terminais de cartões, e 80% de todos os cartões de pagamento, na UE eram conformes à norma EMV[63].

E, embora este facto tenha contribuído para reduzir os abusos associada aos cartões nas operações físicas de pagamento, esses abusos estão agora a deslocar-se cada vez mais para as operações por cartão à distância, nomeadamente para os pagamentos através da Internet.
Hoje em dia a realização de uma transacção física com um cartão de crédito implica, quase necessariamente, a introdução de um código PIN pelo utilizador e a comunicação instantânea entre o terminal automático onde é inserido o cartão (POS) e a entidade emitente do cartão.

Deste modo, ao inserir o cartão num terminal automático de pagamento (o qual fará a ponte entre o cartão e a entidade emissora), este verifica o tipo de transacção, o comerciante (registado e autorizado), o tipo da conexão (que deve obedecer a uma série de protocolos de segurança) e o valor da compra.

O terminal verifica também uma série de outras informações relativas ao cartão utilizado, tais como, o tipo de cartão, a data de validade, o nome do titular e outros detalhes para que a transacção possa ser inicializada. Uma vez conferidos esses dados, é necessário ainda que o titular introduza o código PIN para iniciar a transacção.

Uma vez iniciada a transacção, a entidade emitente do cartão vai conferir todos os dados que foram recolhidos pelo terminal automático e verificar que o cartão dispõe de saldo suficiente para o pagamento. Assim autorizando ou não aquele pagamento. Todo este processo leva poucos segundos e é totalmente automatizado por meios informáticos.

Portanto, segundo este procedimento mais recente de utilização de cartões, torna-se muito difícil, senão quase impossível, ocorrer um pagamento sem que o cartão disponha de saldo suficiente para o efeito. A não ser que se recorra a práticas cibercriminosas, tuteladas pelo *direito penal informático* (no qual se inclui o crime de burla informática)[64].

[63] Livro Verde para um mercado europeu integrado dos pagamentos por cartão, por Internet e por telemóvel, de 11.01.2012, COM (2011) 941 final, disponível na página de Internet em: http://www.europarl.europa.eu/meetdocs/2009_2014/documents/com/com_com(2011)0941_/com_com(2011)0941_pt.pdf.

[64] Sobre a autonomia do direito penal informático, veja-se com interesse, BENJAMIM SILVA RODRIGUES, Direito Penal, Parte Especial, Tomo I – Direito Penal Informático-Digital, Coimbra Editora, Coimbra, 2009, pp. 197 e ss., onde este Autor defende a existência desta autonomia face ao direito penal comum, seguindo essencialmente o modelo de autonomia de ciência criminal proposto por JOSÉ DE FARIA COSTA, "*Direito Penal Económico*", *in Colecção Textos Jurídicos n.º 4*, Quarteto Editora, Coimbra, 2003, mais concretamente, pela existência distintiva de metodologia, objecto e princípios próprios.

Já a utilização pela Internet dos cartões de crédito, para além de muitas vezes ser também rodeada de mecanismos de segurança (tais como a confirmação da operação através da inserção de um código enviado ao titular), indubitavelmente, a sua utilização abusiva, a ocorrer, resultará da utilização em sistemas informáticos de dados sem autorização, o que cai na previsão do referido crime de burla informática.

Com isto concluímos, em primeiro lugar, que a utilização abusiva dos cartões de garantia ou de crédito, hoje em dia, integra-se quase exclusivamente na conduta prevista no crime de burla informática, p. e p. pelo art.º 221.º, n.º 1, do Código Penal, pois essa utilização implica a inserção de dados em sistemas informáticos.

No entanto, como ainda é possível a utilização de cartões em certos terminais manuais ou automáticos de pagamento, em que a assinatura do titular do cartão valida a transacção em substituição da introdução de um código PIN, o crime de abuso de cartão de garantia ou de crédito, p. e p. pelo art.º 225.º do Código Penal, pode vir a ser praticado, mas somente em situações muito residuais.

Isto leva-nos então à segunda conclusão, que o crime de abuso de cartão de garantia ou de crédito, p. e p. pelo art.º 225.º do Código Penal, deveria ser revogado, por violar o carácter subsidiário da tutela penal em sintonia com o princípio da necessidade.

Com efeito, segundo o *principio da não-intervenção moderada* do Direito Penal, os «processos novos de criminalização (chamados processos de neocriminalização) só devem ser aceites como legítimos onde novos fenómenos sociais, anteriormente inexistentes, muito raros ou socialmente pouco significativos, revelem agora a emergência de novos bens jurídicos para cuja protecção se torna indispensável fazer intervir a tutela penal em detrimento de um paulatino desenvolvimento de estratégias não criminais de controle social»[65]. O que não sucede actualmente com o crime de abuso de cartão de garantia ou de crédito em análise, daí a sua necessária revogação em nossa opinião.

IV.Hiperligações e referências bibliográficas

Hiperligações

Banco de Portugal
Bases de dados jurídicas
Acesso ao Direito da União Europeia (Eur-Lex)

[65] Jorge de Figueiredo Dias, Temas Básicos da Doutrina Penal, Coimbra Editora, 2001, p. 62.

Referências bibliográficas

Albuquerque, Paulo Pinto de - Comentário do Código Penal à luz..., Universidade Católica Editora, 2008.

Azevedo, Ana Helena França - Burlas Informáticas: Modos de Manifestação, Tese de Mestrado, Escola de Direito da Universidade do Minho, 2016.

Barreiro, José António - Crimes Contra o Património, Universidade Lusíada Editora, 1996.

Carvalho, Américo Taipa de - Direito Penal - Parte Geral - Questões Fundamentais – Teoria Geral do Crime, Coimbra Editora, 2.ª ed, 2014.

Costa, Almeida - Comentário Conimbricense do Código Penal, Parte Especial, Tomo II, Jorge de Figueiredo Dias [Dir.], Coimbra Editora, 1999.

Cunha, Damião da - Comentário Conimbricense do Código Penal, Parte Especial, Tomo II, Jorge de Figueiredo Dias [Dir.], Coimbra Editora, 1999.

Dantas, A. Leones - A Revisão do Código Penal e os Crimes Patrimoniais, in "Jornadas de Direito Criminal, Revisão do Código Penal", Centro de Estudos Judiciários, 1998.

Fernandes, Maria José - Investigação Criminal e Gestão de Inquérito: práticas de optimização de meios (materiais e humanos) e de métodos de trabalho condicionantes do êxito da investigação, in "Gestão processual: agenda, conclusões, serviço urgente e serviço diário, provimentos e ordens", Centro de Estudos Judiciários, 2013.

Figueiredo Dias, Jorge de - Temas Básicos da Doutrina Penal, Coimbra Editora, 2001.

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

Garcia, M. Miguez - O Risco de Comer uma Sopa e Outros Casos de Direito Penal, Almedina, 2012.

Garcia, M. Miguez - O Direito penal – Passo a Passo, Vol. II, 2.ª Ed., Almedina, 2015.

Garcia, M. Miguez e Castela Rio, J.M. - Código Penal – Parte Geral e Especial, Almedina, 2015.

Machado, Pedro Sá - Os "crimes de detenção" e a "detenção-de-uma-coisa-móvel" no direito penal português: problemas conceptuais, dogmáticos e político-criminais, Tese de Mestrado, Faculdade de Direito da Universidade de Coimbra, 2015.

Ministério da Justiça, Código Penal, Actas e Projecto da Comissão de Revisão, Rei dos Livros, 1993.

Pecorella, Claudia – Il nuovo diritto penale delle "carte di pagamento", in Revista Italiana de Diritto e ProceduraPenale, 1, 1993.

Pereira, Victor de Sá e Lafayette, Alexandre - Código Penal Anotado e Comentado, Quid Juris, 2008.

Rodrigues, Benjamim Silva, Direito Penal, Parte Especial, Tomo I – Direito Penal Informático-Digital, Coimbra Editora, Coimbra, 2009.

Silva, Germano Marques da - Direito Penal Português, Parte Geral I, Editorial Verbo, 1997.

Silva, Germano Marques da - Curso de Processo Penal, Tomo III, 2.ª Ed., Editorial verbo, 2000.

CENTRO
DE ESTUDOS
JUDICIÁRIOS

6.
Crime de burla informática e nas comunicações. Enquadramento jurídico, prática e gestão processual

Paulo Luís Rodrigues Mota

CENTRO
DE ESTUDOS
JUDICIÁRIOS

6. CRIME DE BURLA INFORMÁTICA E NAS COMUNICAÇÕES – ENQUADRAMENTO JURÍDICO, PRÁTICA E GESTÃO PROCESSUAL

Paulo Luís Rodrigues Mota

I. Introdução

As tecnologias de informação e a informática vêm assumindo hodiernamente, na nossa sociedade, um papel cada vez mais preponderante e fundamental no desenvolvimento social, cultural e económico. A constante evolução das tecnologias de informação, nomeadamente do chamado ciberespaço, se por um lado comporta inegáveis vantagens para os utilizadores – hoje toda a informação está à distância de um "click"– o certo é que a liberdade de circulação e comunicação no ciberespaço acarreta também alguns perigos para os mais incautos e oportunidades para quem tenha tendências criminosas.

A informática foi vista desde sempre pelos delinquentes, principalmente aqueles com apetência para as tecnologias de informação, como um instrumento facilitador da prática de factos ilícitos, factos ilícitos estes que, nos primórdios da informática, não se enquadravam nos tipos penais existentes.

A nível nacional, curiosamente, a primeira versão da Constituição da República Portuguesa (Decreto de 10/04 de 1976) contemplava já a "utilização da informática", epígrafe do artigo 35.º que dispunha *"1. Todos os cidadãos têm o direito de tomar conhecimento do que constar de registos mecanográficos a seu respeito e do fim a que se destinam as informações, podendo*

exigir a rectificação dos dados e a sua actualização. 2. A informática não pode ser usada para tratamento de dados referentes a convicções políticas, fé religiosa ou vida privada, salvo quando se trate do processamento de dados não identificáveis para fins estatísticos. 3. É proibida a atribuição de um número nacional único aos cidadãos.", tal preceito constitucional viria a ser sucessivamente alterado pelas revisões constitucionais de 1982, 1989 e finalmente 1997 que lhe conferiu a actual redacção.

Quanto ao direito penal substantivo, o primeiro diploma legal que abordou os crimes informáticos foi a Lei n.º 109/91, de 17 de Agosto (Lei da Criminalidade Informática) que viria a criar os crimes de Falsidade informática, Dano relativo a dados ou programas informáticos, Sabotagem informática, Acesso ilegítimo, Intercepção ilegítima, Reprodução ilegítima de programa protegido.

Mais tarde, o legislador nacional através da reforma do Código Penal de 1995, operada pelo Decreto-Lei n.º 48/95, de 15 de Março, introduziu no referido código a previsão e punição do crime de burla informática no artigo 221.º, n.º 1 e, posteriormente, pela mão da reforma do Código Penal de 1998 (aprovada pela Lei 65/98, de 2 de Setembro), surge a incriminação da burla nas comunicações, acrescentando o n.º 2 ao artigo 221.º, do Código Penal.

Desde tal data, o crime de burla informática e nas comunicações manteve-se inalterado e, apesar da aparente abrangência do tipo legal em questão, a sua aplicação prática nos últimos 20 anos, consideramos que tem sido bastante reduzido o número de despachos acusatórios e de decisões condenatórias a ele reportadas. Pensamos que tal facto ocorre por duas ordens de razões, em primeiro lugar por via da sobreposição dos seus elementos típicos com outros tipos legais, em segundo lugar por dificuldades de enquadramento dos factos, nos elementos objectivos do aludido tipo legal. Assim, com excepção das situações de facto relacionadas com levantamento de dinheiro em utilização indevida de cartões de débito, a jurisprudência sobre o crime de burla informática e nas comunicações é muito escassa, incidindo normalmente sobre os elementos objectivos do tipo de crime, e na sua relação com os tipos que lhe são próximos, nomeadamente os que constam da Lei n.º 109/2009, de 15 de Setembro, actual Lei do Cibercrime[1].

II. Objectivos

Tentaremos, em suma, que este guia se possa constituir como um instrumento que contribua para discussão dos problemas que se levantam com os tipos legais que constituem o crime de Burla informática e nas comunicações, quer em termos substantivos, quer em termos processuais, e que permita a todos os operadores judiciários, nomeadamente aos Magistrados do Ministério Publico, que dirigem a investigação de tais crimes, antecipar algumas das questões que poderão surgir durante o inquérito.

[1] Neste sentido ver notas práticas – jurisprudência sobre o cibercrime, anos 2015 a 2017, disponível em http://cibercrime.ministeriopublico.pt/notas-praticas.

III. Resumo

O presente Guia divide-se em duas partes fundamentais: a primeira respeitante ao enquadramento jurídico dos crimes de burla informática e burla nas comunicações, onde procuraremos efectuar uma abordagem teórico-prática do tipo incriminatório, tendo em conta a doutrina e jurisprudência mais relevante. Numa segunda parte iremos focar-nos numa vertente mais prática que permita fornecer ao leitor pistas para uma gestão processual eficiente e eficaz dos inquéritos em que esteja em causa factualidade que, em abstracto, se possa subsumir aos tipos legais em apreço.

Na primeira parte (Enquadramento Jurídico) abordam-se as questões centrais da imputação dos crimes de burla informática e burla nas comunicações, começando com a análise do bem jurídico protegido com a incriminação, desconstruindo depois os elementos objectivos e subjectivos contidos no artigo 221.º, do Código Penal.

Começando por analisar o crime de burla informática a que alude o n.º 1 do referido preceito legal, tentando dissecar, numa perspectiva prática, as várias condutas susceptíveis de preencher o tipo legal.

De seguida, analisaremos o crime de burla nas comunicações, cuja incriminação é descrita no n.º 2, procurando enquadrar condutas neste tipo legal, adiantando desde já que no nosso entendimento este preceito tem uma aplicação bastante residual.

Na segunda parte (Prática e Gestão Processual), iremos abordar a direcção e gestão do inquérito, numa perspectiva prática, procurando antecipar problemas em termos de prova, fazendo aqui também uma abordagem à aplicação das normas processuais contidas na Lei do cibercrime e a sua importância para a recolha de prova em relação aos crimes de burla informática e nas comunicações.

1. Crime de Burla Informática e nas comunicações – evolução legislativa

A nível europeu o primeiro esforço sério para combate ao chamado cibercrime surge em 1985, pela mão do Conselho da Europa, com a nomeação de um comité que teria como função o estudo dos problemas e compilação de um relatório sobre os crimes informáticos.

No entanto, a Alemanha foi pioneira na previsão e punição do crime de Burla Informática ao introduzir no seu Código Penal em 1986, o § 263-A[2], tal incriminação viria a ser reproduzida

[2] § 263.º-A CP alemão (*Computerbetrug*) "1. Quem, com intenção de obter para si ou para terceiro vantagem patrimonial ilegítima, prejudicar o património de outrem, influindo sobre o resultado de um processo de tratamento de dados, por meio de configuração errónea de programa, uso de dados incorrectos ou incompletos, uso não autorizado de dados ou através de intervenção não autorizada no processamento, será punido com pena de prisão até 5 anos ou multa".

em 1987 pelo Código Penal austríaco e, mais tarde em 1994, pelo Código Penal suíço[3], numa formulação muito semelhante àquela que viria a ser adoptada pelo Código Penal Português.

Entretanto o trabalho iniciado em 1985 pela comissão criada pelo Conselho da Europa viria a produzir os seus frutos, em 13 de Setembro de 1989 com a aprovação pelo Comité de Ministros do Conselho da Europa da recomendação R(89)9, que visava a harmonização das legislações nacionais relativamente aos crimes relacionados com computadores, dessa recomendação fazia parte, em anexo, uma lista mínima e uma lista facultativa de tipos de crimes que deveriam ser transpostos para as legislações nacionais dos países membros.

Na sequência desta recomendação, é aprovada em Portugal a Lei da Criminalidade Informática – Lei n.º 109/91, de 17 de Agosto, que estabeleceu como tipos legais os crimes de Falsidade informática; Dano relativo a dados ou programas informáticos; Sabotagem informática; Acesso ilegítimo; Intercepção ilegítima e Reprodução ilegítima de programa protegido, que precedeu a actual Lei do cibercrime.

Curiosamente, fora dos tipos previstos neste diploma legal ficou, o primeiro crime que surgia na referida lista mínima da recomendação R(89)9, que era precisamente o crime de burla informática ("*computer fraud*")[4], cuja descrição tinha uma formulação muito semelhante àquela que já tinha sido adoptada pela Alemanha no preceito legal supra referido.

A incriminação da Burla informática só viria a ser adoptada pelo legislador nacional, através da reforma do Código Penal de 1995, operada pelo Decreto-Lei n.º 48/95 de 15 de Março, ao introduzir no referido código, por sugestão do Conselheiro Sousa e Brito, a previsão e punição do referido crime no artigo 221.º, n.º 1, com a redacção ainda hoje em vigor.

Conforme consta das actas da comissão revisora do Código Penal, a opção por incluir tal crime no Código Penal, derivou do facto de se entender que se estava perante uma espécie de burla, para a qual não existia incriminação, ao contrário do que sucedia na Alemanha e na Áustria, que, como vimos, já tinham incriminado o ilícito em causa[5].

Para a construção deste novo tipo legal partiu-se da estrutura do crime de burla tradicional, cingindo a sua execução à manipulação de dados informatizados de forma a lesar o património de outrem.

Manuel António Lopes Rocha[6] avança como exemplo de algumas das razões que estiveram subjacentes à criação deste tipo legal:

---

[3] Cfr. Albuquerque, Paulo Pinto de, Comentário ao Código Penal à Luz da Constituição da República e da Convenção Europeia dos Direitos do Homem, Universidade Católica, 3.ª edição, 2015, pág. 859.
[4] "1 COMPUTER FRAUD - The input, alteration, erasure or suppression of computer data or computer programs or other interference with the course of data processing that influences the result of data processing thereby causing economic or possessory loss of property of another person with the intent of procuring an unlawful gain for himself or another person" (cfr. Stein Schjølberg, "The History of Cybercrime: 1976-2014", Kindle Edition, 2014, p. 39).
[5] cfr. Código Penal – Actas e Projecto da Comissão de Revisão, 1993, pág. 455.
[6] Rocha, Lopes, A revisão do Código Penal, Soluções de neocriminalização, Jornadas do Direito Criminal do CEJ, 1993, pág. 93.

– A frequência com que se verificavam utilizações abusivas de caixas automáticas;

– A existência de condutas que, em geral, envolvem riscos consideráveis para o comércio jurídico e para o tráfico ou sistema de provas;

– A difícil detecção dessas condutas, que mereciam uma repulsa social cada vez mais forte; e

– A insuficiência dos tipos penais tradicionais (de enriquecimento patrimonial) para a protecção do bem jurídico.

Para a construção deste novo tipo legal partiu-se da estrutura do crime de burla tradicional, cingindo a sua execução à manipulação de dados informatizados.

O artigo 221.º, do Código Penal, viria a sofrer apenas mais uma alteração, operada com a reforma do Código Penal de 1998, aprovada pela Lei 65/98, de 2 de Setembro, acrescentando ao referido artigo o seu n.º 2, que veio incriminar a burla nos serviços de telecomunicações.

1.1. Bem Jurídico Protegido

É pacífico que um só tipo legal proteja «especialmente», mais do que um bem jurídico, questão a ponderar e a esclarecer, perante cada tipo e cada acção dele violadora.

Ora, na nossa opinião é precisamente o que sucede com o crime de Burla informática e nas comunicações.

O crime de burla informática e nas comunicações[7] tutela em primeira linha o património, a inserção sistemática revela-se, neste aspecto, determinante para a definição e delimitação do bem jurídico protegido. Tal património deverá ser entendido numa acepção jurídico-económica: conjunto de utilidades económicas detidas pelo sujeito e cujo exercício ou fruição a ordem jurídica não desaprova. Incluem-se no património os direitos subjectivos patrimoniais

[7] Artigo 221.º.
Burla informática e nas comunicações
1 - Quem, com intenção de obter para si ou para terceiro enriquecimento ilegítimo, causar a outra pessoa prejuízo patrimonial, interferindo no resultado de tratamento de dados ou mediante estruturação incorrecta de programa informático, utilização incorrecta ou incompleta de dados, utilização de dados sem autorização ou intervenção por qualquer outro modo não autorizada no processamento, é punido com pena de prisão até 3 anos ou com pena de multa.
2 - A mesma pena é aplicável a quem, com intenção de obter para si ou para terceiro um benefício ilegítimo, causar a outrem prejuízo patrimonial, usando programas, dispositivos electrónicos ou outros meios que, separadamente ou em conjunto, se destinem a diminuir, alterar ou impedir, total ou parcialmente, o normal funcionamento ou exploração de serviços de telecomunicações.
3 - A tentativa é punível.
4 - O procedimento criminal depende de queixa.
5 - Se o prejuízo for:
a) De valor elevado, o agente é punido com pena de prisão até 5 anos ou com pena de multa até 600 dias;
b) De valor consideravelmente elevado, o agente é punido com pena de prisão de 2 a 8 anos.
6 - É correspondentemente aplicável o disposto no artigo 206.º.

(de índole real ou obrigacional), os lucros cessantes e demais expectativas legítimas de obtenção de vantagens económicas[8].

Perfilha-se o entendimento dominante na jurisprudência dos nossos Tribunais superiores de que no crime de burla informática e nas comunicações estamos perante um delito contra o património e só secundariamente com ele se visa proteger o correcto funcionamento e a inviolabilidade dos sistemas informáticos[9].

Este entendimento é pacífico no Supremo Tribunal de Justiça, existindo vários acórdãos sobre o tema, entendimento seguido também pelos Tribunais da Relação. Normalmente na jurisprudência a questão do bem jurídico protegido está associada ao concurso de infracções.

1.2. Classificação quanto ao tipo de crime

Estamos perante um crime comum, uma vez que pode ser praticado por qualquer pessoa com acesso a um sistema informático.

É um crime de dano, pelo que só se consuma com a ocorrência de um prejuízo efectivo no património do sujeito passivo ou de terceiro, que irá ocorrer sempre que se verifique uma diminuição do valor económico do património da vítima, em relação à posição em que estaria caso o agente não tivesse realizado a sua conduta. A consumação do crime depende da provocação de um prejuízo patrimonial (diminuição do activo ou aumento do passivo).

Trata-se de um Crime resultado parcial ou cortado, porque a sua consumação depende de um evento espácio-temporalmente destacado da acção que consiste na saída dos bens ou valores da esfera de disponibilidade fáctica da vítima, independentemente da efectiva verificação do benefício económico do agente da infracção ou de terceiro. A registar-se essa circunstância, (enriquecimento do agente) andará bem o tribunal, a nosso ver, se a considerar como agravante em sede de determinação da medida concreta da pena (artigo 71.º, n.º 2, do Código Penal).

Finalmente é um Crime de execução vinculada, a produção do resultado terá de ser determinada por procedimentos e acções que sejam especificamente descritos na norma incriminatória, no caso em apreço, há-de consistir sempre em um comportamento que constitua um artifício, engano ou erro consciente, não directamente em relação a uma pessoa (como no crime burla previsto no artigo 217.º, do Código Penal), mas por intermediação da manipulação de um sistema de dados ou de tratamento informático, ou de equivalente

[8] Cfr. Costa, Almeida no Comentário Conimbricense ao Código Penal, Tomo II, Coimbra Editora, 1999, págs. 279 a 283, anotação ao artigo 217.º, §6 e 7 "conceito jurídico-penal de património".
[9] (v.g. Acórdão do STJ, de 05-12-2007, proc. 07P3864; Acórdão do STJ, de 05-11-2008, proc. 08P2817, Acórdão do TRP, de 20-03-2013, proc. 493/11.0PIPRT.P1; Acórdão do TRC, de 29-02-2012, proc. 183/10.1GATBU.C1; todos disponíveis em www.dgsi.pt). No mesmo sentido, José de Faria Costa e Helena Moniz, Algumas Reflexões sobre a criminalidade informática em Portugal, *in* BFDUC, Vol. LXXIII, 1997, pág. 323.

utilização abusiva de dados[10]. Tal execução vinculada não é, no entanto, fechada ou taxativa: "intervenção por qualquer outro modo não autorizado no processamento de dados". O que constitui uma cláusula geral que confere à enumeração das condutas típicas um carácter apenas exemplificativo, no que à interferência no processamento de dados diz respeito.

1.3. Elementos objectivos do crime de Burla Informática

Quanto aos elementos objetivos em termos do seu resultado, assentará, conforme supra exposto, num dano patrimonial causado a outra pessoa, em que a conduta do agente terá que consubstanciar um erro directo com finalidade se causar prejuízo a terceiro, um engano ou manipulação sobre dados ou aplicações informáticas, interferir no resultado ou estruturação incorrecta de programa informático, utilização de dados de forma incompleta ou incorrecta, utilizar de dados sem autorização ou intervir de forma não autorizada de processamento de qualquer sistema informático[11].

Esmiuçando cada uma das condutas possíveis, teremos:

1) Interferindo no resultado de tratamento de dados, servindo-se o agente directamente do computador ou fornecendo instruções a terceiro, de forma a manipular ou alterar o resultado da introdução dos dados, num determinado programa.

2) Mediante estruturação incorrecta de programa informático[12], ou seja, elaborar ou manipular determinado programa informático de forma a causar ao seu utilizador prejuízo patrimonial, normalmente estas condutas consumam-se pela alteração de programas existentes (acrescentando-lhes rotinas), que provocam, de forma automatizada, deslocações patrimoniais não desejadas pelos utilizadores de tais programas.

3) Utilização incorrecta ou incompleta de dados – ocorre essencialmente quanto a introdução de dados no computador não corresponde à realidade, fazendo com que se efective uma deslocação patrimonial não desejada pelo ofendido (v.g. pagamentos ou transferências bancárias, processamento de subsídios)[13]

4) Utilização de dados sem autorização, talvez a forma mais comum do crime de burla informática e que se traduz na introdução não autorizada do PIN, para utilização de

[10] Cfr. Costa, Almeida, Comentário Conimbricense ao Código Penal, Tomo II, Coimbra Editora, 1999, pág. 329, anotação ao artigo 221.º, §4.
[11] Cfr. Santos, Manuel Simas e Leal-Henriques, Manuel, Código Penal Anotado, Volume III - Artigos 131.º ao 235.º, 4.ª Edição, Rei dos Livros, 2016, pág. 1010.
[12] A anterior Lei da Criminalidade Informática (Lei 109/91, de 17-08), definia, no artigo 2.º, alínea c), Programa informático como *"um conjunto de instruções capazes, quando inseridas num suporte explorável em máquina, de permitir à máquina que tem por funções o tratamento de informações indicar, executar ou produzir determinada função, tarefa ou resultado".*
[13] Neste sentido, Garcia, M, Miguez, Código Penal parte geral e especial com notas e comentários, Almedina, 2.ª edição, 2015, pág. 984.

cartão bancário do ofendido, quer seja para efectuar levantamentos em ATM's, quer para efectuar pagamentos em terminais automáticos.

5) Intervenção por qualquer outro modo não autorizada no processamento de dados – trata-se de uma cláusula aberta que permite abranger eventuais lacunas que não sejam subsumíveis às condutas anteriores ou que a sua subsunção seja duvidosa[14].

Resumindo, segundo o Prof. Almeida Costa[15], no caso de uso de meios informáticos para lesar o património, pode verificar-se uma de duas hipóteses:

1) O agente induz em erro outra pessoa, levando-a através de uma operação informática, a causar prejuízos patrimoniais (próprios ou alheios). Neste caso, verifica-se o duplo nexo de imputação objectiva, característico da burla tradicional. Logo, aplica-se o artigo 217.º e não o artigo 221.º, n.º 1.

2) O agente produz o dano patrimonial mediante interferência directa num sistema informático, sem que exista de permeio a intervenção de uma pessoa em erro. Então, falta o duplo nexo de imputação objectiva e deve aplicar-se o artigo 221.º.

1.4. Elementos Subjectivos do crime de Burla Informática

O elemento subjetivo do crime de burla informática consubstancia-se na "intenção de obter para si ou para terceiro um benefício ilegítimo" o que implica que o agente da infração tenha plena consciência de que a sua conduta, isto é o crime exige o dolo genérico e o dolo específico de enriquecimento ilícito próprio ou de terceiro[16].

Em consequência é denominado de delito de resultado parcial, isto é, requer o *animus* de enriquecimento do agente, que se consuma com o prejuízo patrimonial da vítima[17].

1.5. Burla nas comunicações

Relativamente ao crime de burla nas comunicações, previsto no n.º 2 do artigo 221.º, do Código Penal, tem como especificidade que a ofensa no património do lesado é efectuada através de uma interferência nos serviços de comunicações, assim, o crime consuma-se com a realização dos mesmos elementos subjectivos (dolo e intenção de obter enriquecimento ilícito

[14] Cfr. Rocha, Lopes, A revisão do Código Penal, Soluções de neocriminalização, Jornadas do Direito Criminal do CEJ, 1993, pág. 95.
[15] Costa, Almeida, no Comentário Conimbricense ao Código Penal, Tomo II, Coimbra Editora, 1999, pág. 330, anotação ao artigo 221.º, §5.
[16] Barreiros, José António, Crimes contra o Património no Código Penal de 1995, Universidade Lusíada, 1996, Pág. 187.
[17] Costa, Almeida, Comentário Conimbricense ao Código Penal, Tomo II, Coimbra Editora, 1999, pág. 331, anotação ao artigo 221.º, §7.

próprio ou de terceiro), traduzindo-se a acção típica numa conduta do agente que afecte o normal funcionamento ou exploração do serviço de comunicações[18].

Para a verificação da conduta prevista no n.º 2 do artigo 221.º, do Código Penal, exige-se ainda que tal afectação tenha a virtualidade de causar prejuízo patrimonial a terceiro e diminua, altere ou impeça o normal funcionamento das comunicações.

A modificação operada pelo agente poderá ocorrer por qualquer forma, podendo ser o ofendido aquele sobre o qual recai o prejuízo patrimonial efectivo.

1.6. A tentativa

O crime de burla informática e nas comunicações consuma-se com o efectivo prejuízo patrimonial do ofendido, sendo o crime em causa punido na sua forma tentada, nos termos do artigo 221.º, n.º 3, do Código Penal.

Nos termos do artigo 22.º, n.º 1, do Código Penal, *"há tentativa quando o agente praticar actos de execução de um crime que decidiu cometer, sem que este chegue a consumar-se."*, acrescentando o n.º 2, alínea b), que são actos de execução *"os que forem idóneos a produzir o resultado típico",* ou seja, os que caso as coisas corressem conforme o agente as perspectivou, os actos por ele praticados seriam adequados a produzir o resultado típico. O que acaba por criar um perigo concreto para o bem jurídico protegido, no caso da Burla informática, o património.

Nos termos do artigo 23.º, n. º 3, *"a tentativa não é punível quando for manifesta a inaptidão do meio empregado pelo agente"*, assim, a tentativa não é punível quando aos olhos do homem médio o meio utilizado pelo agente for totalmente inadequado à produção do resultado, visto que nesses casos, nem em termos abstractos o bem jurídico protegido pela incriminação é posto em causa.

Pelo Exposto, *"a punibilidade da tentativa depende da evidência ou não da impossibilidade do meio para produzir o resultado, sendo que a tal determinação preside um critério objectivo – saber se do ponto de vista de um homem médio, colocado na posição dos intervenientes na acção em apreço (agente e vítima), a inadequação do meio era visível, ou seja, se segundo as regras da experiência, observando a conduta do agente e considerando as demais circunstâncias concretas, inclusive tendo em conta os especiais conhecimentos do agente, se poderia concluir, de forma evidente, pela impossibilidade do meio para produzir o resultado – juízo de prognose póstuma ex ante"*[19].

[18] Costa, Almeida, Comentário Conimbricense ao Código Penal, Tomo II, Coimbra Editora, 1999, págs. 332 e 333, anotação ao artigo 221.º, §14.
[19] Acórdão TRE, de 26-06-2012, proc. 264/06.6GBPSR.E1; disponível em www.dgsi.pt.

1.7. Forma agravada do tipo legal

O n.º 5 do artigo 221.º, do Código Penal, prevê o crime de burla informática e nas comunicações na sua forma agravada, em função do valor elevado ou consideravelmente elevado, por referência às definições constantes das alíneas a) e b) do artigo 202.º, do mesmo código.

Caso o Prejuízo seja superior a 50 UC's (actualmente €5.100,00) o agente é punido com pena de prisão até cinco anos ou de multa até 600 dias.

Se o Prejuízo for superior a 200 UC's (actualmente €20.400,00) o agente é punido com pena de prisão até de dois a oito anos.

1.8. Caso de Restituição ou reparação

Por força do n.º 6 do artigo 221.º, do Código Penal, no caso do crime de burla informática e nas comunicações, poderá extinguir-se a responsabilidade criminal do agente ou existir uma atenuação especial da pena nos termos do artigo 206.º, n.ºs 1 e 2, do mesmo Código.

1.9. Concurso de Crimes

1.9.1. Relativamente ao crime de Burla Simples

A distinção entre a Burla informática e burla clássica assenta na circunstância de os computadores ou sistemas informáticos não serem susceptíveis de serem ludibriados, mas sim manipulados informaticamente, através da incorrecta introdução de dados ou estruturação incorrecta de *software* de forma a proporcionar o enriquecimento ilegítimo do agente ou de terceiro e prejudicar patrimonialmente a vítima, afastando-se assim do tipo clássico de burla.

Os dois tipos legais distinguem-se ainda pela ausência do momento intersubjectivo que a caracteriza, a burla informática ocorre quando o prejuízo patrimonial decorre directamente da operação informática, totalmente automatizada em que a intervenção humana não corresponde a um controlo efectivo e crítico do resultado do tratamento informático de dados. Somente nestes casos poderá aplicar-se o regime normativo do artigo 221.º, do Código Penal.

Em conclusão, entendemos que entre os artigos 217.º e 221.º, ambos do Código Penal, há uma relação de alternatividade ou de exclusividade típica, pois as situações enquadráveis no artigo 221.º nunca realizam o tipo de burla do artigo 217º, em face dos diferentes modos de execução de cada um dos tipos legais[20].

[20] Neste sentido, Albuquerque, Paulo Pinto de, Comentário ao Código Penal à Luz da Constituição da República e da Convenção Europeia dos Direitos do Homem, Universidade Católica, 3.ª edição, 2015, pág. 861.

1.9.2. Relativamente ao crime de furto simples

Reporta-se aos casos em que o agente se apropria de cartão bancário contra a vontade do respectivo titular, fazendo-o coisa sua, sem consentimento e à revelia do ofendido e, tendo conhecimento ou acesso ao respectivo código PIN, efectua levantamentos em numerário, ou procede a pagamentos com tal cartão, não estando para tal autorizado, resultando de tais transações um prejuízo ao ofendido.

Se a sua conduta preencheu os elementos típicos do crime de furto e do crime de burla informática, constituindo duas resoluções criminosas distintas, entendemos haver nestes casos uma relação de concurso efectivo entre o crime de furto e o crime de burla informática[21].

1.9.3. O crime de falsidade Informática

O Supremo Tribunal de Justiça há muito fixou a jurisprudência[22] no sentido de que, no caso de a conduta do agente preencher as previsões de falsificação e de burla do artigo 256.º, nº 1, alínea a), e do artigo 217.º, nº 1, ambos do Código Penal, se verifica um concurso real ou efectivo de crimes.

Mas entendemos, porque estamos perante tipos legais manifestamente destintos, que tais argumentos não poderão ser aplicáveis à relação entre o crime de falsidade informática, previsto no artigo 3.º da Lei do Cibercrime e o crime de burla informática, pois apesar de não serem totalmente coincidentes os bens jurídicos tutelados, sendo a falsidade operada no sistema informático o instrumento para a consumação do crime de burla informática, realizada com a intenção de obter um enriquecimento ilegítimo, para o agente ou para terceiro, é, deste modo, consumida pelo crime de burla informática, subsistindo entre estes dois tipos legais de crime uma relação de concurso aparente, mais propriamente de consumpção pura[23].

Ao invés, nos casos do chamado "*Phishing*"[24], que ocorre aquando da criação de uma página web falsa, em tudo idêntica à página oficial da instituição bancária e o ofendido ao aceder a tal página, julgando que se trata da página legítima do banco, faculta os seus dados, preenche em nosso entender os dois tipos legais em análise, porque o objectivo da falsidade destina-se a um indeterminado número de utilizadores, colocando em causa em primeira linha a credibilidade e idoneidade dos sistemas informáticos, lesando depois todos aqueles que acedendo a tal página inserem os seus dados pessoais permitindo ao agente, num segundo momento, praticar o crime de burla informática, ao dispor do património dos lesados, assim,

[21] Acórdão TRC de 29-02-2012, proc. 183/10.1GATBU.C1; disponível em www.dgsi.pt.
[22] Acórdão do Supremo Tribunal de Justiça de Fixação de jurisprudência 10/2013, de 05-06-2013, proc. 29/04.0JDLSB-Q.S1.
[23] Neste sentido, Albuquerque, Paulo Pinto de, Comentário ao Código Penal à Luz da Constituição da República e da Convenção Europeia dos Direitos do Homem, Universidade Católica, 3ª edição, 2015, pág. 861.
[24] Verdelho, Pedro – *Phishing* e outras formas de defraudação nas redes de comunicação, Direito da sociedade de informação, volume VIII, Coimbra Editora, 2009, págs.414 e 415.

consideramos que estamos perante bens jurídicos distintos e diferentes resoluções criminosas, pelo que deverá considerar-se que os crimes foram praticados em concurso efectivo[25].

Tal como acontece quando se trate da colocação em circulação como legítimo de um cartão de débito falsificado nos termos do artigo 3º, n.º 2, da Lei do Cibercrime, o concurso de crimes dá-se entre este ilícito e o crime de burla informática, caso o cartão bancário falseado seja criado com intenção de causar prejuízo a outrem e obter benefício ilegítimo.

1.9.4. O crime de acesso ilegítimo

A acção típica caracterizadora deste tipo legal assenta naqueles casos em que o agente acede ao sistema informático da vítima à sua revelia e sem o seu conhecimento, através da introdução de um vírus informático, com a finalidade de capturar todos os elementos bancários existentes, nomeadamente dados de cartões de crédito ou de acesso a *homebanking*, e ainda todo o tipo de informação que agente pretenda (v.g. dados pessoais).

Consideramos que entre estes crimes existe uma relação de concurso aparente, consumpção pura, uma vez que a concretização do crime de burla informática implica em algumas das suas condutas típicas, supra referidas, aceder ilegitimamente a determinado sistema, pelo que teríamos que considerar o crime de acesso ilegítimo como crime meio, sendo absorvido pelo consagrado no artigo 221.º, n.º 1, do Código Penal[26].

2. Prática e Gestão Processual

2.1. A aquisição da notícia do crime e definição do objecto do processo

2.1.1. Generalidades

A aquisição da notícia do crime de Burla informática, à semelhança dos outros crimes, nos termos do artigo 241.º do Código de Processo Penal, pode acontecer de três formas, por conhecimento próprio, por intermédio dos órgãos de polícia criminal ou mediante denúncia.

O crime de burla informática na sua forma simples tem natureza semi-pública, por o respectivo procedimento criminal depender de queixa (cfr. artigo 221.º, nº 4, do Código Penal).

Tendo legitimidade para apresentar queixa o ofendido, considerando a lei como tal "o titular dos interesses que a lei especialmente quis proteger com a incriminação" (cfr. artigo 113.º, n.º 1, do Código Penal).

[25] Teixeira, Paulo Alexandre Gonçalves, O Fenómeno do Phishing – Enquadramento Jurídico-Penal, Dissertação de Mestrado, Universidade Autónoma de Lisboa, 2013, pág. 23.
[26] Neste sentido acórdão do Supremo Tribunal de Justiça, datado de 20-09-2006, processo 06P1942, disponível em www.dgsi.pt.

A noção de queixa tem conteúdo e natureza processual específicos; não constitui, como a denúncia, a simples transmissão do facto com relevância criminal, isto é, não constitui processualmente queixa uma simples declaração de ciência feita acerca de um facto. A queixa exige que o ofendido efectue uma declaração de vontade específica de perseguição criminal pelo facto, e distingue-se nos seus elementos da denúncia, pois na queixa além da declaração de ciência na transmissão da ocorrência de um facto, *"exige-se ainda uma manifestação de vontade de que seja instaurado um processo para averiguação da notícia e procedimento contra o agente responsável."*[27]

Todavia, não é toda e qualquer pessoa eventualmente afectada pela prática de um crime que pode formular essa manifestação de vontade, ou seja, que pode validamente apresentar queixa contra o autor dos factos, mas somente o ofendido, sendo este, o titular dos interesses que a lei especialmente quis proteger com a incriminação, no que constitui a identificação do critério para definição da legitimidade para o exercício do direito de queixa.

O artigo 113.º, n.º 1, do Código Penal, exige, pois, como condição de legitimidade, e existência de um interesse que a lei quis especialmente proteger com a incriminação, isto é de um interesse específico, particularmente qualificado, que intercede na relação entre o bem jurídico e o sujeito afectado, no caso do crime de burla informática e nas comunicações, será o indivíduo que sofreu o efectivo prejuízo patrimonial com a actuação do agente.

Recebida a notícia do crime, o Ministério Público, e mediante os factos relatados, cumpridos os requisitos de procedibilidade, determina a abertura de inquérito, nos termos do artigo 262.º, n.º 2, do Código de Processo Penal, delimitando, dentro do possível, o objecto do processo perante os factos que lhe são transmitidos, subsumindo os mesmos ao tipo legal que melhor os enquadra.

Tendo em vista "investigar a existência de um crime, determinar os seus agentes e a responsabilidade deles e descobrir e recolher as provas, em ordem à decisão sobre a acusação" – artigo 262.º, n.º 1, do Código de Processo Penal. Razão pela qual todos os actos efectuados durante a fase investigatória deverão terem vista a prolação da melhor decisão de encerramento de inquérito, no menor prazo possível, pelo que qualquer diligência ordenada deverá ter em vista a utilidade para a prova de determinado facto, que se enquadre no âmbito do objecto do processo.

Sendo o Ministério Público o titular da acção penal cabe-lhe a direcção do inquérito, sendo coadjuvado pelos órgãos de polícia criminal, que actuam sobe a sua directa orientação, encontrando-se na sua dependência funcional (artigos 263.º, 53.º, n.º 2, alínea, b), 55.º e 56.º, todos do Código de Processo Penal). Cumpre, em primeira linha ao Ministério Público definir, desde logo, a linha investigatória a seguir no caso em concreto.

A Constituição da República Portuguesa dispõe no seu artigo 202.º, n.º 3, que *"no exercício das suas funções os tribunais têm direito à coadjuvação das outras autoridades"*.

[27] Cfr. SILVA, GERMANO MARQUES DA, Direito Processual Penal Português do Procedimento (marcha do processo), Universidade Católica Editora, 2015, pág. 57.

Por outro lado, o artigo 9.º, n.º 2, do Código de Processo Penal estabelece: *"No exercício da sua função, os tribunais e demais autoridades judiciárias têm direito a ser coadjuvados por todas as outras autoridades; a colaboração solicitada prefere a qualquer outro serviço"*, preceituando o artigo 55.º, n.º 1, do mesmo código, que *"compete aos órgãos de polícia criminal coadjuvar as autoridades judiciárias com vista à realização das finalidades do processo".*

Assim, atentos os poderes de direcção do inquérito atribuídos ao Ministério Público, determinam a imediata comunicação da notícia do crime por parte dos OPC's (cfr. artigos 243.º, n.º 3, 245.º e 248.º, todos do Código de Processo Penal), recebida tal comunicação caberá ao Ministério Público determinar a abertura do respectivo inquérito caso se mostrem verificados os pressupostos de procedibilidade.

A investigação do crime de burla informática e nas comunicações mostra-se genericamente delegado na Policia Judiciária, atento o disposto no artigo 270.º, n.ºs 1 e 4, do Código de Processo Penal, do Ponto II, n.º 1, da Circular da Procuradoria-Geral da República n.º 6/2002, de 11 de Março e o disposto nos artigos 7.º, n.º 3, alínea l), da Lei n.º 49/2008, de 27 de Agosto, podendo ser delegado noutro OPC nos termos do disposto no artigo 8.º da referida Lei.

2.1.2. As diligências de inquérito

Inicio do inquérito

Recebida a notícia do crime e registado o respectivo inquérito, deverá o Magistrado do Ministério Público proferir o primeiro despacho no processo, no qual deverá avaliar os factos noticiados, avaliando o enquadramento jurídico dos mesmos. Para além disso, deverá efectuar a apreciação de questões de competência, legitimidade, procedibilidade, ponderar as vantagens na delegação da investigação em OPC ou execução directa da investigação pelos Serviços do Ministério Público.

Em caso de opção por delegação da competência de investigação no OPC, o Magistrado do Ministério Público deverá efectuar uma definição mínima das diligências a executar. Neste ponto, chama-se a atenção para a urgência na recolha de determinados elementos de prova, cuja relevância poderá ser essencial para prova dos elementos objectivos e subjectivos do crime de burla informática e nas comunicações.

Os inquéritos relativos à criminalidade informática encerram dificuldades acrescidas em termos de prova, requerendo muitas vezes a sua investigação conhecimentos especializados, a necessidade de realização de perícias a sistemas informáticos, recolha de prova digital e recolha de imagens de videovigilância, assumindo particular importância uma adequada prática e gestão processual,

Entre os inúmeros problemas inerentes à investigação, as características deste tipo de crime, assim como o elevado grau técnico que muitas das vezes exigem, o elevado número de processos e carência de meios humanos especializados, leva a um prolongamento excessivo nos inquéritos relativos à criminalidade informática

A identificação do agente que cometeu o ilícito é talvez a maior dificuldade na investigação relativa ao crime de Burla Informática e nas comunicações, hoje em dia, o típico criminoso informático apresenta, cada vez mais capacidade de se manter incógnito na web, tornando muitas vezes impossível a acção da justiça na sua identificação, normalmente são indivíduos socialmente integrados, de elevada capacidade intelectual, com formação académica na área informática e que não se expõem, actuando quase sempre na sombra, utilizando máscaras de IP's ou movendo-se na DARK WEB, o que muitas vezes torna praticamente impossível a sua identificação.

Aplicação da Lei do Cibercrime ao crime de burla informática

Só a partir de 15 de Setembro de 2009 – data da entrada em vigor da Lei do Cibercrime – surgiu no direito processual penal português um regime que regulou de forma específica e detalhada o modo de obtenção da prova digital.

Nos termos do artigo 11.º da Lei n.º 109/2009, de 15 de Setembro, o regime processual previsto em tal lei, não é aplicável somente a processos relativos a crimes previstos na respectiva lei, como também a processos relativos a crimes cometidos através de um sistema informático ou em qualquer processo criminal em que seja necessário proceder a recolha da chamada prova digital[28].

A Lei do Cibercrime prevê um conjunto de mecanismos processuais relativos à obtenção da prova digital, de carácter geral, aplicável ao crime de que se ocupa o presente estudo, em concreto:

a) Preservação expedita de dados (artigo 12.º);

b) Revelação expedita de dados (artigo 13.º);

c) Injunção para apresentação ou acesso a dados (artigo 14.º);

d) Pesquisa informática (artigo 15.º);

[28] Artigo 11.º
Âmbito de aplicação das disposições processuais
1 - Com excepção do disposto nos artigos 18.º e 19.º, as disposições processuais previstas no presente capítulo aplicam-se a processos relativos a crimes:
a) Previstos na presente lei;
b) Cometidos por meio de um sistema informático; ou
c) Em relação aos quais seja necessário proceder à recolha de prova em suporte electrónico.
2 - As disposições processuais previstas no presente capítulo não prejudicam o regime da Lei n.º 32/2008, de 17 de Julho.

e) Apreensão de dados informáticos (artigo 16.º);

f) Apreensão de correio electrónico e registos de comunicações de natureza semelhante (artigo 17.º);

g) Já nos artigos 18.º e 19.º prevêem-se dois meios de prova específicos para o combate a determinados tipos de crime, não aplicável ao crime de burla informática e nas comunicações.[29]

Actos urgentes a ordenar em sede de primeiro despacho

Dependendo dos factos em apreciação, cujas condutas poderão consubstanciar o crime em apreço, poderá mostrar-se essencial desde logo, no primeiro despacho:

I – **Assegurar a preservação de imagens de videovigilância**

Quando está em causa a utilização de dados sem autorização, talvez a forma mais comum do crime de burla informática e que se traduz na introdução não autorizada do PIN, para utilização de cartão bancário da vítima para levantamentos monetários em multibancos ou pagamentos em terminais automáticos.

Tais imagens poderão revelar-se essenciais para identificação do agente do crime, que efectuou os levantamentos ou os pagamentos caso existam, nesses locais sistemas de videovigilância, pelo que deverá ter-se em especial atenção o disposto nos artigos 8.º e 9.º, ambos da Lei n.º 1/2005, de 10 de Janeiro[30], nomeadamente o prazo de máximo de 30 dias, para a conservação das imagens captadas.

[29] Venâncio, Pedro Dias, Lei do Cibercrime anotada e comentada, Coimbra editora, 1ª edição, 2011, pág.91

[30] **Lei n.º 1/2005**
Artigo 8.º
Aspetos procedimentais
1 - Quando uma gravação, realizada de acordo com a presente lei, registe a prática de factos com relevância criminal, a força ou serviço de segurança que utilize o sistema elabora auto de notícia, que remete ao Ministério Público juntamente com a fita ou suporte original das imagens e sons, no mais curto prazo possível ou, no máximo, até 72 horas após o conhecimento da prática dos factos.
2 - Caso não seja possível a remessa do auto de notícia no prazo previsto no número anterior, a participação dos factos é feita verbal ou eletronicamente, remetendo-se o auto no mais curto prazo possível.
3 - A decisão de autorização de instalação de câmaras e a decisão de instalação em caso de urgência são comunicadas ao Ministério Público.
Artigo 9.º
Conservação das gravações
1 - As gravações obtidas de acordo com a presente lei são conservadas, em registo codificado, pelo prazo máximo de 30 dias contados desde a respetiva captação, sem prejuízo do disposto no artigo anterior.
2 - Todas as pessoas que tenham acesso às gravações realizadas nos termos da presente lei, em razão das suas funções, devem sobre as mesmas guardar sigilo, sob pena de procedimento criminal.
3 - Com exceção dos casos previstos no n.º 1, é proibida a cessão ou cópia das gravações obtidas de acordo com a presente lei.
4 - O código a que se refere o n.º 1 fica a cargo das forças e serviços de segurança responsáveis.

xemplo de primeiro despacho:

Os factos denunciados, abstractamente considerados, são susceptíveis de integrar, para além do mais, o crime de burla informática, previstos e punidos pelos artigos 221.º, n.º 1, do Código Penal.

Nos termos do artigo 270.º, n.º 4, do Código de Processo Penal e artigo 7.º, n.º 2, alínea l), da Lei n.º 49/2008, de 27 de Agosto, e Ponto II.1 da Circular da Procuradoria-Geral da República n.º 6/2002, delego na Polícia Judiciária, a competência para realização das investigações e diligências necessárias à instrução do presente inquérito, nomeadamente:

A) Inquirição na qualidade de testemunhas do queixoso (A), no prazo de 10 dias, devendo:

i. Fornecer cópias dos extractos bancários onde estejam discriminados os movimentos não autorizados, esclarecendo de forma pormenorizada:

1. Quais os movimentos bancários (levantamentos ou pagamentos) que foram realizados sem a sua autorização.
2. Se sabe ou suspeita de quem teve acesso ao seu cartão ou dados bancários e respectivo PIN ou dados de acesso.

ii. Indicar o nome e morada de testemunhas dos factos (familiares, vizinhos ou quaisquer outras pessoas que tenham assistido aos factos referidos)

B) Notificação de imediato da(s) respectiva(s) entidade(s) para preservação das imagens de videovigilância respeitantes aos dias, horas e locais onde foram efectuados os movimentos não autorizados identificados pelo queixoso.

C) Inquirição de todas as testemunhas dos factos conhecidas, e efectivação de todas as demais diligências que se tenham por úteis e oportunas para a investigação dos factos e descoberta da verdade.

Prazo: 60 dias

Deixando traslado, remeta os autos à Polícia Judiciária de …

Após 60 dias, nada sendo junto, solicite informações sobre o estado das investigações e a data em que previsivelmente estarão concluídas.

II – **Assegurar a recolha de IP's e a expedita identificação do seu utilizador**

Muitas das vezes a identificação do agente do crime passa pela identificação e localização do seu endereço "IP", que pode ser estático ou dinâmico, consoante os casos, mas em todos eles é atribuído por um prestador de serviços, para que seja possível identificar qual o utilizador

que estava ligado a determinado endereço "IP", num determinado dia e hora, os prestadores de acesso e de hospedagem devem manter uma base de dados electrónicos, tais bases de dados também tem prazos relativamente à preservação de dados, neste aspecto, transcreve-se, na parte aplicável ao crime de Burla informática e nas comunicações, o quadro explicativo constante da nota prática n.º 8/2016, de 18 de Fevereiro de 2016, do Gabinete do Cibercrime[31]

Tipo de dados	Âmbito	Prazo	Competência	Fundamento Legal
Identificação do cliente	Todos os crimes	Sem prazo	Ministério Público	Artigo 14.º, n.º 4, b), da Lei do Cibercrime
Endereço IP	Todos os crimes	6 meses	Ministério Público	Artigo 14.º, n.º 4, b), da Lei do Cibercrime

Nos casos em que existiram trocas de *emails* entre o suspeito e a vítima é essencial a recolha imediata dos Cabeçalhos Técnicos de Mensagens de Correio Eletrónico

III – **Após a identificação do IP do suspeito, solicitar o mais breve possível a identificação do utilizador às operadoras de comunicações ou fornecedores de serviços de internet**

Neste aspecto, assume particular importância a Circular da Procuradora-Geral da República nº 12/2012, de 25 de Setembro[32], que procede à uniformização de procedimentos de informação dirigidos aos operadores de comunicações.

Tal Circular teve origem num protocolo de cooperação efectuado com operadores de comunicações, no âmbito da investigação da cibercriminalidade e da obtenção de prova digital.

Assim, sempre que se mostre necessária a prestação de informação por parte de um operador e o Ministério Publico solicitar elementos de prova, deve fazê-lo através de um conjunto de formulários pré-elaborados, tornando os pedidos mais simples e eficazes.

Tais pedidos devem obedecer a um critério de necessidade, atendendo à descoberta da verdade, assim como de clareza quanto aos pedidos efectuados, indicando com exactidão os dados que pretendem.

Actualmente tais pedidos terão que ser remetidos via papel, pois ainda não se mostra em funcionamento a plataforma destinada à sua transmissão electrónica.

Exemplo de primeiro despacho:

Vide despacho supra (…)

[31] Disponível em: http://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/nota_pratica_8_pedido_de_info_a_isp_0.pdf.
[32] Disponível em: http://www.ministeriopublico.pt/iframe/circulares.

A) Inquirição na qualidade de testemunhas do queixoso (A), no prazo de 10 dias, devendo:

i. Esclarecer de forma pormenorizada, fazendo-se acompanhar dos *emails* trocados com o suspeito:

1. Qual o prejuízo que suportou com os factos denunciados.
2. Se sabe ou suspeita de quem foi o autor de tais factos.

ii. Indicar o nome e morada de testemunhas dos factos (familiares, vizinhos ou quaisquer outras pessoas que tenham assistido aos factos referidos)

iii. Deverá ser efectuada a imediata recolha dos Cabeçalhos Técnicos de Mensagens de Correio Eletrónico trocados entre o suspeito e vítima ou identificação por qualquer outra forma do IP do suspeito

B) Obtido o IP do suspeito deverá de imediato ser remetida tal informação ao Tribunal a fim de ser obtida a sua identificação junto das operadores ou fornecedores de serviços de internet.

(…)

IV. Buscas e apreensões

As Buscas e apreensões seguem um regime misto onde deverão ser tidas em consideração as normas previstas no código de processo penal e as normas processuais previstas na Lei do Cibercrime.

Definição e pressupostos da busca, artigo 174.º do Código de Processo Penal

Competência para determinar a busca, quanto ao crime de Burla Informática e nas comunicações:

– Juiz de Instrução no caso de buscas em casa habitada ou numa sua dependência fechada, artigos 177.º, n.º 1 e 269.º, n.º 1, al. c),

– No caso de buscas não domiciliárias, ressalvando os casos especiais[33], a competência para determinar a busca é da Autoridade Judiciária competente.

[33] Buscas não domiciliárias obrigatoriamente determinadas e presididas pelo Juiz de Instrução Criminal
Escritório de Advogado - artigo 177º/5 do CPP e artigo 70.º do Estatuto da Ordem dos Advogados;
Consultório médico -artigo 177º/5 do CPP;
Estabelecimento oficial de saúde artigo 177º, n.º 6, do CPP;
Estabelecimento bancário - artigo 181º/1 do CPP;
Domicílio pessoal ou profissional de Magistrados Judiciais e do Ministério Público (Estatutos respetivos);
Escritório ou local de arquivo de solicitador – artigo 105º do Estatuto dos Solicitadores;

Quanto à apreensão de dados informáticos seguem o regime dos artigos 16.º da Lei do Cibercrime Tal como o regime da pesquisa de dados informáticos tem semelhanças com o regime das tradicionais buscas, também o regime da apreensão de dados informáticos acaba por ser uma adaptação (à realidade digital) das tradicionais apreensões, reguladas pelos artigos 177.º e seguintes do Código de Processo Penal.

Assim, é a autoridade judiciária[34] que tem competência pra autorizar ou ordenar a realização da apreensão, podendo esta apreensão ser levada a cabo sem a prévia autorização da autoridade judiciária quando se verifique "urgência ou perigo na demora", nos termos do artigo 16.º n.ºs 1 e 2, da Lei do Cibercrime.

Nos termos do artigo 16.º, n.º 3, quando esteja em causa a apreensão de "dados pessoais ou íntimos, que possam pôr em causa a privacidade do respectivo titular", os mesmos têm que ser apresentados ao juiz, só podendo ser juntos aos autos após uma ponderação, que deverá ter em conta "os interesses do caso concreto".

O artigo 17.º da Lei do Cibercrime regula a apreensão das mensagens de correio electrónico e registos de natureza semelhante.

Exemplo de despacho de Busca Domiciliaria

Em face da prova carreada para os até ao momento, existem fortes indícios que o suspeito (A) continua a manter na sua registos das operações informáticas que levou a cabo, e que se traduziram num prejuízo no montante de (x) para o lesado (B).

Não se vislumbrando neste momento outras diligências, para além das que infra se requerem, que se mostrem úteis ao esclarecimento dos factos e descoberta da verdade, afigurando-se necessário e adequado, neste momento, a realização de buscas à residência do suspeito, de forma a serem apreendidos todos os computadores pessoais, telemóveis e todos os dispositivos ou meios de armazenamento digital que ai forem encontrados, e que contenham armazenados registos das operações informáticas efectuadas.

Nestes Termos,

1. Remetam-se os presentes autos à Secção Central de Instrução Criminal para que, com urgência, apresentados ao Mmº. Juiz de Instrução, a quem se requer:

i. Que seja ordenada a busca à residência do suspeito (A), sita na Rua xxx, em Setúbal, e respectivas arrecadações, logradouros, anexos e garagens, se necessário com recurso a arrombamento, a realizar pela Polícia Judiciária, para apreensão dos seus computadores pessoais, telemóveis e todos os dispositivos ou meios de armazenamento digital que ai

Órgão de comunicação social - artigos 11º, n.º 6 do Estatuto dos Jornalistas;
Escritório de Revisores Oficiais de Contas - artigo 72º A e 72.º B do Estatuto dos ROCS.

[34] Verdelho, Pedro, A NOVA Lei do Cibercrime - revista de direito comparado português e brasileiro, Outubro a Dezembro 2009, Tomo LVIII, número 320, pág. 741.

forem encontrados, e que contenham armazenados registos das operações informáticas que consubstanciam o crime de Burla informática em investigação, sendo emitidos os respectivos mandados, pelo prazo de 30 dias, nos termos das disposições conjugadas dos artigos 32.º, n.º 4 da Constituição da República Portuguesa e 174.º, 176.º, 177.º, n.º 1 e 269.º, n.º 1, alínea c), todos do Código de Processo Penal.

ii. Que seja autorizada a apreensão de todas as mensagens de correio electrónico ou SMS, que se reportem às mensagens trocadas entre suspeito e lesado, nos termos das disposições conjugadas do artigo 17.º da Lei n.º 109/2009, de 15 de Setembro e 179.º, n.ºs 2 e 3, do Código de Processo Penal, por se afigurar que poderão ser fundamentais para a descoberta da verdade e para a prova,

***

2. Caso mereça deferimento a pretensão do Ministério Público, desde já se autoriza, pelo prazo de 30 dias, nos termos do artigo 15.º, n.ºs 1 e 2, da Lei n.º 109/2009, de 15 de Setembro, que o OPC responsável pela realização da busca, proceda a uma pesquisa informática nos computadores pessoais, telemóveis e todos os dispositivos ou meios de armazenamento digital que ai forem encontrados, <u>para que sejam apreendidos, apenas aqueles que contenham armazenados elementos de prova relevantes para os presentes autos</u>.

***

3. Mais se determina a apreensão de todos os dados ou documentos informáticos cujo conteúdo seja necessário para a prova, caso o conteúdo de tais dados seja susceptível de revelar dados pessoais ou íntimos, que possam pôr em causa a privacidade do respectivo titular ou de terceiro, deverão tais dados ou documentos ser de imediato apresentados, pelo OPC, ao juiz de instrução, para que este pondere a sua junção aos autos, nos termos do artigo 16.º, n.ºs 1 e 3, da Lei n.º 109/2009, de 15 de Setembro.

Após a devolução dos autos, entregue o inquérito à Policia Judiciária, deixando traslado, para cumprimento dos mandados de busca e demais diligências de investigação.

Prazo 30 dias, nada sendo junto, solicite informações sobre o estado das investigações e a data em que previsivelmente estarão concluídas.

O Gabinete do Cibercrime da Procuradoria Geral da República

No dia 7 de Dezembro de 2011 foi criado por despacho do Procurador-Geral da República Gabinete Cibercrime, que tem sede na Procuradoria-Geral da República, de quem é diretamente dependente. Tem como propósitos a coordenação, a formação específica de magistrados do Ministério Público, a interação com o setor privado e os órgãos de polícia criminal e, residualmente, o acompanhamento de processos concretos.

O Gabinete Cibercrime é neste momento coordenado pelo Exmo. Procurador da República Dr. Pedro Verdelho, e segundo a informação institucional constante da página da internet de tal

gabinete[35] *"mantém uma rede de pontos de contacto em todo o território nacional (pelo menos, um magistrado por cada uma das Comarcas). Aos pontos de contacto da rede compete estabelecer a comunicação do Gabinete Cibercrime com os colegas da sua Comarca, partilhando, num sentido, as questões referentes a cibercrime e a obtenção de prova digital que se suscitarem nos processos concretos; no outro, o resultado dos debates que se forem suscitando.*

Nalgumas Comarcas, o ponto de contacto é assegurado pelos magistrados a quem são distribuídos os inquéritos desta área (crimes previstos na Lei do Cibercrime e burlas informáticas) e os inquéritos em que haja particulares exigências na obtenção de prova digital ou em que se investiguem factualidades particularmente complexas, praticas com o uso de tecnologias. Nas restantes comarcas, sendo os pontos de contacto igualmente magistrados especializados nestas temáticas ou particularmente sensibilizados ou interessados nelas, são também um embrião de uma futura especialização na distribuição de processos deste tipo."

Pelo Gabinete do cibercrime são ainda publicadas na sua página da internet e também através do SIMP – separador temático sobre o cibercrime – notas práticas, na sua maioria relacionadas com procedimentos quanto à recolha de prova em ambiente digital.

Desde o ano de 2015 o referido gabinete tem vindo a publicar anualmente duas notas práticas sobre a jurisprudência mais relevante do ano respectivo, uma sobre os tipos legais relacionados com a criminalidade informática e outra sobre a prova digital.

Sendo que, quanto ao crime de burla informática e nas comunicações, as notas práticas relativas aos anos de 2015 a 2017 referem que a maioria da jurisprudência relaciona-se com as situações de facto, relacionadas com levantamento de dinheiro em utilização indevida de cartões bancários. Sendo tal jurisprudência ainda escassa e em geral, as decisões conhecidas incidem sobre a essência do tipo de crime, quer na sua generalidade, quer na relação com outros tipos legais que com este conexos.

2.1.3. Encerramento do inquérito

Quanto às formas de encerramento do inquérito o crime de Burla informática e nas comunicações, previsto e punido no artigo 221.º do Código Penal, não tem qualquer especificidade que cumpra destacar, ou seja, realizadas todas as diligências úteis e pertinentes à descoberta da verdade e ao esclarecimento dos factos, visando investigar o crime em causa, determinar os seus agentes e a sua responsabilidade, haverá, conforme o caso, lugar ao arquivamento do inquérito – artigo 277º, n.ºs 1 e 2, do Código de Processo Penal ou caso sejam recolhidos indícios suficientes da prática do crime à suspensão provisória do processo, a requerimento para aplicação de pena em processo sumaríssimo ou a acusação pública para julgamentos em processo abreviado ou comum.

[35] http://cibercrime.ministeriopublico.pt/pagina/quem-somos.

Por se tratar de criminalidade reditícia, chama-se a atenção para a possibilidade da aplicação do instituto da perda de instrumentos, produtos e vantagens do crime – sem prejuízo dos direitos do ofendido, artigo 110.º, n.º 6, do Código de Processo Penal – (v.g. material informático usado na prática dos factos e valores monetários de que o agente se apropriou), nos termos artigos 109.º, 110.º e 111.º, todos do Código Penal.

V. Hiperligações e referências bibliográficas

Hiperligações

Centro de Estudos Judiciários
Comissão Europeia
Parlamento Europeu
www.dgsi.pt
http://cibercrime.ministeriopublico.pt/
http://cibercrime.ministeriopublico.pt/notas-praticas
http://www.ministeriopublico.pt/iframe/circulares

Referências bibliográficas

Albuquerque, Paulo Pinto de, Comentário ao Código Penal à Luz da Constituição da República e da Convenção Europeia dos Direitos do Homem, Universidade Católica, 3.ª edição, 2015;

Barreiros, José António, Crimes contra o Património no Código Penal de 1995, Universidade Lusíada, 1996;

Código Penal – Actas e Projecto da Comissão de Revisão, 1993;

Costa, Almeida, Comentário Conimbricense ao Código Penal, Tomo II, Coimbra Editora, 1999;

Garcia, M, Miguez, Código Penal parte geral e especial com notas e comentários, Almedina, 2.ª edição, 2015;

José de faria Costa e Helena Moniz, Algumas Reflexões sobre a criminalidade informática em Portugal, *in* BFDUC, Vol. LXXIII, 1997;

Rocha, Lopes, A revisão do Código Penal, Soluções de neocriminalização, Jornadas do Direito Criminal do CEJ, 1993;

Santos, Manuel Simas e Leal-Henriques, Manuel, Código Penal Anotado, Volume III – Artigos 131.º ao 235.º, 4ª Edição, Rei dos Livros, 2016;

SILVA, GERMANO MARQUES DA, Direito Processual Penal Português do Procedimento (marcha do processo), Universidade Católica Editora, 2015;

Schjølberg, Stein "The History of Cybercrime: 1976-2014", Kindle Edition, 2014;

Teixeira, Paulo Alexandre Gonçalves, O Fenómeno do Phishing – Enquadramento Jurídico-Penal, Dissertação de Mestrado, Universidade Autónoma de Lisboa, 2013;

Venâncio, Pedro Dias, Lei do Cibercrime anotada e comentada, Coimbra Editora, 1.ª edição, 2011;
Verdelho, Pedro, a NOVA Lei do Cibercrime – revista de direito comparado português e brasileiro, Outubro a Dezembro 2009, Tomo LVIII, número 320;

Verdelho, Pedro – Phishing e outras formas de defraudação nas redes de comunicação, Direito da sociedade de informação, volume VIII, Coimbra Editora, 2009.

7.
O crime de abuso de cartão de garantia ou de crédito. Enquadramento jurídico, prática e gestão processual

Rui Miguel Ferreira

dos Santos Cruz

CENTRO
DE ESTUDOS
JUDICIÁRIOS

7. O CRIME DE ABUSO DE CARTÃO DE GARANTIA OU DE CRÉDITO. ENQUADRAMENTO JURÍDICO, PRÁTICA E GESTÃO PROCESSUAL

Rui Miguel Ferreira dos Santos Cruz

I. Introdução

O presente trabalho versará sobre o crime de abuso de cartão de garantia ou de crédito, previsto no artigo 225.º do Código Penal, ínsito no Capítulo III – Crimes contra o património em geral. A pertinência do tema está relacionada com a utilização que é dada a este tipo de cartões e cujo tipo criminal, muitas vezes, se confunde com outros que lhe são próximos, nomeadamente, o crime de burla informática, o que poderá levar a alguma confusão, com implicações óbvias no andamento da investigação e no desfecho do inquérito. Este tipo criminal já foi objeto de atenção redobrada por parte do legislador, quando, por força dos artigos 3.º, n.º 1, b), e 4.º, n.º 1, b) da Lei 38/2009, de 20 de Julho, quis que a prevenção e investigação deste crime fossem prioritárias. Assim, apesar de ser considerado, amiúde, que este ilícito só poderá ocorrer da forma tradicional, entenda-se, através da utilização do cartão de garantia ou de crédito em compras convencionais, veremos que também poderá suceder em ambiente digital.

II. Objetivos

O presente guia tem como principais destinatários os magistrados do Ministério Público e tem o fito de lhes emprestar algumas soluções quando se depararem com inquéritos relativos a este tipo de crime. Por força da economia de espaço necessária nesta exposição, não será possível uma abordagem exaustiva de todas as vertentes passíveis de se verificarem aquando da sua ocorrência, pelo que nos debruçaremos sobre os aspetos que entendemos como mais pertinentes.

III. Resumo

Faremos o enquadramento jurídico deste ilícito criminal, onde nos empenharemos sobre o bem jurídico protegido, os elementos objetivos, o elemento subjetivo, os elementos qualificadores, a atenuação especial e a extinção da responsabilidade criminal, a tentativa, o concurso e as várias naturezas do crime.

Seguidamente, faremos uma exposição sobre o andamento do inquérito e respetiva estratégia, passando pelos meios de obtenção de prova aplicáveis a este tipo de crime, terminando com as soluções possíveis de que os magistrados podem lançar mão.

1. Enquadramento Jurídico

1.1. Do crime de abuso de cartão de garantia ou de crédito

O crime de abuso de cartão de garantia ou de crédito vem previsto no artigo. 225.º do Código Penal. Tal preceito, explana o seguinte:

"*1 – Quem, abusando da possibilidade, conferida pela posse de cartão de garantia ou de crédito, de levar o emitente a fazer um pagamento, causar prejuízo a este ou a terceiro é punido com pena de prisão até 3 anos ou com pena de multa.*
– A tentativa é punível.
– O procedimento criminal depende de queixa.
– É correspondentemente aplicável o disposto nos artigos 206.º e 207.º 5
– Se o prejuízo for:
De valor elevado, o agente é punido com pena de prisão até 5 anos ou com pena de multa até 600 dias;
De valor consideravelmente elevado, o agente é punido com pena de prisão de 2 a 8 anos.
6 – No caso previsto no número anterior é correspondentemente aplicável o disposto no artigo 206.º."

Este tipo criminal foi introduzido pelo DL 48/95 de 15 de Março, por proposta do Exmo. Conselheiro Sousa e Brito[1]. Tal introdução não foi pacífica, porque se levantavam dúvidas sobre a dignidade penal destas condutas, já que as mesmas resultam do facto de se violarem regras contratuais (as quais estão subjacentes à emissão dos próprios cartões), tratando-se, portanto, de uma responsabilização penal por obrigações civis.

Mas a justificação para tal introdução, aponta, todavia, noutro sentido, que é o de que em causa está um abuso de uma relação de confiança que é concedida ao agente e que tem como único escopo causar um empobrecimento no património alheio[2]. Teve como objetivo colmatar uma lacuna de punibilidade, uma vez que a conduta do titular do cartão de garantia ou de crédito que o utilizasse conhecendo a sua impossibilidade de pagamento, era atípica. Quanto ao terceiro que utilizava um cartão de outrem sem a devida autorização, já seria punível pelo crime de burla, nos termos do artigo 217.º do Código Penal, se o enganado fosse uma pessoa, ou pelo crime de burla informática, nos termos do artigo 221.º do mesmo diploma legal (cuja introdução foi contemporânea com a do crime que agora estudamos), se fosse cometido através de manipulação informática.[3]

O que se cura neste tipo criminal é a utilização "abusiva" de dois tipos de cartão: o de **garantia** e o de **crédito**. Importa, por isso, explicar em que consistem estes cartões.

Desse modo, o **cartão de garantia** é um "*cartão destinado a garantir, até um determinado montante, cheques que foram validados por um comerciante, quer com base num cartão emitido ao titular do cheque ou através de uma base de dados central, à qual os comerciantes têm acesso. Os cheques validados são garantidos pela entidade emissora do cartão de garantia, o banco sacado ou pelo operador do sistema. Este cartão pode acumular outras funções, como, por exemplo, a de cartão de caixa ou de cartão de débito.*"[4].

Já o **cartão de crédito** é um "*cartão que indica que foi concedida uma linha de crédito ao seu titular, permitindo-lhe efectuar compras e/ou levantar dinheiro ("cash-advance") até um limite acordado previamente; o crédito concedido pode ser liquidado na sua totalidade no final de um período específico ou pode ser liquidado parcialmente, sendo o saldo considerado como uma extensão do crédito. São cobrados juros sobre o montante de qualquer extensão do crédito e, por vezes, é cobrada uma comissão anual ao respectivo titular.*"[5]. No fundo,

[1] *In* Código Penal, Actas e Projecto da Comissão de Revisão, Rei dos Livros, Acta n.º 39, de 9 de Julho de 1990, pág. 450.
[2] Ideia avançada por CUNHA, J. M. Damião, *in* Comentário Conimbricense do Código Penal, Parte Especial, Tomo II, Coimbra Editora, 1999, pág. 374.
[3] Como nos explica ALBUQUERQUE, Paulo Pinto, *in* Comentário do Código Penal, à Luz da Constituição da República e da Convenção Europeia dos Direitos do Homem, UCP, 2008, pág. 620. Concordante, parece-nos, ROCHA, Miguel António Lopes, *in* A Revisão do Código Penal, Soluções de Neocriminalização, Jornadas de Direito Criminal, Revisão do Código Penal, CEJ, Volume I, pág. 96. Mas com algumas críticas sobre este preceito, DANTAS, António Leones, *in* A Revisão do Código Penal e os Crimes Patrimoniais, Jornadas de Direito Criminal, Revisão do Código Penal, CEJ, Volume II, págs. 516 e 517.
[4] Definição constante em https://www.bportugal.pt/glossario/c.
[5] Definição constante em https://www.bportugal.pt/glossario/c. Também poderá ser encontrada outra definição no Aviso do Banco de Portugal n.º 11/2001, no seu artigo 1.º, a), que consagra a definição de cartão de crédito como "*qualquer instrumento de pagamento, para uso eletrónico ou não, que seja emitido por uma instituição de crédito ou por uma sociedade financeira (adiante designadas por emitentes) que possibilite ao seu detentor*

difere-se para o futuro o pagamento pelo titular do cartão. Assim, o **cartão de crédito** "*integra-se num sistema que compreende três partes (…), reunindo sucessivamente a entidade emissora (…), geralmente um grupo de bancos, o titular do cartão de crédito (…) e um universo de comerciantes aderentes (…). Quando se faz uma compra, a pessoa legitimada para usar o cartão (…) aceita pagar ao emitente assinando a fatura do comerciante, donde constam os elementos do cartão e a indicação do quantitativo a pagar. O vendedor tem meios de verificar se o cartão é válido e se o titular dispõe de crédito suficiente para pagar o preço. (…) Para o comércio, uma transação com cartão de crédito é mais segura do que outras formas de pagamento (…).*"[6].

Não são, por isso, abrangidos por esta incriminação, os cartões de débito ou os cartões de moeda eletrónica, os quais importam para o titular o débito imediato do valor disponível, no ato da sua utilização. Ou seja, estes cartões estão associados a uma determinada conta. Por isso mesmo, em relação ao cartão de garantia ou de crédito, se os mesmos acumularem a função de cartão de débito[7], há que distinguir se a sua utilização versou sobre essa vertente. Se assim foi, então, a conduta é atípica, relativamente ao tipo criminal em apreço.

Aqui chegados, é importante que nos detenhamos e aprofundemos a abrangência que tem a aplicação deste preceito. Assim, torna-se mister elencar os argumentos para tal interpretação:

- O artigo 225.º do Código Penal é uma norma especial, já que trata, apenas, da utilização do cartão de garantia ou de crédito, sendo o único preceito em todo o Código Penal que tutela expressamente a utilização abusiva deste tipo de cartões;

- Como já foi referido *supra*, este tipo criminal foi introduzido pelo DL 48/95, de 15 de Março, o qual entrou em vigor no dia 1 de Outubro desse mesmo ano. Ou seja, acompanha-nos há cerca de 23 anos e nunca foi alterado;

- Com esta introdução, e como também já foi acima explicado, o legislador visou afastar a punição do abuso de cartão de garantia ou de crédito pelo artigo 217.º do Código Penal (quando realizada por terceiro) ou pelo artigo 221.º do Código Penal (quando realizada através da utilização de meios informáticos), já que, ao criar o artigo 225.º do Código Penal, pretendeu, claramente, aglutinar todas as condutas num único tipo criminal. Esta ideia retira-se da inclusão, logo no início do preceito do ínsito "*Quem*", abrangendo por isso, tanto o titular do cartão, como terceiros, ou seja, abrange todas as pessoas, tratando-se, por isso, de um crime comum;

- Apesar deste ilícito criminal ter sido introduzido no longínquo ano de 1995, onde o cartão de crédito era utilizado unicamente nas máquinas das lojas (vulgo "*ferro de*

(adiante designado por titular) a utilização de crédito outorgado pela emitente, em especial para a aquisição de bens ou de serviços." (https://www.bportugal.pt/sites/default/files/anexos/cartas-circulares/11-2001a.pdf).
[6] GARCIA, M. Miguez e RIO, Castela, *in* Código Penal, Parte Geral e Especial, Almedina, 2015, 2.ª edição, pág. 952.
[7] Situação possível, conforme a definição *supra* descrita.

engomar"), nos dias de hoje, a sua utilização poderá ocorrer em muito mais situações. É que, desde aquela altura, até à atualidade, a tecnologia evoluiu de forma absolutamente estrondosa e, como tal, aumentou as possibilidades de utilização dos cartões de garantia ou de crédito. Há, por isso, que fazer uma interpretação atualista do preceito[8], nos termos do artigo 9.º, n.º 1 do Código Civil. Tal interpretação atualista versará sobre o ínsito "*abusando da possibilidade*", permitindo que, tal conduta, abranja todas as possibilidades e todas as modalidades passíveis de existirem atualmente nos cartões de crédito e que não existiam no ano de 1995, quando o preceito foi introduzido, ou seja, a interpretação a fazer será a de que o que é abarcado por este crime, é uma utilização abusiva, qualquer que seja a modalidade dessa utilização;

- De referir que o preceito que aqui curamos nunca foi alterado, logo, o legislador terá querido que o mesmo mantivesse a sua aplicação, até porque, se quisesse que as condutas por ele abrangidas fossem tuteladas por outro preceito, tê-lo-ia feito expressamente, como ocorreu com o crime de falsidade informática, previsto no artigo 3.º, n.º 2, da Lei 109/2009, de 15 de Setembro (Lei do Cibercrime). Mas o facto é que o legislador manteve a sua opção original. Note-se, ainda, o teor dos artigos 3.º, n.º 1, b), e 4.º, n.º 1, b), da Lei 38/2009, de 20 de Julho (Lei de Política Criminal – Biénio de 2009-2011). Naquela altura, já a tecnologia seria muito próxima da que temos actualmente e o sistema que funcionava em 1995, era puramente residual, quando comparado com o que já existia em 2009, mas o legislador entendeu que "*a burla informática e nas telecomunicações prevista na alínea b) do n.º 5 do artigo 221.º do Código Penal e o abuso de cartão de garantia ou de crédito previsto na alínea b) do n.º 5 do artigo 225.º do Código Penal*" eram de investigação prioritária, ou seja, estava atento à evolução e percebeu que, com o advento da tecnologia, as formas de consumar o crime são muito mais do que as que existiam originalmente.

- Mas há, ainda, um argumento forte que entendemos ser preponderante. O artigo 225.º, n.º 4, do Código Penal prevê expressamente a aplicação do artigo 207.º do mesmo diploma legal (o qual trata da acusação particular). Imagine-se, então, a seguinte situação: um jovem que, viciado em jogos da *Playstation*, não tira boas notas na escola e o pai proíbe-o de comprar mais jogos. O jovem, na sua rebeldia, aproveita uma distração do pai e retira-lhe o cartão de crédito, com o respetivo código, e faz uma compra. Se o fizer numa loja, apresentando o cartão, dúvidas não restarão que estamos no âmbito do "nosso" crime, usufruindo do regime previsto no artigo 207.º do Código Penal. Mas, e se for uma compra *online*, ou seja, a mesma compra, pelo mesmo preço, utilizando o mesmo cartão (neste caso, os seus dados

[8] A interpretação atualista é perfeitamente admissível em Direito Penal, desde que não se contenda com o princípio da legalidade. Neste sentido, entre outros, avulta o Acórdão de Fixação do Jurisprudência do Supremo Tribunal de Justiça 5/2008, o qual se encontra acessível para leitura integral em https://dre.pt/application/dir/pdf1sdip/2008/05/09200/0262302628.PDF, explanando que "*a interpretação atualista não será completamente inadmissível em direito penal, mas ela terá de ser afastada sempre que implicar a violação de algum dos princípios estruturais do direito penal, como é o princípio da legalidade, que tem assento na própria CRP — artigo 29.º, n.ºs 1 e 3.*"

> informáticos) e originando o mesmo prejuízo, já não é o crime que aqui curamos, mas o de burla informática e o dito jovem já não poderá beneficiar daquele regime? Não nos parece que tenha sido essa a intenção do legislador, isto é, não cremos que o legislador queira ter afastado aquele regime, só porque a compra foi feita *online* e não na loja.

Esta é a única interpretação possível de se fazer, sob pena de o preceito ficar completamente vazio de conteúdo, o que, como é bom de ver, seria absolutamente contra a vontade do legislador.

Pelo agora exposto, e por ser imprescindível esta distinção, vincamos que se estivermos perante uma situação em que foi utilizado, de forma abusiva, um cartão de garantia ou de crédito e desde que essa utilização tenha sido no âmbito da sua real função (aquela para que foram emitidos), então, seja a utilização física (tendo o cartão na mão, entenda-se), seja em ambiente digital (através da inserção de dados dos mesmos num qualquer sistema informático), o crime praticado é aquele que aqui nos ocupa, porque é um crime especial relativamente a outros. Mais, não releva para esta classificação se o cartão exige a inserção de um PIN ou não[9] ou se tem inserido um chip ou, ainda, se é utilizado *online* ou em caixas de pagamento automático. O que releva, única e exclusivamente, é que a utilização abusiva ocorra através da utilização de um cartão de crédito no âmbito das suas reais funções.

1.2. O bem jurídico tutelado

O bem jurídico tutelado por esta incriminação é o património de outra pessoa. O património inclui, numa conceção jurídico-económica, "*todos os direitos, as posições jurídicas e as expetativas com valor económico compatíveis com a ordem jurídica*."[10]. Podemos ainda acrescentar que "*paralelamente, também o crédito em geral e a confiança que merecem os cartões como meios de pagamento são aqui acessoriamente defendidas*."[11]

1.3. Os elementos objetivos

Este tipo criminal é constituído por vários elementos objetivos, designadamente, *o abuso da possibilidade conferida pela posse do cartão de garantia ou de crédito* e que, tal utilização abusiva, *leve o emitente a fazer um pagamento* e *causando prejuízo a este ou a terceiro*.

[9] Realidade reiterada por CUNHA, J. M. Damião, *in op. cit.*, pág. 377 e ALBUQUERQUE, Paulo Pinto de, *in op. cit.*, pág. 621.
[10] ALBUQUERQUE, Paulo Pinto de, *in op. cit.*, pág. 598, mas SÁ PEREIRA, Victor e LAFAYETTE, Alexandre, *in* Código Penal Anotado e Comentado, QUIDJURIS, 2008, pág. 598, entendem que o que se protege aqui é o património individual do emitente, porque "*é este, com efeito, que, pagando, sofre um prejuízo, desencadeado pelo abuso do utilizador, ao servir-se, de modo ilegítimo, da 'possibilidade de levar o emissor a fazer um pagamento'*".
[11] BARREIROS, José António, *in* Crimes Contra o Património no Código Penal de 1995, CEJ, 1996, pág. 215.

Primeiro, importa relembrar que, para que este crime possa ser praticado, é necessário que o agente tenha na sua posse o cartão de garantia ou de crédito, seja em termos físicos, sejam os dados digitais a eles referentes.

Dissertemos sobre cada um destes elementos. Assim, relativamente ao *abuso da possibilidade conferida pela posse do cartão de garantia ou de crédito*, tal situação consiste em utilizar tais cartões sem autorização para tal. Ou seja, este elemento preenche-se aquando da utilização abusiva do cartão de garantia ou de crédito, em duas situações distintas:

■ Quando o próprio titular do cartão o utiliza fora das situações contratadas com a entidade emitente, seja quando ultrapassa o *plafond* acordado, seja quando é utilizado após ter cessado o período da sua validade (situação este que, nos dias de hoje, dificilmente poderá ocorrer) ou

■ Quando um terceiro, sem autorização do titular, utiliza o cartão, não sendo necessário, quanto a nós, que tal cartão já tenha passado da sua validade ou que se ultrapasse o limite do crédito concedido, bastando que a utilização não tenha sido autorizada pelo seu titular.

Temos assim um tipo alargado, em que está abrangido, não só o titular do cartão, mas também, um terceiro.

Quanto ao segundo elemento objetivo, o levar o emitente a fazer um pagamento, fica preenchido quando, como consequência da utilização abusiva do cartão de garantia ou de crédito, o emitente efetua um pagamento. Ou seja, por força da relação de confiança que estes cartões oferecem, a sua utilização acaba por levar a que o emitente realize o pagamento do valor do incremento patrimonial que o utilizador abusivo pretende alcançar.

Resta, ainda, um último elemento objetivo, que é causar prejuízo ao emitente ou a terceiro. Assim, para que a conduta seja típica, necessário se torna que a ação empreendida pelo agente provoque um prejuízo patrimonial à entidade emitente do cartão ou a terceiro (normalmente, o titular, mas poderá, eventualmente, ser o comerciante). Como tal, este elemento fica preenchido quando ocorre um empobrecimento no património do ofendido, descontando-se o proveito que ele tenha, eventualmente, obtido em consequência da conduta do agente. Assim sendo, a partir do momento em que ocorre um empobrecimento patrimonial, o crime consuma-se.

Trata-se, por isso, de um crime de dano e de resultado.

1.4. O elemento subjetivo

O elemento subjetivo deste tipo criminal só admite o dolo, em qualquer das suas vertentes. Ou seja, para o preenchimento do elemento subjetivo do tipo criminal em apreço, torna-se necessário que o agente queira o resultado previsto. Destarte, é necessário que se encontrem

reunidos os dois elementos do dolo, designadamente, o elemento volitivo e o elemento intelectual. Quanto ao primeiro, é sabido que se trata da vontade que o agente tem de cometer o crime. Ele quer atingir o resultado pretendido. Quando ao elemento intelectual, necessário se torna que se encontrem reunidos, tanto a representação do abuso, como do prejuízo.[12] Exige-se, apenas, o dolo genérico.[13]

1.5. Os elementos qualificadores

No n.º 5 do preceito que aqui tratamos, o legislador estabeleceu graus de qualificação, da mesma forma que o fez em relação a outros crimes contra o património em geral, nomeadamente, os crimes de burla (se bem que, neste caso, um crime autónomo, previsto no artigo 218.º do Código Penal), burla relativa a seguros (artigo 219.º, n.º 4, a) e b) do Código Penal) e burla informática (artigo 221.º, n.º 5, a) e b), do Código Penal). Trata-se de uma opção legislativa de submeter a uma punição mais pesada as condutas em que o agente origina um prejuízo maior à vítima, o que nos parece perfeitamente lógico.

Como tal, foram previstos dois graus de qualificação, tendo como balizas, tanto o valor elevado, como o valor consideravelmente elevado do prejuízo. Temos, por isso, que lançar mão dos conceitos previstos no artigo 202.º, a) e b), do Código Penal.

1.6. A atenuação especial da pena e a extinção da responsabilidade criminal

O preceito prevê, também, uma atenuação especial da pena por força da aplicação do artigo 206.º, n.º 2 do Código Penal, se houver restituição ou reparação. Tal atenuação é aplicável ao crime simples (n.º 4), bem como aos crimes agravados (n.º 6). Funciona, por isso, em conexão com os artigos 72.º e 73.º do Código Penal.

Mas a aplicação daquele preceito, por força do seu n.º 1, poderá implicar, também, a extinção da responsabilidade criminal. Esta opção tem a ver com uma questão de prevenção, já que "*as necessidades preventivas desaparecem em relação ao agente que repõe integralmente as coisas no estado em que elas se encontravam antes do crime cometido.*".[14]

1.7. A natureza do crime

O crime de abuso de cartão de garantia ou de crédito pode revestir-se de natureza pública, semipública ou particular.

[12] Ideia que nos é explicada por SÁ PEREIRA, Victor e LAFAYETTE, Alexandre, *in op. cit.*, pág. 599.
[13] Situação que é criticada por BARREIROS, José António, *in op. cit.*, pág. 217, que entende ser inadmissível que, apesar de estarmos perante um crime contra o património, não se prever um dolo específico de enriquecimento.
[14] ALBUQUERQUE, Paulo Pinto de, *in op. cit.*, pág. 570.

Assim, se estivermos no âmbito de uma conduta subsumível aos elementos previstos para o crime simples (n.º 1), a natureza do crime será semipública, por força do n.º 3 do mesmo artigo, ou seja, sujeita às regras do artigo 49.º do Código de Processo Penal. Mas poderá acontecer que, por estarmos no âmbito da aplicação do artigo 207.º do Código Penal, *ex vi* n.º 4 do artigo em apreço, a natureza do crime seja particular, logo, sujeita ao explanado no artigo 50.º do Código de Processo Penal.

Quanto aos tipos do n.º 5, os mesmos têm natureza pública.

1.8. A tentativa

O crime de abuso de cartão de garantia ou de crédito prevê, no n.º 2 do preceito, a punibilidade da tentativa. De facto, o tipo de prejuízos que estas condutas podem provocar, bem como, a situação fragilizada em que a vítima poderá ficar, obrigaram a que o legislador tenha tomado medidas mais drásticas, a fim de afastar a possibilidade de ocorrência deste tipo de crime.

Quanto a este regime, importa explanar aqui a ideia de que esta previsão da punibilidade da tentativa, apenas se justifica para as situações previstas no n.º 1, porque em relação às condutas previstas no n.º 3, a tentativa é sempre punível, por força ao abrigo do consagrado no artigo 23.º, n.º 1, do Código Penal.

A tentativa neste tipo de crime ocorrerá quando são realizados atos de execução, previstos no artigo 22.º, n.º 2, do Código Penal. Mas poderão ocorrer situações em que a tentativa se reveste de tal impossibilidade que, por essa razão, terá de se lhe aplicar o regime previsto no artigo 23.º, n.º 3, do mesmo diploma legal, ou seja, tratando-se de uma tentativa impossível, tal é a ineptidão do meio utilizado[15]. E isto decorre das condições de segurança que rodeiam a utilização deste tipo de cartões. Mas já é considerada tentativa, a situação em que o agente tenta utilizar um cartão numa determinada compra e o funcionário da loja se apercebe de que o cartão não lhe pertence ou que já está fora do prazo. É também aplicável o artigo 24.º do Código Penal.

[15] Sobre a ineptidão do meio, e apesar de versar sobre o crime de burla informática, mas perfeitamente aplicável ao crime que aqui trabalhamos, o Ac. TRE de 26-06-2012 (relator Martinho Cardoso), processo n.º 264/06.6GBPSR.E1, acessível para leitura com texto integral em www.dgsi.pt, indica-nos que "*não se pode concluir que o digitar aleatório de três códigos seja manifestamente inidóneo para a produção do resultado almejado de proceder ao levantamento de dinheiro com um cartão multibanco a que se acedeu ilicitamente e contra a vontade do legítimo titular e do qual não se tem o código. Digitar à sorte três códigos não é, por natureza, um meio inapto, de uma inidoneidade absoluta, para acertar no código do cartão multibanco. Digitar à sorte três códigos, sendo um meio em si mesmo idóneo ou apto, tornou-se inapto para produzir o resultado, por o agente não ter acertado na combinação correcta.*"

1.9. A forma continuada

No ilícito criminal em apreço, importa tratar de uma figura que cremos ser de vital importância na sua investigação e que poderá levar a resultados diferentes, conforme o ponto de vista com que se encaram estas situações. Falamos do crime continuado.

Assim, diz-nos o artigo 30.º, n.º 2 do Código Penal que "*Constitui um só crime continuado a realização plúrima do mesmo tipo de crime ou de vários tipos de crime que fundamentalmente protejam o mesmo bem jurídico, executada por forma essencialmente homogénea e no quadro da solicitação de uma mesma situação exterior que diminua consideravelmente a culpa do agente*.". Ora, quer isto dizer que o agente do crime, quando sujeito a um estímulo externo, determina-se a cometer, várias vezes, o mesmo ilícito criminal, sendo essa uma forma de diminuir consideravelmente a sua culpa.[16]

Interessante, neste momento, determinar "*as situações exteriores típicas que, preparando as coisas para a repetição da actividade criminosa, diminuem consideravelmente o grau de culpa do agente: a) assim, desde logo, a circunstância de se ter criado, através da primeira actividade criminosa, uma certa relação, um acordo entre os seus sujeitos; b) a circunstância de voltar a verificar-se uma oportunidade favorável à prática do crime, que já foi aproveitada ou que arrastou o agente para a primeira conduta criminosa; c)a circunstância da perduração do meio apto para realizar um delito, que se criou ou adquiriu com vista a executar a primeira conduta criminosa; d) a circunstância de o agente, depois de executar a resolução que tomara, verificar que se lhe oferece a possibilidade de alargar o âmbito da sua actividade criminosa."*[17]

O tipo criminal que agora abordamos é um dos exemplos paradigmáticos para a aplicação do instituto do crime continuado, senão vejamos: Imaginemos um indivíduo que consegue chegar à posse de um cartão de crédito e com ele vai fazendo pagamentos diários durante uma semana seguida. Nesta situação, parece-nos que estamos perante a consumação do crime, na forma continuada, porque todos as condutas típicas que o agente realizou se encontram contidas num espaço temporal curto. Se, ao, invés o agente toma posse do mesmo cartão de crédito e faz um pagamento no mesmo dia, fazendo um outro dois meses depois, então, estaremos, claramente, perante a prática de dois crimes.[18]

Claro que, se com a sua conduta, o agente do crime ultrapassar o limite do valor elevado, então, já estaremos na esfera do crime agravado, ou seja, o crime simples na forma continuada, tem como limite máximo aquele valor.

Como tal, é preciso aferir caso a caso da possibilidade de estarmos perante esta situação.

---

[16] Entre muitos outros, o Ac. TRL de 13-04-2011 (relator Rui Gonçalves), processo n.º 250/06.6PCLRS.L1-3, acessível com texto integral em www.dgsi.pt, expõe com grande assertividade sobre o crime continuado e seus pressupostos.

[17] CORREIA, Eduardo, *in* Direito Criminal, Volume II, Reimpressão, Almedina, 1992, pág. 210, cuja clareza dispensa qualquer outro esclarecimento.

[18] A título de exemplo, no processo com o n.º 274/05.0PATVR (que correu termos na antiga Comarca de Tavira), foi a arguida condenada por este crime na forma continuada.

1.10. A comparticipação

A comparticipação na consumação deste crime rege-se pelas regras gerais previstas no artigo 26.º do Código Penal, porque se trata de um crime comum, podendo ser praticado por qualquer pessoa. Aplicam-se, por isso, os regimes previstos nos artigos 25.º e 28.º do mesmo diploma. Como tal, se um dos comparticipantes decidir desistir da tentativa, a mesma não é punível se o mesmo voluntariamente impedir a consumação ou que se esforce seriamente para que tal não aconteça. Também no caso de a ilicitude ou grau da ilicitude do facto dependerem de certas qualidades ou relações especiais do agente, tal comunica-se aos demais.

1.11. O concurso

Como já expusemos *supra*, para que se verifique o crime que curamos no presente trabalho, é necessário que a utilização do cartão de garantia ou de crédito ocorra por força das suas específicas finalidades, isto é, torna-se necessário aferir se a sua utilização abusiva ocorreu no âmbito das funções para que o mesmo foi emitido.

Assim, relativamente ao concurso, tal situação levanta-se imediatamente, quando está em causa o crime que esteve na génese daquele que aqui tratamos, designadamente, o crime de burla, previsto no artigo 217.º, n.º 1, do Código Penal. O problema é, em muitos dos contextos que ocorrem, estarmos perante factos que estão abrangidos pelos dois tipos criminais. Por conseguinte, e como estamos perante uma incriminação especial em relação ao crime de burla simples, se forem utilizados abusivamente cartões de garantia ou de crédito, é o crime que aqui trabalhamos que é praticado, existindo, assim, um concurso aparente entre ambos.[19] Mas poderão, ainda, suceder outras situações de concurso, quando, por exemplo, é utilizado um cartão de crédito, mas com intenções diferentes daquela a que se destina a específica função do cartão. Aí, o crime em questão não pode ser este, mas sim, o da burla.

Ocorrerá, também, um concurso aparente entre o crime de abuso de cartão de garantia ou de crédito com o crime de infidelidade, previsto no artigo 224.º do Código Penal. É que, nesta situação, há acordo do titular do cartão (uma sociedade, por exemplo) para que um seu funcionário utilize o cartão, logo, tal conduta, em relação ao "nosso" crime é atípica, porque está numa relação de consunção relativamente a ele.

O crime que nos ocupa está numa relação de especialidade com o crime de burla informática, previsto no artigo 221.º do Código Penal. Por vezes, confundem-se estes tipos criminais, porque, assim que se utiliza um qualquer meio informático, parte-se imediatamente para o segundo crime referido. Mas essa situação não deve ser encarada de forma tão linear. Veja-se, a título de exemplo, uma situação em que o agente do crime insere, de forma incompleta, dados informáticos que se encontram no interior da banda

[19] O mesmo pensamento serve relativamente aos tipos criminais agravados dos crimes em causa, designadamente, os previstos nos artigos 218.º e 225.º, n.º 5, ambos do Código Penal.

magnética de um cartão de crédito. Nesta situação, apesar de estarmos perante uma conduta subsumível ao crime de burla informática, designadamente, a prevista no n.º 1 da norma, o facto de se tratar de um cartão de crédito ou garantia, implica que tal conduta seja subsumível ao tipo criminal que analisamos na nossa apresentação.

Já quanto ao crime de falsificação, previsto no artigo 256.º, n.º 1, c), do Código Penal (quando o agente assina os talões das compras), existe um concurso efetivo entre ambos os crimes, porque estamos perante crimes que tutelam bens jurídicos de natureza distinta.

Por sua vez, haverá concurso efetivo entre o crime de furto, previsto no artigo 203.º, n.º 1, do Código Penal, em que o agente se apodera do cartão de crédito e com ele fará uma utilização abusiva posteriormente.[20]

No entanto, em relação ao crime de roubo, o crime de abuso de cartão de garantia ou de crédito mostra-se consumido.[21]

2. O inquérito

2.1. A notícia do crime

A notícia do crime é adquirida nos termos do artigo 241.º do Código de Processo Penal. Neste tipo criminal, a notícia terá, quase sempre, o próprio ofendido que, quando se apercebe de que ocorreu o uso indevido do seu cartão de garantia ou de crédito, denuncia tal situação.

Mas poderá ter origens diferentes. A título de exemplo, veja-se o inquérito n.º 380/09.2JACBR (que correu termos na antiga Comarca de Portimão), cuja notícia do crime sucedeu quando se investigava o desaparecimento do titular do cartão de crédito, cartão esse, que foi utilizado em compras em vários pontos do país, partindo daí toda a investigação que levaria à descoberta do corpo e a acusação por vários crimes. A situação tratada nesse processo, refere-se a um valor elevado, logo, a partir do momento em que o mesmo é atingido, pela sua natureza pública, há que prosseguir com o procedimento criminal.

Importa relembrar, a este propósito, o previsto no artigo 242.º, n.º 1, do Código de Processo Penal. Assim, há uma obrigação legal de denúncia por parte dos Órgãos de Polícia Criminal (a)), bem como, para os funcionários, na aceção do artigo 386.º do Código Penal (b)). E aqui, assume relevância acrescida, o facto de o dever de denúncia por parte de funcionário poder

[20] Como nos explica o Ac. STJ de 04-12-2008 (relator Pires da Graça), processo n.º 08P3552, acessível com texto integral em www.dgsi.pt.
[21] É o que nos elucida o Ac. STJ de 05-11-2008 (relator Henriques Gaspar), processo n.º 08P2817, acessível para leitura em texto integral em www.dgsi.pt, se bem que a situação explanada é relativa ao crime da burla informática prevista no artigo 221.º do Código Penal, mas cuja lógica é perfeitamente aplicável aqui. Esta foi a solução encontrada no processo n.º 380/09.2JACBR (que correu termos em Portimão), em que o Tribunal Colectivo absolveu pelo crime de abuso de cartão de garantia ou de crédito, por entender que o mesmo foi consumido pelo crime de roubo, pelo qual, os agentes foram condenados.

entrar em conflito com o dever de sigilo profissional. Nesse caso, terá de prevalecer o dever de denúncia, já que visa proteger interesses de ordem pública de valor superior.[22]

2.2. Especificidades

Abordaremos, de seguida, a dinâmica do inquérito, isto é, a orientação que entendemos ser a mais adequada na prossecução da investigação quando está em causa este crime.

A competência para a investigação deste ilícito criminal deverá ser delegada nos Órgãos de Polícia Criminal, como consagra o artigo 270.º, n.º 1, do Código de Processo Penal.[23]

Nos inquéritos iniciados aquando da apresentação de uma denúncia relativamente a este crime, importa assegurar *ab initio* a junção de documentação que possa, pelas mais variadas razões, entregar armas à investigação para, dessa forma, ser possível chegar à verdade material.

Torna-se necessário, em primeira mão, que sejam juntos aos autos, tanto o contrato celebrado entre o denunciante e a entidade bancária emitente do cartão[24], bem como, documentos referentes aos extratos bancários referentes aos cartões que foram utilizados de forma abusiva. Esse será, parece-nos, o ponto de partida para se conseguir perceber o fluxo dos movimentos, designadamente, a sua origem, o seu destino e o seu valor. Não há outra forma de o fazer. De referir, ainda, que na documentação referente ao contrato, é preciso que esteja devidamente estipulado o valor limite que poderá ser utilizado pelo titular do cartão[25]. É que, se assim não for, torna-se impossível saber se a utilização foi abusiva.

Na posse de tais documentos, compete perceber a dinâmica que o agente do crime utilizou na prossecução da sua conduta. Normalmente, estes cartões são utilizados para realizar compras, logo, torna-se indispensável perceber qual será a entidade cujos produtos foram adquiridos através da compra realizada com a utilização abusiva do cartão.

Obtida a informação sobre quais foram as lojas onde as compras ocorreram, deverão as mesmas ser visitadas, a fim de se conseguir aferir como a prática do crime se desenrolou. Se tais lojas forem *online*, então, entramos no âmbito dos meios de obtenção de prova previstos na Lei 109/2009, de 15 de Setembro (Lei do Cibercrime), que é aplicável a este tipo de situações, for força do seu artigo 11.º, n.º 1, b). Aplicáveis seriam, assim, os meios de obtenção de prova previstos nos artigos 14.º, 15.º, 16.º e 17.º daquele diploma legal, através dos operadores de comunicações, das empresas tecnológicas, etc..

---

[22] COSTA, Maia, *in* Código de Processo Penal Comentado, Almedina, 2.ª Edição Revista, 2016, pág. 883.
[23] Sobre a delegação de competências, ver a Diretiva da Procuradoria-Geral da República 6/2002, bem como, o artigoº 7.º, n.º 3, l), da Lei 49/2008, de 27 de Agosto (lei da Organização da Investigação Criminal), quando a utilização abusiva ocorre através da utilização de meio informático.
[24] Como nos explica o Ac. TRL de 07-10-2003 (relator Vasques Dinis), processo n.º 9914/2002-5, acessível para leitura integral em www.dgsi.pt.
[25] *Idem* (o aresto trata de uma situação em que, entre outras coisas, não se provou qual o valor limite do *plafond* do cartão).

Note-se que poderá ocorrer uma qualquer utilização abusiva numa caixa ATM, por exemplo. Aqui, e se no extrato bancário não estiver a referência ao local onde tal utilização ocorreu, então, deverá o Ministério Público lançar mão do mecanismo previsto no artigo 79.º, n.º 2, e), do DL 298/92, de 31 de Dezembro (Regime Geral das Instituições de Crédito e Sociedades Financeiras)[26], porque se for possível identificar aquele ATM, partiremos, quase de certeza, para a recolha de imagens do sistema de videovigilância que, por norma, existem nesses locais.

Aqui chegados, a investigação poderá seguir várias direções. Vejamos: É preciso verificar se tais estabelecimentos se encontram abrangidos por um sistema de videovigilância e, na afirmativa, importa salvaguardar as imagens referentes aos períodos temporais em que ocorreram as compras. Não esquecer que é preciso verificar em todas as lojas onde tal ocorreu, porque bastará que, numa delas, o agente do crime tenha sido filmado, para se conseguir um avanço enorme na investigação.[27] Imaginando uma situação em que a utilização abusiva ocorre num posto de combustível e é possível verificar a matrícula da viatura usada pelo agente do crime, tornava-se possível e, até, vantajoso, perceber quem é o proprietário daquela viatura e tentar que a investigação avance por esse caminho.

Adquiridas as imagens, há que proceder à inquirição de testemunhas que tenham presenciado a utilização do cartão, nomeadamente, os funcionários das lojas onde o mesmo foi utilizado. Estamos, aqui, no âmbito da prova testemunhal, prevista nos artigos 128.º e seguintes do Código de Processo Penal.

Torna-se importante, também, proceder à apreensão dos talões de venda originais, porque uma compra com um cartão de garantia ou de crédito, obriga sempre a uma assinatura, lançando mão, assim, do meio de obtenção de prova previsto nos artigos 178.º e seguintes do Código de Processo Penal.

É pertinente, também, aferir dos exatos n.ºs de série, se for possível, dos artigos adquiridos.

Avançando, imagine-se que o estabelecimento comercial onde ocorreu a utilização do cartão não dispõe de sistema de videovigilância. Nesta eventualidade e se, entretanto, se conseguir chegar a um qualquer suspeito, além de se proceder à apreensão dos talões originais, também nos parece ser relevante, que se procedam a diligências de reconhecimento, nos termos dos artigos 147.º e seguintes do Código de Processo Penal, sendo essa uma forma de, eventualmente, se conseguir chegar ao agente do crime.

[26] A jurisprudência tem sido favorável à utilização deste mecanismo e sem haver necessidade de fundamentar a fundo para que tal informação seja disponibilizada. A título de exemplo, veja-se o Ac. TRL de 14-09-2011 (relator Fernando Estrela), processo n.º 1214/10.0PNSNT-A.L1, disponível em: http://www.pgdlisboa.pt/docpgd/files/1214_10.0PBSNT%20segredo%20bancario.pdf, que explana que "*o que a Lei 36/2010, ao dar nova redacção à alínea d), do n.º 2, do artigo 79.º consagrou, foi reconhecer que o interesse da investigação criminal é preponderante face ao direito de reserva da vida privada do titular de uma conta bancária, no que à mesma diz respeito e, por isso, o dever de segredo quanto aos elementos dessa conta cai perante a solicitação, no âmbito de um processo penal, da autoridade judiciária.*"

[27] Nesta situação, o fator tempo é crucial, porque as imagens de videovigilância só ficam guardadas pelo prazo de 30 dias, nos termos do artigo 31.º, n.º 2, da Lei 34/2013, de 16 de Maio.

Após estas diligências probatórias e se for possível chegar, de facto, ao agente do crime, deverão ser realizadas outras diligências, designadamente, revistas, previstas nos artigos 174.º e seguintes do Código de Processo Penal. Quantas vezes, aquando de uma abordagem, se verifica que o agente do crime ainda mantém na sua posse o cartão que utilizou na consumação dos factos ilícitos, os respetivos talões e, até, os bens ilegitimamente adquiridos. É certo que a mera posse não pode, por si só, levar à conclusão de que o possuidor é o autor do crime[28], mas tal posse, além de poder ser um ponto de partida para diligências posteriores, permitirá, quando relacionada com outros meios de prova, alicerçar os indícios que se pretendem alcançar com a investigação.

Chegados à identificação de um suspeito, então, há que avançar, se eventualmente se entender como relevante, para a realização de buscas domiciliárias, já que é perfeitamente possível que os cartões utilizados, bem como os comprovativos de tais utilizações e, ainda, os artigos adquiridos, se encontrem, ainda, no interior das residências dos suspeitos[29]. O seu regime está previsto no artigo 177.º do Código de Processo Penal, como bem se sabe. Claro que, o mesmo raciocínio se fará para as buscas não domiciliárias, previstas nos artigos 174.º, n.º 2 e 176.º, ambos do Código de Processo Penal.

Facilmente se perceberá que, apesar de valer para aqui o mesmo raciocínio referido *supra,* relativamente à detenção dos bens, este será sempre um passo muito importante para que a investigação avance. É que, na posse dos talões, torna-se mais fácil chegar à prova pericial, designadamente, através de exame pericial de documentos e escrita manual. É de referir, a este propósito, que será esta uma forma de se chegar a meios de prova fortes, porque a comparação entre escritas poderá levar a resultados com um grau de certeza bastante acentuado. É que, nos termos do artigo 163.º do Código de Processo Penal, o juízo técnico, científico ou artístico inerente a este tipo de prova, está subtraído à livre apreciação do julgador, a não ser em situações excecionais. Mais, é sabido que "*os arguidos que se recusarem à prestação de autógrafos, para posterior exame e perícia, ordenados pelo Exm.º Magistrado do M.º P.º, em sede de inquérito, incorrem na prática de um crime de desobediência, previsto e punível pelo artigo 348.º, n.º 1 b), do Código Penal, depois de expressamente advertidos, nesse sentido, por aquela autoridade judiciária.*"[30]. Torna-se, assim, num recurso essencial para a investigação. Claro que, na eventualidade da perícia permitir perceber que a assinatura do comprovativo de utilização abusiva do cartão, isto é, associar inequivocamente tal utilização a uma pessoa determinada, também daí advirá prova de um crime de falsificação, previsto no artigo 256.º, n.º 1, c), com referência ao artigo 255.º, a), ambos do Código Penal.

[28] Se bem que tratando de um crime de furto, mas perfeitamente aplicável às situações que aqui curamos, o Ac. TRP de 01-07-2015 (relator Pedro Vaz Pato), processo n.º 425/11.6GFPNF.P2, acessível em www.dgsi.pt, explana que "*A simples detenção dos objetos furtados por parte do arguido, desacompanhada de qualquer outro indício, não permite induzir a forma como as coisas furtadas foram por ele obtidas, nem que ele as obteve nas condições requeridas pelo artigo 203.º do Código Penal.*"

[29] Daí se ter referido *supra*, sobre a importância de recolher informação sobre os números de série dos bens adquiridos.

[30] Acórdão de Fixação de Jurisprudência 14/2014, disponível em www.stj.pt.

De aludir, ainda no âmbito dos meios de obtenção de prova, à utilização de interceções telefónicas, nos termos dos artigos 187.º e seguintes do Código de Processo Penal. Neste campo, por força do requisito previsto no artigo 187.º, n.º 1, a), daquele diploma legal (crimes puníveis com pena de prisão superior, no seu máximo, a três anos), quando estiverem em causa os crimes agravados do ilícito criminal de que cuidamos, seria aplicável este meio de obtenção de prova. No entanto, importa aprofundar um pouco este tema e perceber se, de facto, tal será pertinente. Assim, a utilização de escutas telefónicas, apenas deverá suceder como *ultima ratio*, ou seja, quando, de outra forma, a prova fosse impossível ou muito difícil de obter e quando esta diligência fosse indispensável para a descoberta da verdade. Enfrentamos, por isso, um problema de proporcionalidade que é preciso ter sempre presente quando se procede à realização de uma escuta telefónica.

No caso dos crimes que curamos neste trabalho, justificar-se-ia a utilização deste meio de obtenção de prova? Cremos que não, por duas razões: Primeira, a já referida *ultima ratio*, porque não vislumbramos qualquer situação em que fosse uma escuta telefónica que permitisse desbloquear uma investigação, porque a interceção telefónica só seria realizada contra um suspeito ou intermediário. Ora, se tais sujeitos já estiverem identificados, então, torna-se bem mais fácil lançar mão de outros meios de obtenção de prova. Segunda, cremos que tal se revelaria completamente inútil, porque a experiência diz-nos que, assim que um ofendido se apercebe de que o seu cartão de garantia ou de crédito está a ser utilizado abusivamente, a primeira coisa que fará, será, obviamente, tratar do seu cancelamento. A partir desse momento, o agente do crime deixará de ter possibilidade de o voltar a usar, logo, parece-nos que uma escuta telefónica não acrescentaria absolutamente nada à investigação.

2.3. O final do inquérito

Terminadas as diligências realizadas no âmbito do inquérito, importa apreciar se estão verificados indícios suficientes da prática do crime e de quem foram os seus autores. Assim, nos termos do artigo 283.º, n.º 2, do Código de Processo Penal, consideram-se "*suficientes os indícios sempre que deles resultar uma possibilidade razoável de ao arguido vir a ser aplicada, por força deles, em julgamento, uma pena ou uma medida de segurança.*".

Os indícios são "*sinais, vestígios, referências factuais, etc. que permitem entrever algo, sem revelar directamente, constituindo princípio de prova, ou ainda que sugerem no espírito do julgador a adequação da condição causal, equiparando o valor probatório ao da prova directa. Ora, a suficiência indiciária afere-se em função das provas ("representativas") e indícios ("lógicas"), ou seja, do material probatório coligido no inquérito, permitindo ao MP proferir ou não um despacho de acusação.*"[31]

[31] TEIXEIRA, Carlos Adérito, *in* "Indícios Suficientes": Parâmetro de Racionalidade e "Instância" de Legitimação Concreta do Poder-Dever de Acusar, Revista do CEJ, 2.º semestre de 2004, número 1, pág. 155.

Atingido este ponto, torna-se forçoso analisar os elementos que o inquérito nos oferece e aferir da possibilidade de os mesmos conseguirem sustentar uma certeza de que o agente do crime acabará condenado pela prática dos factos que lhe são imputados.

Se, dessa análise, concluirmos que os indícios não são suficientes, mormente, porque não se conseguiu chegar à identificação do agente do crime ou porque não se conseguiu perceber, com a certeza exigida, de que o agente praticou, de facto, o ilícito, então, o caminho só poderá ser o arquivamento do inquérito, nos termos do artigo 277.º, n.º 2, do Código de Processo Penal.

Ao invés, se o inquérito nos fornecer matéria suscetível de convencimento por parte do julgador da prática do ilícito criminal, então, abrem-se portas a várias possibilidades por parte do Ministério Público.

2.4. As soluções de consenso[32]

2.4.1. A suspensão provisória do processo

A suspensão provisória do processo é uma solução de consenso. Avulta, aqui, a importância dos instrumentos hierárquicos que vinculam o Ministério Público e que obrigam a seguir determinado caminho. Neste âmbito, destaca-se a Diretiva da Procuradoria-Geral da República 1/2014, que versa sobre a aplicação deste instituto. Assim, o seu Capítulo I, explana as situações que, no seguimento do consagrado no artigo 281.º, n.º 1, do Código de Processo Penal, são propensas a ser-lhes aplicado este regime.

É sabido que a aplicação da suspensão provisória do processo é permitida se estiverem em causa crimes com uma pena de prisão máxima abstratamente aplicável de cinco anos. Como tal, e olhando para o crime em apreço no presente estudo, o Ministério Público, se considerar que se verificam indícios suficientes da prática do mesmo e se estiverem reunidos os pressupostos previstos no referido preceito, deverá seguir a via da aplicação deste instituto, quando se deparar com um crime na sua forma simples ou, então, a prevista no artigo 225.º, n.º 5, a), do Código Penal, ou seja, a conduta sujeita a uma agravação menor, já que se fixa num valor elevado, cuja pena máxima de prisão abstratamente aplicável é de cinco anos. Está abrangida a prática do crime continuado.

A aplicação deste regime poderá processar-se, ainda, quando estiver em causa um concurso de crimes, cujas penas somadas ultrapassem os cinco anos de prisão, mas cujas penas

[32] ALBUQUERQUE, José P. Ribeiro, *in* workshop Évora 3/7/2008 – A Gestão do Inquérito. Instrumentos de Consenso e Celeridade, disponível para leitura integral em: http://www.pgdlisboa.pt/novidades/files/gestao_inquerito_albuquerque.pdf, explica-nos que "no *processo de ponderação há um juízo prévio – claramente de concreta oportunidade – sobre os mecanismos alternativos de diversão, oportunidade e consenso possíveis, i.e. um juízo de adequação de um ou de outro, cabendo ao magistrado do MºPº uma avaliação prática que identifique as características do crime e as características do arguido para poder reconhecer a possibilidade efectiva da solução consensual ou consentida e que está subjacente à forma de processo sumaríssimo e mesmo à suspensão provisória*."

parcelares não ultrapassem esse limite. Como tal, imaginando que estamos perante dois crimes de abuso de cartão de garantia ou de crédito, na sua forma simples ou na forma menos agravada, em concurso efetivo entre si, está viabilizada a aplicação deste instituto.

A este fito, e idealizando um caso em que haja uma pluralidade de arguidos e um deles esteja em condições de ver ser-lhe aplicado este regime (na hipótese de ele próprio o requerer, por exemplo), "*o procedimento criminal pode ser suspenso relativamente a um dos arguidos e prosseguir relativamente a outros, sejam eles co-arguidos dos mesmos crimes ou não. Verificando-se os pressupostos de aplicação do instituto relativamente a um dos arguidos, deve determinar-se a separação de processos e a extracção de certidão do processado relativamente ao arguido que beneficia da suspensão.*"[33]

2.4.2. A mediação penal

O instituto da mediação penal encontra-se previsto na Lei 21/2007, de 12 de Junho e veio alargar as possibilidades que existem relativamente às soluções de diversão aplicáveis à criminalidade menos grave, permitindo aproximar os cidadãos da realização da justiça.[34]

No entanto, este regime provoca algumas perplexidades, já que o artigo 2.º, n.º 3, daquele diploma legal, explana que "*Independentemente da natureza do crime, a mediação em processo penal não pode ter lugar nos seguintes casos:*

a) O tipo legal de crime preveja pena de prisão superior a 5 anos;
b) Se trate de processo por crime contra a liberdade ou autodeterminação sexual;
c) Se trate de processo por crime de peculato, corrupção ou tráfico de influência;
d) O ofendido seja menor de 16 anos;
e) Seja aplicável processo sumário ou sumaríssimo.".

Ora, releva aqui, principalmente, a proibição da aplicação quando ao caso for aplicável o processo sumaríssimo. Como descrito *infra*, o processo sumaríssimo é aplicável a crimes cuja pena de prisão máxima abstratamente aplicável seja inferior a cinco anos. A mediação penal, por sua vez, também só poderá ser aplicada quando, além de outras situações, estejam em causa crimes puníveis com pena de prisão máxima abstratamente aplicável inferior a cinco anos e desde que não seja aplicável o processo sumaríssimo. Então, com regras de tal forma restritivas, onde poderemos encaixar a aplicação deste instituto? Concordamos que "*se arguido e ofendido, em crime que admite a mediação penal, a requererem antes do encerramento do inquérito, não vemos como pode o Ministério Público opor-se a esta pretensão por entender que ao caso poderá ser aplicável o processo sumaríssimo.*"[35] Se assim não se pensar, estamos a ir contra o espírito do legislador.

[33] ALBUQUERQUE, Paulo Pinto, *in* Comentário do Código de Processo Penal à Luz da Constituição da República e da Convenção Europeia dos Direitos do Homem, UCP, 2011, pág. 760.
[34] A possibilidade de recorrer à mediação penal existe apenas em determinados locais, como explana o Artº. 2.º da Portaria n.º 68-C/2008, de 22 de Janeiro.
[35] Ideia expressada por CARMO, Rui, *in* Um Exercício de Leitura do Regime Jurídico da Mediação Penal, acessível em https://pt.scribd.com/document/47613009/Mediacao-Penal.

Nestes moldes e assumindo frontalmente que é passível de ser aplicada a mediação penal ao crime sobre o qual nos debruçamos, entendemos que deve o Ministério Público rodear-se de algumas cautelas e transmitir ao mediador designado todas as informações relevantes para o bom desempenho das suas funções.[36] *Havendo uma pluralidade de arguidos e sendo proposta a mediação, cada um deles pode aceitar ou não, sem que esteja de algum modo dependente dos restantes, prosseguindo a mediação apenas quanto àquele(s) que se mostraram disponíveis*.[37] Nesta situação, quanto aos demais arguidos, o processo seguirá uma qualquer forma que lhes seja aplicável.

Este regime poderá, por isso, ser aplicado quando estiveram em causa os crimes de abuso de cartão de garantia ou de crédito simples ou o menos agravado, porque só assim se respeitará o limite de pena de prisão máxima abstratamente aplicável de cinco anos.

2.5. Os processos especiais

2.5.1. O processo sumário

O processo sumário vem previsto nos artigos 381.º e seguintes do Código de Processo Penal, sendo aplicável aos crimes em que o agente do crime tenha sido detido em flagrante delito e cuja pena máxima abstratamente aplicável não seja superior a cinco anos (n.º 1) ou quando, apesar de tal limite ser ultrapassado ou quando haja concurso de infracções, o Ministério Público entender que não deve ser aplicada de prisão superior àquele limite (n.º 2).

Poderemos indagar-nos se é passível de ser aplicado ao crime que aqui tratamos. Cremos que sim. A título de exemplo, imaginemos uma situação num estabelecimento comercial, em que o próprio titular do cartão, que já suspeitava quem era o agente do crime, observa-o a utilizar o seu cartão de crédito sem autorização, ou seja, de forma abusiva. Nessa altura, retém-no e entrega-o, momentos depois, a um Órgão de Polícia Criminal, que acaba por detê-lo, nos termos do artigo 255.º, n.ºs 1, b), e 2, do Código de Processo Penal. Ora, esta situação, tem a potencialidade de permitir que se faça um julgamento em processo sumário, até porque, tudo o que é necessário, nomeadamente, a denúncia, a solicitação do extrato bancário e outra documentação que, eventualmente, seja relevante, podem ser perfeitamente conseguidos no prazo dos 20 dias após a detenção, tudo nos termos do artigo 382.º, n.ºs 4 e 5, do Código de Processo Penal, permitindo perfeitamente ao Ministério Público a realização de um "para-inquérito".[38]

Claro que, apesar de conseguirmos imaginar situações como a que referimos e outras, mais ou menos rebuscadas, admitimos que a aplicação deste regime seria, apenas, residual.

[36] ALMEIDA, Carlota Pizarro, *in* Diferentes versões do consenso: Suspensão provisória do processo e mediação penal, Revista do CEJ, 2º semestre 2011, número 16, pág. 107.
[37] *Idem*, pág. 105.
[38] Expressão utilizada por ALBUQUERQUE, Paulo Pinto, *in op. cit.*, pág. 992.

Pelo exposto, esta forma de processo é aplicável quando estivermos perante o tipo criminal simples ou o menos agravado, bem como, o mais agravado, por força da possibilidade da sua aplicação quando se entenda que não é de haver condenação em pena superior aos cinco anos de prisão.

2.5.2. O processo abreviado

Quanto ao processo abreviado, cremos que a sua aplicação ao crime em apreço, também não levanta grandes problemas, porque o legislador previu a aplicação deste instituto a uma panóplia bem maior de crimes, já que, apesar do artigo 391.º-A, n.º 1, do Código de Processo Penal prever a sua aplicação a crimes cuja pena máxima abstratamente aplicável for de cinco anos, o seu n.º 2, abre o leque de possibilidades e permite que o Ministério Público, se entender que ao crime em concreto, apesar de punível com pena máxima superior a cinco anos, não seja de lhe aplicar tal pena, acuse em processo abreviado. É aplicável, por isso, às situações em que nos deparamos com um concurso de crimes.

Trata-se, assim, de uma possibilidade forte de que o Ministério Público pode e deve lançar mão, porque, pelo que foi agora referido, abrange todos os tipos criminais do crime que aqui tratamos. Ou seja, apesar do tipo criminal mais grave ser punível com pena de prisão máxima de oito anos, o legislador abriu aqui a porta à aplicação deste processo especial, quando for de prever que o arguido não será condenado a pena superior a cinco anos de prisão. A este propósito, é preciso não esquecer que o Ministério Público deverá, na sua acusação, explicar as razões por que entende não ser de aplicar pena superior a cinco anos de prisão.

Mais, o facto de o legislador ter previsto prazo máximo de 90 (noventa) dias para deduzir a acusação, depois do conhecimento do crime ou de denúncia, nos termos do artigo 391.º-B, n.º 2, do Código de Processo Penal, dá tempo para carrear para o inquérito meios de prova essenciais. Apesar de tal prazo ser apertado, acaba por ser suficiente para aprofundar a investigação. Não esquecer o que nos indica o artigo 391.º-A, n.º 3, do Código de Processo Penal, quando fala do conceito de provas simples e evidentes, as quais, pela exposição feita aquando da explicação das diligências adequadas à investigação deste tipo criminal, nos parece ser aqui o caso, porque, numa investigação, é possível aceder a um contrato bancário para a utilização dos cartões de garantia ou de crédito e dos respectivos extratos, bem como, inquirir algumas testemunhas no período temporal de 90 (noventa) dias, sendo tal período perfeitamente suficiente para terminar um inquérito relativo ao crime sobre o qual nos debruçamos.

Parece-nos, por isso, que deverá o Ministério Público ter presente que a aplicação deste processo especial permite uma maior celeridade na aplicação da justiça, devendo orientar a sua investigação nesse sentido. Diríamos, até, que o crime que aqui tratamos será terreno fértil para a aplicação deste processo especial.

2.5.3. O processo sumaríssimo

Não sendo possível a aplicação de uma suspensão provisória do processo, deverá avançar-se para a aplicação do processo sumaríssimo, na senda daquilo que vem sendo o desejo do legislador quando alargou o seu âmbito de aplicação.[39]

O processo sumaríssimo é outra solução de diversão. Mais uma vez, os instrumentos hierárquicos próprios do Ministério Público têm aqui um lugar de aplicação privilegiado. Neste caso, releva a Diretiva da Procuradoria-Geral da República 1/2016.

Assim, este instituto é aplicável quando aos crimes praticados corresponda pena de prisão máxima não superior a cinco anos ou pena de multa, como explana o artigo 392.º, n.º 1, do Código de Processo Penal. Assim, o "nosso" tipo criminal simples e o menos agravado estão abrangidos pelo âmbito da sua aplicação, já que a pena máxima de prisão abstratamente aplicável a estes crimes não é superior a cinco anos. O concurso de crimes já não é passível de tal aplicação, pelos motivos aduzidos.

O processo sumaríssimo tem regras um pouco mais apertadas que as da suspensão provisória do processo, senão vejamos: enquanto esta é aplicável quando existe um concurso de crimes, cuja soma das penas seja superior a cinco anos, desde que as penas parcelares não o sejam, no caso daquele, os cinco anos de prisão são o limite máximo, ou seja, poderá haver um concurso de crimes, mas a pena máxima de prisão aplicável a esses crimes nunca poderá ser superior a esse limite imperativo dos cinco anos. Nesse seguimento, também não será aplicável nos casos em que o Ministério Público entenda que não deva, ao caso concreto, ser aplicada pena superior aos referidos cinco anos de prisão.

2.6. A acusação em processo comum

Findo o inquérito e verificados indícios suficientes da prática do crime de abuso de cartão de garantia ou de crédito, e não sendo possível a aplicação dos institutos descritos *supra*, então, há que avançar para uma acusação em processo comum, nos termos do artigo 283.º, n.º 1, do Código de Processo Penal.

Neste âmbito, é importante distinguir as várias possibilidades que existem. Assim, se estivermos perante um crime na sua forma simples ou na sua forma menos agravada, a acusação é para julgamento por Tribunal Singular. Se estivermos perante um crime na sua vertente mais grave, então, a acusação terá de ser para julgamento por Tribunal Coletivo. Claro que, haverá sempre a possibilidade de aplicar o artigo 16.º, n.º 3, do Código de Processo Penal, quando estamos perante o crime na sua forma mais grave ou quando estamos perante um concurso de crimes que, no somatório das penas aplicáveis, ultrapasse o limite de cinco anos previsto para o julgamento por Tribunal Singular.

[39] Operado pela Lei 48/2007, de 29 de Agosto que alterou o limite da pena de prisão abstratamente aplicável de três para cinco anos.

IV. Referências bibliográficas

Referências bibliográficas

ALBUQUERQUE, José P. Ribeiro, *workshop* Évora 3/7/2008 – A Gestão do Inquérito. Instrumentos de Consenso e Celeridade, disponível para leitura integral em http://www.pgdlisboa.pt/novidades/files/gestao_inquerito_albuquerque.pdf.

ALBUQUERQUE, Paulo Pinto, Comentário do Código Penal, à Luz da Constituição da República e da Convenção Europeia dos Direitos do Homem, UCP, 2008.

ALBUQUERQUE, Paulo Pinto, Comentário do Código de Processo Penal, à Luz da Constituição da República e da Convenção Europeia dos Direitos do Homem, UCP, 2011.

ALMEIDA, Carlota Pizarro, Diferentes versões do consenso: Suspensão provisória do processo e mediação penal, Revista do CEJ, 2º semestre 2011, número 16.

BARREIROS, José António, Crimes Contra o Património no Código Penal de 1995, CEJ, 1996.

CARMO, Rui, Um Exercício de Leitura do Regime Jurídico da Mediação Penal, acessível em https://pt.scribd.com/document/47613009/Mediacao-Penal.

Código Penal, Actas e Projecto da Comissão de Revisão, Rei dos Livros, Acta n.º 39, de 9 de Julho de 1990.

CORREIA, Eduardo, Direito Criminal, Volume II, Reimpressão, Almedina, 1992.

COSTA, Maia, Código de Processo Penal Comentado, Almedina, 2ª.Edição Revista, 2016.

CUNHA, J. M. Damião, Comentário Conimbricense do Código Penal, Parte Especial, Tomo II, Coimbra Editora, 1999.

DANTAS, António Leones, A Revisão do Código Penal e os Crimes Patrimoniais, Jornadas de Direito Criminal, Revisão do Código Penal, CEJ, Volume II.

GARCIA, M. Miguez e RIO, Castela, Código Penal, Parte Geral e Especial, Almedina, 2015, 2ª.edição.

ROCHA, Miguel António Lopes, A revisão do Código Penal, Soluções de Neocriminalização, Jornadas de Direito Criminal, Revisão do Código Penal, CEJ, Volume I.

SÁ PEREIRA, Victor e LAFAYETTE, Alexandre, Código Penal Anotado e Comentado, QUIDJURIS, 2008.

TEIXEIRA, Carlos Adérito, "Indícios Suficientes": Parâmetro de Racionalidade e "Instância" de Legitimação Concreta do Poder-Dever de Acusar, Revista do CEJ, 2º semestre de 2004, número 1.

8.
Crime de abuso de cartão de garantia ou de crédito. Enquadramento jurídico, prática e gestão processual

Rui Miguel Lima Alves

CENTRO
DE ESTUDOS
JUDICIÁRIOS

8. CRIME DE ABUSO DE CARTÃO DE GARANTIA OU DE CRÉDITO. ENQUADRAMENTO JURÍDICO, PRÁTICA E GESTÃO PROCESSUAL

Rui Miguel Lima Alves

I. Introdução

O presente trabalho versa sobre o crime de abuso de cartão de garantia ou de crédito, previsto e punido pelo artigo 225.º, do Código Penal, com particular enfoque no enquadramento jurídico do mesmo, abordando-se a sua consagração legal, o bem jurídico protegido, os elementos objectivos e subjectivos do tipo, as formas especiais do crime (tentativa, concurso, comparticipação), as causas de justificação, a moldura penal e a natureza do crime. Posteriormente são expostos alguns problemas relacionados com a prática e a gestão processual do inquérito, nomeadamente quanto à aquisição da notícia do crime, à investigação, às medidas cautelares e de polícia, à recolha da prova e do encerramento do inquérito, abordando-se, ainda, a possibilidade de aplicação dos institutos de celeridade, simplificação, oportunidade e de consenso no processo penal.

Procura-se, assim, efectuar uma análise sistemática que permita uma compreensão do ilícito em causa.

II. Objectivos

Realizado no âmbito do 2.º Ciclo de Formação, do 32.º Curso de Formação de Magistrados para os tribunais judiciais (Ministério Público), o presente estudo visa abordar no plano jurídico-penal o crime de abuso de cartão de garantia ou de crédito, bem como reflectir sobre questões conexas, com um carácter tendencialmente prático. Tem como primeiros destinatários os colegas Auditores de Justiça, mas também os Magistrados do Ministério Público, Magistrados Judiciais, Juristas e Órgãos de Polícia Criminal, de forma a propiciar o debate e uma reflexão sobre o crime em análise, desde a sua criação até actualmente, buscando-se soluções para se lidar com este ilícito no quotidiano judiciário.

III. Resumo

Analisou-se, no presente estudo, o crime de abuso de cartão de garantia e de crédito, previsto e punido pelo artigo 225.º, do Código Penal. Dividiu-se o mesmo em dois capítulos, sendo o Capítulo I designado por "O Abuso de Cartão de Garantia de Crédito – Enquadramento Jurídico", no qual se aborda o enquadramento jurídico, referindo a origem da norma, o bem jurídico protegido, os tipos objectivo e subjectivo, causas de exclusão da culpa e da ilicitude, as formas especiais do crime, a pena e a natureza do crime, enquanto que no Capítulo II se analisa a Prática e Gestão Processual, no que diz respeito à fase de inquérito, à aquisição da notícia do crime, à investigação e recolha de prova, à aplicação de instrumentos de celeridade, simplificação, oportunidade, consenso ou de mera concordância no processo penal, ao arquivamento e à acusação.

CAPÍTULO I – O abuso de cartão de garantia ou de crédito – Enquadramento jurídico

1. Disposições Introdutórias. Definições

1.1. Instituição de Crédito

A Instituição de crédito é uma empresa cuja actividade consiste em receber do público depósitos ou outros fundos reembolsáveis e em conceder crédito por conta própria (artigo 2.º-A, alínea w), do Decreto-Lei n.º 298/92, de 31/12 - Regime Geral das Instituições de Crédito e Sociedades Financeiras)[1].

Segundo o artigo 3.º, do referido diploma legal, são instituições de crédito:

a) Os bancos[2];
b) As caixas económicas;
c) A Caixa Central de Crédito Agrícola Mútuo e as caixas de crédito agrícola mútuo;
d) As instituições financeiras de crédito;
e) As instituições de crédito hipotecário;
k) Outras empresas que, correspondendo à definição do artigo 2.º, como tal sejam qualificadas pela lei.

1.2. Conta Bancária

A conta bancária é um produto de depósito existente nas instituições financeiras credenciadas pelo Banco de Portugal, através do qual o banco guarda o dinheiro do cliente, mediante o pagamento de contrapartidas por este. A abertura de conta é um contrato celebrado entre o banqueiro e o seu cliente, pelo qual ambos assumem deveres recíprocos relativos a diversas práticas bancárias (depósitos, levantamentos, transferências).

1.3. Cartão de Garantia

Inicialmente, no âmbito da Comissão de Revisão do Código Penal de 1995, designava-se "Cartão de Cheques", tendo sido alterada a designação para "Cartão de Garantia"[3].

O cartão de garantia funciona em associação com os cheques, mediante o qual o emitente cauciona a utilização dos cheques pelo titular, seu subscritor, funcionando o mesmo como

[1] Cfr. SANTOS, António Carlos dos, GONÇALVES, Maria Eduarda, MARQUES, Maria Manuel Leitão, Direito Económico, 7.ª edição, Almedina, 2014, págs. 442-443.
[2] Entre outros, por força do disposto no artigo 4.º, alíneas a) a c), do Decreto-Lei n.º 298/92, de 31/12 (Regime Geral das Instituições de Crédito e Sociedades Financeiras), os bancos podem efectuar as operações seguintes: *"a) Receção de depósitos ou outros fundos reembolsáveis; b) Operações de crédito, incluindo concessão de garantias e outros compromissos, locação financeira e factoring; c) Serviços de pagamento, tal como definidos no artigo 4.º do regime jurídico dos serviços de pagamento e da moeda electrónica […]*".
[3] Cfr. Código Penal, Actas e Projecto da Comissão de Revisão, Rei dos Livros, 1993, págs. 450-451.

garantia de pagamento do cheque até determinado montante. Não é um meio de pagamento autónomo.

O cartão de garantia assemelha-se ao cartão de crédito, na medida em que, como constitui uma garantia de pagamento, concede ao seu titular um crédito[4], e, assim, facilita a aceitação do cheque como meio de pagamento, pois o banco garante, até determinado montante, que o cheque será pago, independentemente da condição da conta bancária a que se encontre associado (tenha ou não provisão)[5].

1.4. Cartão de Crédito

O cartão de crédito[6] é qualquer instrumento de pagamento, para uso electrónico ou não, emitido por uma instituição de crédito ou por uma sociedade financeira que possibilite ao seu titular a utilização de crédito outorgado pela emitente, em especial para a aquisição de bens ou de serviços[7].

Este tipo de cartão possibilita ao seu titular "*adquirir bens e serviços cujo pagamento é assegurado pela actuação intermediadora do emissor que se lhe substitui junto do comerciante, e cujo reembolso pelo titular é diferido, podendo eventualmente ser escalonado em prestações mensais mediante o pagamento de juros*."[8], sem necessidade de utilização de outro meio de pagamento, bem como a proceder a levantamentos até determinado montante, com referência a uma conta bancária aberta em nome do titular[9].

Assenta numa relação triangular que é composta pela entidade emitente, pelo titular do cartão de crédito e pelos comerciantes associados ao sistema/rede[10]. Face a esta relação, no momento da compra de bens ou serviços o utilizador do cartão aceita pagar ao emitente do mesmo o montante que despendeu, de forma diferida, nos moldes supra mencionados; enquanto que o vendedor verifica se o cartão é válido e se dispõe de crédito para pagar o preço, sendo posteriormente remetidas para o titular o documento que contém a listagem das compras efectuadas, o qual terá de pagar pontualmente as prestações, que incluem juros e despesas.

[4] Cfr. VASCONCELOS, Joana de, *in* Revista de Direito e de Estudos Sociais, Coimbra, Outubro-Dezembro 1992, págs. 346-347.
[5] Cfr. VASCONCELOS, Joana de, ob. cit., págs. 347-348.
[6] O cartão de crédito teve origem no "*Diner´s Club*", local onde membros restritos do clube podiam utilizar um cartão a crédito de forma a usufruírem de refeições em alguns restaurantes aderentes de Nova Iorque. Posteriormente surgiram os cartões de crédito *American Express*, *Carte Blanche* e o *VISA* (assim CORDEIRO, António Menezes, Manual de Direito Bancário, 3.ª Edição, Coimbra, Almedina, 2006, pág. 512).
[7] Cfr. Aviso do Banco de Portugal, n.º 11/2001, que define cartões de crédito e de débito e respectivas condições de utilização, pág. 1, disponível em https://www.bportugal.pt/sites/default/files/anexos/cartas-circulares/11-2001a.pdf.
[8] Cfr. VASCONCELOS, Joana de, ob. cit., pág. 329.
[9] Cfr. PEREIRA, Sá, e LAFAYETTE, Alexandre, "Código Penal Anotado e Comentado", Legislação Conexa e Complementar, Quid Juris, Sociedade Editora, 2014, pág. 647.
[10] Cfr. VASCONCELOS, Joana de, ob. cit., págs. 313-314.

Em caso de incumprimento de pagamento, o banco pode declarar o crédito incobrável, inserindo o titular do cartão na "Central de Responsabilidades de Crédito"[11].

1.5. Cartão de Débito

O cartão de débito constitui um instrumento de pagamento, para uso electrónico, que possibilita ao seu titular a utilização instantânea do saldo de uma conta de depósito associada, junto da instituição de crédito que emite o cartão, nomeadamente para efeitos de levantamento de numerário, aquisição de bens ou serviços e pagamentos, quer através de máquinas automáticas quer em estabelecimentos comerciais, pelo que a sua utilização depende do saldo existente na conta bancária do titular[12].

1.6. Cartão de Moeda Electrónica

O cartão de moeda electrónica permite que o seu titular o carregue com determinada quantia monetária, que fica associada ao mesmo, e pode ser utilizado no pagamento imediato de bens ou serviços, representado por um crédito sobre o emitente e emitido após recepção de notas de banco, moedas e moeda escritural, para efectuar operações de pagamento (depositar, transferir ou levantar fundos)[13]. Quando utilizado origina reduções no valor pré-pago ou no saldo disponível[14].

2. Enquadramento Jurídico

2.1. A Consagração Legal do crime de abuso de cartão de garantia ou de crédito

O tipo de crime em análise foi introduzido no ordenamento jurídico português com a revisão do Código Penal de 1995, através do Decreto-Lei n.º 48/95, de 15/03. A criação deste novo preceito deveu-se ao facto de se pretender colmatar lacunas, na medida em que existiam situações que não eram enquadráveis no crime de burla (artigo 217.º, do Código Penal) ou no crime de infidelidade (artigo 224.º, do Código Penal) ou no crime de burla informática (artigo 221.º, do Código Penal), conforme se expõe adiante.

[11] A Central de Responsabilidades de Crédito (CRC), usualmente conhecida como "lista negra", contém informação sobre as responsabilidades de crédito efectivas assumidas por qualquer pessoa singular ou colectiva perante as entidades participantes, bem como as responsabilidades de crédito potenciais que representem compromissos irrevogáveis. A CRC encontra-se regulamentada pelo Decreto-Lei n.º 204/2008, de 14/10, e pela Instrução do Banco de Portugal n.º 21/2008. A CRC dispõe da Autorização n.º 4241/2011, de 27/04, concedida pela Comissão Nacional de Protecção de Dados, nos termos da Lei n.º 67/98, de 26/10: https://www.bportugal.pt/perguntas-frequentes/276.

[12] Cfr. Aviso do Banco de Portugal, n.º 11/2001, pág. 1.

[13] Cfr. Artigo 2.º, alínea g), do Regime Jurídico dos Serviços de Pagamento e da Moeda Electrónica, anexo ao Decreto-Lei n.º 317/2009, de 30/10, actualizado pelo Decreto-Lei n.º 157/2014, de 24/10.

[14] Cfr. Cadernos do Banco de Portugal, n.º 6, Cartões Bancários, pág. 5, disponível em https://www.bportugal.pt/sites/default/files/anexos/cartas-circulares/11-2001a.pdf.

Refere-se no preâmbulo no Decreto-Lei n.º 48/95, de 15/03: "[…] *cumpre assinalar um conjunto significativo, se bem que limitado, de propostas de neocriminalização, resultante quer da revelação de novos bens jurídico-penais ou de novas modalidades de agressão ou perigo, quer de compromissos internacionais assumidos ou em vias de o serem por Portugal. Como exemplos de neocriminalização destacamos: […] a burla informática (artigo 221.º), o abuso de cartão de garantia ou de crédito (artigo 225.º)* […]". Procurou-se, assim, articular o Direito com a "*evolução económica para a desmaterialização da riqueza e corresponder às novas formas de tutela, que ditam exigências especiais*."[15], de forma a se proteger o património face aos novos e cada vez mais utilizados meios de pagamento.

Inspirada no § 266b, do Código Penal alemão (Missbrauch von Scheck- und Kreditkarten), introduzida em 1986, a previsão legal do Código Penal português é mais abrangente, já que, para além das condutas de abuso praticadas pelos titulares do cartão, previstas naquele ordenamento jurídico, inclui a responsabilização criminal de terceiros que usem um cartão de garantia ou de crédito de outrem, prevendo-se agravações em função do valor.

Contudo, a criação desta norma não foi pacífica. Na Comissão de Revisão do Código Penal foi proposta a adopção de um novo artigo (219.º-A), referente ao abuso de cartões de cheques e de crédito, uma vez que não existia um enquadramento penal para as situações relacionadas com a utilização não autorizada de cartões de crédito.

Inicialmente surgiram dúvidas quanto à dignidade penal da conduta, uma vez que se entendia que o que estava em causa era a violação de disposições contratuais inerentes à emissão do cartão, o que poderia resultar na "*responsabilização penal por obrigações civis*."[16], e que tal ilícito diz respeito a uma situação em que o portador do cartão vai para além da autorização de crédito concedido pela instituição de crédito, logo matéria do foro privado e que não deveria ser criminalizada[17].

Levantaram-se, ainda, dificuldades quanto ao enquadramento penal a dar ao tipo de condutas previstas na nova norma, nomeadamente quanto à possibilidade de as subsumir ao crime de burla (artigo 217.º, do Código Penal), ou ao crime de infidelidade (artigo 224.º, do Código Penal).

Quanto ao crime de burla, a subsunção dos factos relativos ao agente que utilizasse o cartão de crédito ou de garantia, sabendo da impossibilidade de pagamento, originaria problemas de verificação do tipo de crime, em virtude do não preenchimento do erro ou da astúcia que levam ao prejuízo patrimonial.

[15] Cfr. BELEZA, Teresa Pizarro, e PINTO, Frederico Lacerda da Costa, *in* "*A tutela penal do património após a revisão do código penal de 1995*", Lisboa, Associação Académica da Faculdade de Direito de Lisboa, 1998, págs. 12-13.
[16] Cfr. CUNHA, J. M. Damião da, Comentário Conimbricense do Código Penal, Tomo II, Coimbra, Coimbra Editora, 1999, pág. 374.
[17] Cfr. Código Penal, Actas e Projecto da Comissão de Revisão, Rei dos Livros, 1993, pág. 520; CUNHA, J. M. Damião da, ob. cit., pág. 374. Neste sentido, manifestou-se o Exmo. Sr. Procurador-Geral da República, José Narciso da Cunha Rodrigues, enquanto membro da comissão de revisão do Código Penal e do Código do Processo Penal

Seria, ainda, difícil subsumir tais factos ao crime de infidelidade, na medida em que o titular do cartão poderia agir no seu próprio interesse e não de acordo com o interesse da entidade que o emite, o que seria susceptível de não causar, intencionalmente, e com grave violação dos deveres que lhe incumbiam, prejuízo patrimonial importante[18].

Pretendeu-se salvaguardar, com a nova incriminação, o correcto uso dos cartões de garantia e de crédito, bem como reprimir e punir os abusos que a massificação do seu uso podem gerar[19].

Face à semelhança com o crime de burla foi adoptado um regime punitivo idêntico para o crime de abuso de cartão de garantia ou de crédito, mormente no que diz respeito às agravações em função do valor[20]. A norma, constante do artigo 225.º, do Código Penal, prevê que:

"1 - Quem, abusando da possibilidade, conferida pela posse de cartão de garantia ou de crédito, de levar o emitente a fazer um pagamento, causar prejuízo a este ou a terceiro é punido com pena de prisão até 3 anos ou com pena de multa.

2 - A tentativa é punível.

3 - O procedimento criminal depende de queixa.

4 - É correspondentemente aplicável o disposto nos artigos 206.º e 207.º

5 - Se o prejuízo for:

a) De valor elevado, o agente é punido com pena de prisão até 5 anos ou com pena de multa até 600 dias;

b) De valor consideravelmente elevado, o agente é punido com pena de prisão de 2 a 8 anos.

6 - No caso previsto no número anterior é correspondentemente aplicável o disposto no artigo 206.º".

3. O Bem Jurídico Protegido

O bem jurídico protegido no crime de abuso de cartão de garantia ou de crédito, desde logo, em virtude da sua inclusão no Capítulo III ("*Dos Crimes contra o Património em geral*"), é o património[21].

Neste tipo de crime pode ser prejudicado o emitente, isto é, aquele que se encontra contratualmente ligado ao titular do cartão e foi levado a efectuar um pagamento, bem como

[18] Cfr. CUNHA, J. M. Damião da, ob. cit., pág. 374; ALBUQUERQUE, Paulo Pinto de, Comentário do Código Penal à luz da Constituição da República e da Convenção Europeia dos Direito do Homem, 3.ª ed. actualizada, Lisboa, Universidade Católica Editora, 2015, pág. 872.
[19] Cfr. ALBUQUERQUE, Paulo Pinto de, ob. cit., pág. 872.
[20] Cfr. Assim Costa Andrade, Figueiredo Dias, Actas, ob. cit., pág. 451.
[21] Assim *vide* CUNHA, J. M. Damião da, ob. cit., pág. 375; ALBUQUERQUE, Paulo Pinto de, ob. cit. pág. 872.

o próprio titular, alvo de abuso de outrem, não titular do cartão, que ilegitimamente ou abusivamente o utilizou[22].
Pode ser, ainda, prejudicado o comerciante, igualmente ligado ao emitente por força de um contrato, perante o agente, o abusador, titular ou não do cartão, que o utilizou, na medida em que pode ser responsabilizado pelo prejuízo sofrido. Em relação ao emitente, comerciante e titular pode suceder que, em concreto, apenas um seja prejudicado, ou, ainda, que dois ou mais o sejam, dependendo se existe ou não prejuízo patrimonial e quem o sofreu[23].
Contudo, no seio da Comissão Revisora do Código Penal referiu-se que é o "*património da entidade emissora do cartão*" o "*bem jurídico protegido*", atendendo-se à "*forma como se consubstancia a infracção (abuso da garantia da entidade emissora)*". M. Miguez Garcia, e J. M. Castela Rio defendem que o "*bem jurídico protegido é o património de bancos e instituições de crédito emitentes do cartão de garantia ou de crédito atingidos pelo facto*"[24].

Porém, somos da opinião de que não se pode assim considerar, na medida em que o sujeito passivo é aquele que, efectivamente, sofre o prejuízo. O que equivale a dizer que só tem sentido considerar como único sujeito passivo o emitente do cartão, se apenas o agente do crime fosse sempre o titular do cartão, o que não acontece[25].

O emitente do cartão efectua um pagamento, do qual decorre uma diminuição patrimonial, para o próprio ou para terceiro (o titular do cartão ou o comerciante), sendo todos estes os sujeitos passivos por serem prejudicados patrimonialmente com a utilização abusiva do cartão[26].

Concomitantemente, este crime visa proteger a confiança do crédito em geral, bem como do tráfego jurídico dos cartões de crédito e de garantia, em especial[27].

4. O Tipo Objectivo de Ilícito

Para se mostrar preenchido o ilícito previsto no artigo 225.º, do Código Penal, é necessário que alguém abuse da possibilidade que lhe é dada pelo facto de se encontrar na posse de um cartão de crédito ou de garantia, que leve o emitente do mesmo a fazer um pagamento, e, que, em consequência se verifique um prejuízo patrimonial para o emitente ou para terceiro, que pode ser o próprio titular do cartão ou o comerciante.

Quer isto significar que o agente tem de:

a. Abusar de um cartão de crédito ou de garantia;

[22] Cfr. PEREIRA, Sá e LAFAYETTE, Alexandre, ob. cit., pág. 648. Em sentido diverso, de que apenas tutela o património da entidade que emitiu o cartão, *vide* BARREIROS, José António, Crimes contra o património, Lisboa, Lisboa: Universidade Lusíada, 1996, pág. 215.
[23] Cfr. PEREIRA, Sá e LAFAYETTE, Alexandre, ob. cit., pág. 648.
[24] Cfr. GARCIA, M. Miguez, RIO, J. M. Castela, ob. cit., pág. 953.
[25] Cfr. por exemplo Acórdão do Tribunal da Relação de Guimarães, proc. 102/09.8GEBRG.G2, de 29/04/2014.
[26] Neste sentido PEREIRA, Sá e LAFAYETTE, Alexandre, ob. cit., pág. 648. No caso do titular apenas quando o cartão é utilizado por terceiro.
[27] Cfr. BARREIROS, José António, ob. cit., pág. 215.

b. Ter a posse de um destes cartões;
c. Levar o emitente a efectuar um pagamento;
d. Abusar de tal faculdade;
e. Causar um prejuízo ao emitente do cartão ou a terceiro.

4.1. Análise dos elementos do crime

4.1.1. Abusar de um cartão de garantia ou de crédito em virtude de o ter na sua posse

A acção típica consiste no facto de o agente abusar de um cartão de garantia ou de crédito, por estar na posse de um desses cartões, que levam o emitente a efectuar um pagamento.

Para se considerar a acção abusiva, quando o cartão é utilizado pelo titular, é necessário que, para além da verificação dos demais elementos do tipo, este ultrapasse o valor do crédito concedido ("*plafond*") ou que a validade do cartão se mostre ultrapassada[28].

Como refere Damião da Cunha "*a determinação do abuso por parte do titular tem de ser aferida em função das condições do contrato subjacente à emissão do cartão de garantia ou de crédito, pelo que dependerá, nomeadamente, do montante de crédito cujo pagamento a entidade emitente assegure.*"[29].

O abuso do cartão de crédito ou de garantia acontece quando são violadas as condições contratuais com base nas quais o mesmo foi emitido (v.g. cartão expirado ou quando é ultrapassado o limite máximo permitido[30]), que a instituição de crédito e o titular contratualizaram[31].

Apenas existe crime quando são utilizados o cartão de garantia ou de crédito que permita a utilização de crédito do emitente e nunca de débito directo de uma conta bancária associada.

Este preceito aplica-se, igualmente, a terceiro que utilize o cartão de outra pessoa desrespeitando as suas instruções e directivas, ou sem o seu consentimento, mormente porque se apoderou do mesmo[32].

---

[28] Assim HENRIQUES, Manuel de Oliveira Leal e SANTOS, Manuel José Carrilho de Simas, ob. cit., pág. 950-951.
[29] Cfr. CUNHA, J. M. Damião da, ob. cit., pág. 377.
[30] O limite de utilização do cartão de crédito é o valor máximo que, em qualquer momento, pode estar em dívida perante a entidade emitente do cartão. O limite disponível é a diferença entre o limite de utilização definido para o cartão e o valor das transacções, juros, comissões e outros encargos que, entretanto, foram lançados na conta-cartão. A entidade emitente é livre de definir os critérios de determinação do limite de utilização – Cfr. Cadernos do Banco de Portugal, n.º 6, Cartões Bancários, pág. 16.
[31] Neste sentido José Narciso da Cunha Rodrigues, *in* Actas, ob. cit., pág. 520; ALBUQUERQUE, Paulo Pinto de, ob. cit. pág. 873.
[32] Assim *vide* Sousa e Brito, *in* Actas, ob. cit., pág. 450; CUNHA, Damião da, ob. cit., pág. 378, HENRIQUES, Manuel de Oliveira Leal e SANTOS, Manuel José Carrilho de Simas, Código Penal Anotado, 3.ª Ed., II Vol., Rei dos Livros, 2000, pág. 950; GONÇALVES, Maia, ob. cit., pág. 766; GARCIA, M. Miguez e RIO, J. M. Castela, ob. cit., pág. 954; ALBUQUERQUE, P. P., ob. cit., pág. 873.
Na Jurisprudência, entre outros: Acórdão do Tribunal da Relação do Porto, proc. 0010659, de 08/03/2000, Acórdão do Supremo Tribunal de Justiça, proc. 1604/09.1JAPRT.S1, de 26/10/2016, Acórdão do Tribunal da Relação de Coimbra, proc. 1588/10.3PBCBR.C1, de 27/06/2012, disponíveis em www.dgsi.pt.

O agente tem de ter a posse de um destes cartões, independentemente de ser ou não o seu titular, já que tanto pode ser sancionado penalmente o respectivo titular, como qualquer outra pessoa, mesmo que o possua de forma lícita, pois o que importa é a utilização abusiva do cartão e a existência de prejuízo.

A forma como o cartão de garantia ou de crédito se encontra na posse do agente pode ocorrer por qualquer forma, mormente pelo facto de este o ter encontrado, de o cartão lhe ter sido entregue pelo seu titular ou pelo facto de se ter dele apoderado[33].

Trata-se de um crime comum, na medida em que pode ser praticado por qualquer pessoa[34].

4.1.2. Abusar da possibilidade de levar o emitente a efectuar um pagamento

O agente tem de abusar da possibilidade de levar o emitente a efectuar um pagamento, designadamente pagar bens ou serviços, em virtude de ter a posse do cartão. Para isso, basta que o possuidor do cartão leve o emitente a efectuar o pagamento, sendo que tal tem de resultar da posse e da função específica do cartão (de garantia ou de crédito). É indiferente se o abuso tem origem na aquisição de bens ou de serviços, verificando-se o cometimento do ilícito desde que o emitente, verificados os demais requisitos, efectue o pagamento.

O abuso do cartão de garantia ou de crédito levado a cabo pelo titular do mesmo, resulta numa violação do contrato celebrado com a entidade que o emitiu (ex: ultrapassar o montante de crédito contratualizado com o emitente), na medida em que origina um dever de pagamento e um prejuízo patrimonial para o emitente[35].

O ilícito em análise possibilita a responsabilização penal de outrem que não o titular do cartão de garantia ou de crédito, pelo que quando o agente não é o titular do cartão, a prática do crime acontecerá quando aquele o utilize contrariando as instruções do titular do cartão ou sem o seu conhecimento e autorização.

O modo de levar o emitente a efectuar o pagamento é indiferente, podendo ocorrer, na sequência da apresentação do cartão ou da falsificação da assinatura do titular no talão de pagamento.

4.1.3. Causar um prejuízo ao emitente do cartão ou a terceiro

Quando é o próprio titular que abusa do cartão, designadamente quando o utiliza para adquirir um bem a um comerciante, violando as cláusulas contratuais que celebrou com o emitente, mormente por exceder o "*plafond*" ou por utilizar um cartão cujo prazo de validade

[33] Deste modo GARCIA, M. Miguez e RIO, J. M. Castela, ob. cit., pág. 953-954. BARREIROS, José António, ob. cit., pág. 214, defende que a incriminação não se aplica a pessoas que tenham ganho acesso ilegítimo a tais cartões.
[34] Cfr. CUNHA, J. M. Damião da, ob. cit., pág. 376; PEREIRA, Sá e LAFAYETTE, ob. cit., pág. 647.
[35] Cfr. GARCIA, M. Miguez e RIO, J. M. Castela, ob. cit., pág. 954.

se encontra ultrapassado, atinge imediatamente o património deste, na medida em que o emitente efectua o pagamento ao comerciante e vê diminuído o seu património, causando um prejuízo. Igualmente, existe a possibilidade de ficar lesado o património do comerciante, se com culpa, não verificou as condições contratuais, levou o emitente a efectuar o pagamento e, consequentemente, entregou o bem ao agente, já que poderá ser responsabilizado pela violação das condições contratuais celebradas com a instituição de crédito.

Quando o agente é outra pessoa que não o titular do cartão, é possível que seja atingido o património do próprio titular e do emitente, verificando-se a consumação criminosa quando exista prejuízo patrimonial, desde logo quando o cartão é utilizado sem consentimento ou contrariando as directivas do titular.

Se o agente (terceiro) adquirir um bem e o pagar com recurso ao cartão, violando as cláusulas contratuais celebradas com o emitente, atinge imediatamente o património deste, pois efectuou o pagamento ao comerciante, e do titular do cartão, pois é a este que será apresentada a factura e a quem será cobrada a mesma.

Pode, ainda, o comerciante ser afectado patrimonialmente se aceitou o pagamento, com culpa e sem observação do clausulado, e entregou o bem àquele, pois poderá sofrer um prejuízo patrimonial ao ser responsabilizado pela instituição de crédito, por não ter observado as condições contratuais.

Assim, o prejuízo pode ocorrer por força dos dois contratos celebrados, isto é, entre a entidade que emitiu o cartão e o titular do mesmo, bem como entre aquela entidade e os comerciantes que aderiram a tal forma de pagamento e à rede de crédito.

A existência de prejuízo é o elemento fundamental para a verificação do tipo de crime, e já não o património de quem é atingido[36]. É necessária a existência do abuso e o consequente prejuízo patrimonial, mas não é requisito que o agente cause prejuízo a pessoa determinada ou individualize o património que visa atingir através da utilização do cartão, designadamente se causa prejuízo a um banco ou a um comerciante ou ao próprio titular (se utilizado por terceira pessoa)[37].

O prejuízo tem de ser patrimonial, e deverá ser determinado "*através da aplicação de critérios objectivos de natureza económica à concreta situação patrimonial da vítima, concluindo-se pela existência de um dano sempre que se observe uma diminuição do valor económico por referência à posição em que o lesado se encontraria se o agente não houvesse realizado a sua conduta.*"[38]. O prejuízo patrimonial é todo o empobrecimento do património do ofendido, descontado o proveito que tenha obtido em consequência da conduta do agente[39].

[36] Assim *vide* PEREIRA, Sá e LAFAYETTE, ob. cit., pág. 648.
[37] Cfr. PEREIRA, Sá e LAFAYETTE, Alexandre, ob. cit., pág. 650.
[38] Cfr. COSTA, A. M. Almeida, ob. cit., págs.283-284.
[39] Cfr. ALBUQUERQUE, Paulo Pinto de, ob. cit. pág. 848.

Trata-se, portanto, de um crime de dano, quanto ao bem jurídico protegido, e de resultado, quanto à forma de consumação do ataque ao objecto da acção, que se consuma precisamente no momento em que aquele ocorre[40].

4.2. Outras situações relacionadas com a incriminação

O tipo não abrange a utilização do cartão de débito e do cartão de moeda electrónica ou pré-pago, uma vez que estes constituem meios de pagamento imediatos, através de desconto do respectivo montante na conta bancária associada ao cartão ou do próprio cartão.

A utilização do cartão de garantia ou de crédito pelo seu titular, para aquisição de bens ou serviços, e que, posteriormente, não efectue o pagamento das mensalidades dos montantes em dívida, não preenche o tipo, sendo apenas um ilícito civil.

O abuso do cartão de débito, não consentido pelo seu titular, constitui um furto e/ou uma burla informática, enquanto que a utilização deste tipo de cartão, consentida pelo seu titular, mas para fim diverso daquele para o qual foi o agente autorizado, constitui a prática de um crime de abuso de confiança[41]. Por identidade de razões não se inclui no tipo do artigo 225.º, do Código Penal, a utilização do cartão de crédito quando funciona como mero cartão de débito, com a inserção do código secreto (PIN), associado a uma conta bancária com desconto imediato do respectivo saldo[42].

Igualmente, não se verifica a consumação do tipo de crime em estudo quando o titular do cartão consente na utilização do mesmo por outrem, desde que o terceiro o utilize de acordo com as instruções daquele (do titular) e com as condições contratuais.

A problemática da utilização do cartão de crédito para levantamento de numerário através da máquinas multibanco foi, desde logo, colocada pelo Sr. Dr. Lopes Rocha, no seio da Comissão de Revisão do Código Penal de 1995, referindo que esta actuação "*pode já caber de alguma forma na ideia de fraude informática.*"[43].

Face à letra da Lei (artigo 225.º, do Código Penal) resulta que esta conduta se encontra abrangida por este tipo de crime, somente quando o levantamento é efectuado a crédito[44]. Se se tratar de um levantamento a débito, não autorizado, o mesmo encontra-se limitado, em

[40] Cfr. Figueiredo Dias e Sousa e Brito, Actas, ob. cit., pág. 451; ALBUQUERQUE, Paulo Pinto de, ob. cit. pág. 872; BARREIROS, José António, ob. cit., pág. 217.
[41] Assim COSTA, Almeida, ob. cit., pág. 811-812; GONÇALVES, M. Maia, Código Penal Português – Anotado e Comentado, 18.ª Ed., 2007, Almedina, pág. 911.
[42] No sentido de que caso seja utilizado cartão de crédito com código PIN se está perante um crime de burla informática: CUNHA, J. M. Damião da, ob. cit., pág. 379; GARCIA, M. Miguez, RIO, J. M. Castela, ob. cit., pág. 952; e defendendo que se está perante um crime de abuso de cartão de garantia ou de crédito quando é utilizado um cartão de crédito com recurso a código PIN: GONÇALVES, M. Maia, ob. cit. pág. 829; PEREIRA, Sá e LAFAYETTE, Alexandre, ob. cit., pág. 649-650; e a favor na Jurisprudência: Na Jurisprudência, entre outros: Acórdão do Tribunal da Relação do Porto, proc. 0010659, de 08/03/2000, Acórdão do Supremo Tribunal de Justiça, proc. 1604/09.1JAPRT.S1, de 26/10/2016, Acórdão do Tribunal da Relação de Coimbra, proc. 1588/10.3PBCBR.C1, de 27/06/2012, disponíveis em www.dgsi.pt.
[43] Cfr. Lopes Rocha, Actas, ob. cit., pág. 451.
[44] Assim CUNHA, J. M. Damião da, ob. cit., pág. 376, 379. Ver anotação n.º 42.

norma, pelo montante máximo disponível, existente na conta bancária ou ao valor contratualizado, o que constitui um crime de burla informática[45].

A utilização abusiva do cartão de crédito por terceira pessoa implica, uma vez que a maioria dos cartões de crédito o exige, o conhecimento do código secreto, o qual poderá ter sido fornecido pelo seu titular ou obtido, por qualquer forma, pelo possuidor do cartão, o que lhe permitirá efectuar o levantamento de numerário ou pagamento de bens ou serviços (mediante utilização do cartão de crédito e inserção de código PIN)[46]. Esta conduta será subsumível aos crimes de abuso de cartão de garantia ou de crédito (artigo 225.º, do Código Penal), no caso de ser um levantamento / pagamento a crédito, ou de burla informática (artigo 221.º, do Código Penal), nas situações de levantamento / pagamento a débito, e, eventualmente, de furto (artigo 203.º, do Código Penal), dependendo da forma como o cartão chegou à posse do utilizador[47].

Maia Gonçalves sustenta que a utilização abusiva de cartão em sistemas automatizados de pagamento pode ser subsumível à previsão do artigo 225.º, do Código Penal, por o agente "*ter tido conhecimento do número secreto (PIN) que possibilita a utilização do cartão que está em seu poder, porque o descobriu, porque forçou o titular a revelá-lo, ou por qualquer outro processo.*"[48]

5. O Tipo Subjectivo de Ilícito

O tipo subjectivo admite qualquer modalidade do dolo, não sendo punível a título de negligência. É um crime de dolo genérico, nos termos do artigo 14.º, do Código Penal, não se exigindo o dolo específico de enriquecimento[49].

6. As causas de exclusão da Ilicitude

Aplicam-se as regras gerais das causas de exclusão da ilicitude, pelo que o agente que cometa um facto previsto num tipo incriminador (facto típico), por força da aplicação daquelas, não pratica um facto ilícito[50].

Face ao disposto no artigo 31.º, n.ºs 1 e 2, do Código Penal, o facto não é punível quando a sua ilicitude for excluída pela ordem jurídica considerada na sua totalidade, não sendo,

[45] Neste sentido Acórdão do Tribunal da Relação de Guimarães, proc. 102/09.8GEBRG.G2, de 29/04/2014.
[46] Fazendo-o num terminal de pagamento POS - um ponto de venda ou ponto de serviço (do inglês: *Point of Sale ou Point of Service)* - ou na rede Multibanco ou *online* com inserção do número do cartão de crédito e código de segurança (três dígitos de verificação existente no verso do cartão).
[47] Cfr. HENRIQUES, Manuel de Oliveira Leal e SANTOS, Manuel José Carrilho de Simas, ob. cit., pág. 950-951; GARCIA, M. Miguez, RIO, J. M. Castela, ob. cit., pág. 952, 954; CUNHA, J. M. Damião da, ob. cit., pág. 379.
[48] Cfr. GONÇALVES, Maia, ob. cit., pág. 767.
[49] BARREIROS, José António, ob. cit., pág. 217, critica o facto de não se exigir o dolo específico de enriquecimento, uma vez que se trata de um crime contra o património.
[50] Cfr. SILVA, Germano Marques da, Direito Penal Português - Teoria do Crime, Lisboa, Universidade Católica Portuguesa Editora, 2015, pág. 149.

designadamente, ilícito o facto praticado em legítima defesa; no exercício de um direito; no cumprimento de um dever imposto por lei ou por ordem legítima da autoridade; ou com o consentimento do titular do interesse jurídico lesado. Destaca-se a possibilidade de aplicação do direito de necessidade, mediante o qual se tutela um direito em perigo, actual, de sofrer um dano através do sacrifício de outro direito de pessoa que não interveio voluntariamente na criação daquele perigo. É essencial que se verifique uma superioridade do bem a defender relativamente ao bem a sacrificar, e se o meio usado é justo de forma a que se possa exigir a solidariedade do titular do bem sacrificado[51].

7. As causas de exclusão da culpa

O crime é um facto típico ilícito e culpável, sendo a culpa um juízo de reprovação ao agente por ter, voluntariamente, desobedecido a um comando legal, e ter consciente e livremente praticado o ilícito[52]. O juízo de culpa pressupõe a prática de um facto ilícito, mas há causas que suprimem ou influenciam a vontade no seu exercício, e que determinam a maior ou menor desculpabilidade da vontade, como são as causas de exclusão da culpa.

Na parte geral do Código Penal encontram-se previstas causas que excluem a culpa, nomeadamente as previstas nos artigos 17.º (erro sobre a ilicitude), 33.º, n.º 2 (excesso de legítima defesa resultante de perturbação, medo ou susto, não censuráveis), 35.º (estado de necessidade desculpante) e 37.º (obediência indevida desculpante). Relativamente ao crime de abuso de cartão de garantia ou de crédito são aplicáveis todas as causas de exclusão da culpa, em especial o estado de necessidade desculpante[53].

8. As formas especiais do crime

8.1. A Tentativa

A tentativa é punível, por força do disposto nos artigos 225.º, n.º 2, e 23.º, n.º 1, do Código Penal[54]. A punibilidade da tentativa não estava inicialmente pensada pela Comissão Revisora do Código Penal, de 1995, tendo sido acrescentada mediante proposta do professor Doutor Figueiredo Dias, uma vez que o regime de punição criado para o abuso de cartão de garantia e de crédito era semelhante ao do crime de burla[55]. Em virtude da massificação da utilização de tais cartões[56], mostra-se elevada a possibilidade de, igualmente, aumentarem o número de situações em que o agente pretende utilizar o cartão sem conseguir causar um prejuízo patrimonial ao emitente, o que pode, inclusive, redundar em tentativas impossíveis[57].

[51] Cfr. CUNHA, J. M. Damião da, ob. cit., pág. 380.
[52] Assim SILVA, Germano Marques da, ob. cit., pág. 272.
[53] Neste sentido *vide* CUNHA, J. M. Damião da, ob. cit., pág. 380; PEREIRA, Sá e LAFAYETTE, Alexandre, ob. cit., pág. 650.
[54] Cfr. GARCIA, M. Miguez, RIO, J. M. Castela, ob. cit., pág. 954; CUNHA, J. M. Damião da, ob. cit., págs. 380-381.
[55] Cfr. Figueiredo Dias, Actas, ob. cit., pág. 451.
[56] Cfr. VASCONCELOS, Joana de, ob. cit., págs. 308, 312.
[57] *"Diz-se que a tentativa é inidónea ou impossível e também se denomina de crime impossível a conduta do agente inapta à consumação do crime, quer em razão dos meios empregados quer por falta do objecto essencial. É que,*

São aplicáveis as regras gerais da desistência. Dispõe o artigo 24.º, n.ºs 1 e 2, do Código Penal, que:

"*1. A tentativa deixa de ser punível quando o agente voluntariamente desistir de prosseguir na execução do crime, ou impedir a consumação, ou, não obstante a consumação, impedir a verificação do resultado não compreendido no tipo de crime; 2. Quando a consumação ou a verificação do resultado forem impedidas por facto independente da conduta do desistente, a tentativa não é punível se este se esforçar seriamente por evitar uma ou outra.*".

Assim, a tentativa de cometimento do crime, subsumível à previsão dos artigos 22.º e 23.º do Código Penal, pode não ser punível, mas para assim ocorrer tem o agente de desistir da execução do delito, desde que tal desistência seja relevante. A desistência é relevante quando o agente:

a) Abandona voluntária e espontaneamente a execução do crime, ou seja, se não pratica mais actos de execução e desiste de forma voluntária (artigo 24.º, n.º 1, 1.ª parte, do Código Penal);
b) Impede voluntária e espontaneamente a consumação do crime, o que pode efectuar por actividade própria e voluntária, ainda que com o auxílio de outras pessoas, de forma a evitar que o resultado do crime se produza (artigo 24.º, n.º 1, 2.ª parte, do Código Penal);
c) Impede a verificação do resultado não compreendido no tipo, quando se tratem de crimes formais / que se verificam independentemente da produção de resultado material, e o agente tenha evitado, através da sua própria intervenção, mesmo que com o auxílio de terceiros, que se produza o resultado (artigo 24.º, n.º 1, 3.ª parte, do Código Penal);
d) Faça um esforço sério, através de actos concretos, para evitar a consumação do crime ou o seu resultado mas, que, todavia, não foi suficiente para o evitar (artigo 24.º, n.º 2, do Código Penal).

A desistência relevante da tentativa é uma causa pessoal de exclusão da punibilidade, motivo pelo qual para se aferir do carácter voluntário da desistência se tem de levar em consideração o comportamento exteriorizado pelo agente e analisá-lo de forma a se concluir se o seu objectivo era, realmente, impedir a consumação do crime.

8.2. O Concurso

Dispõe o artigo 30.º, n.º 1, do Código Penal, que: "*O número de crimes determina-se pelo número de tipos de crime efectivamente cometidos, ou pelo número de vezes que o mesmo tipo de crime for preenchido pela conduta do agente.*"

---

para haver tentativa, como dispõe o art.º 22.º, é necessário que sejam praticados actos de execução de um crime e os actos de execução ou preenchem um elemento constitutivo de um tipo de crime, ou são idóneos a produzir o resultado típico ou são de natureza a fazer esperar que se lhes sigam actos das espécies anteriores (art.º 22.º, n.º 2). Quando os actos praticados pelo agente não são actos de execução (não são típicos) diz-se que a tentativa é inidónea e quando falta o objecto diz-se que a tentativa é impossível." – cfr. SILVA, Germano Marques da, ob. cit., págs. 327-328.

Assim, a mesma conduta do agente pode constituir vários crimes ou várias vezes o mesmo crime, o que sucederá quando a mesma lese vários bens jurídicos, pelo que face às diversas possibilidades de utilização dos cartões de garantia e de crédito, desde logo devido ao modo como o cartão pode ter sido obtido ou à sua posterior utilização.

O concurso efectivo de crimes não se confunde com o concurso aparente de crimes, pois este é um concurso de normas que pressupõe a unidade do facto e a pluralidade de normas potencialmente aplicáveis, mas o facto constitui apenas um crime, daí se designar por aparente.

8.2.1. O crime de burla

O crime de burla é aquele que mais dúvidas levanta no que diz respeito ao concurso de crimes com o ora em estudo, na medida em que se poderão verificar os dois tipos, sendo certo que o crime de abuso de cartão de garantia ou de crédito tem uma relação de especialidade com o crime previsto no artigo 217.º, do Código Penal[58].

Os requisitos para a verificação do crime de abuso de cartão de garantia ou de crédito são menos exigentes do que os que se têm de verificar em relação ao crime de burla. Quando se utilizam abusivamente cartões de garantia ou de crédito, deverá tal conduta ser subsumida ao tipo de crime em análise, uma vez que é, como se disse, uma norma especial em relação ao crime de burla[59]. A incriminação do abuso de cartão de garantia ou de crédito surgiu precisamente para resolver os problemas gerados com a sua utilização e com a ligação entre a conduta fraudulenta e o prejuízo patrimonial, visto que ficariam por verificar o erro e a astúcia que levaram ao prejuízo[60].

Se o agente utilizar o cartão de crédito, cujo montante máximo permitido ("*plafond*") se encontra ultrapassado e disso tem conhecimento, e, para tanto, convencer, através de algum logro ou artifício, o comerciante a aceitar o pagamento, sem obter a necessária autorização do emitente do cartão, estarão preenchidos os dois tipos de crime. Isto porque, tal conduta afecta o património do comerciante, uma vez que não cumpriu as cláusulas contratuais que celebrou com o emitente e que, portanto, poderá ser responsabilizado pelo prejuízo, nos moldes anteriormente referidos, situação em que existirá uma relação de concurso aparente entre o crime de abuso de cartão de garantia ou de crédito e o crime de burla[61].

8.2.2. O crime de burla informática

[58] Cfr. ALBUQUERQUE, Paulo Pinto de, ob. cit., pág. 873.
[59] GARCIA, M. Miguez, RIO, J. M. Castela, ob. cit., pág. 954, e ALBUQUERQUE, Paulo Pinto de, ob. cit., pág. 873, defendem que existe uma relação de concurso aparente entre o crime de abuso de cartão de garantia ou de crédito e os crimes de burla e burla informática.
[60] Assim Sousa e Brito, Actas, ob. cit., págs. 450, 541.
[61] Cfr. CUNHA, J. M. Damião da, ob. cit., pág. 381. Contudo, com o desenvolvimento dos novos meios tecnológicos tal hipótese afigura-se de difícil verificação face à comunicação instantânea entre o emitente e o comerciante.

Quando é utilizado um cartão de crédito, como meio de pagamento de bens ou levantamento de dinheiro, que permite ao agente a apropriação de dinheiro através da introdução e da utilização do sistema informático das *A.T.M.* ("*automated teller machine*" - Caixa automática multibanco) sem autorização, com a introdução do cartão e digitação do código secreto, obtendo um enriquecimento ilegítimo e causando um correspondente prejuízo patrimonial ao titular do cartão, verifica-se a prática de um crime de burla informática[62], se o pagamento / levantamento for a débito, e de abuso de cartão de garantia ou de crédito, se o pagamento / levantamento for a crédito[63]. Trata-se de uma questão muito debatida e controversa[64], contudo não se pode olvidar que o crime previsto no artigo 225.º do Código Penal, tem uma relação de especialidade em relação ao crime de burla informática[65], pelo que esta se nos afigura como a melhor solução e enquadramento legal. Caso assim não se entendesse, e uma vez que, actualmente, a esmagadora maioria dos cartões de crédito exige a inserção de código secreto aquando da sua utilização, resultaria no esvaziamento e inutilidade do crime em estudo, na medida em que a utilização abusiva do cartão de crédito, para pagamento a crédito, com recurso a código PIN, seriam subsumidas ao crime de burla informática[66], conforme referido anteriormente.

8.2.3. O crime de infidelidade

Pode ocorrer concurso efectivo entre o crime de abuso de cartão de garantia ou de crédito e de infidelidade nas situações em que uma empresa concede a um seu trabalhador um cartão de crédito (vulgarmente designado por "cartão empresa"), o qual tem um limite de utilização mensal associado, e funciona para pagar despesas relacionadas com a prestação do trabalho.

Tal concurso sucede quando o agente desrespeita e ultrapassa o limite do crédito concedido pelo emitente, utiliza o cartão de crédito para além desse montante, e, simultaneamente, quebra a relação de confiança com a empresa / entidade empregadora, na medida em que utilizou o cartão de forma contrária às finalidades para o qual lhe foi atribuído. Isto pode ter lugar quando os pagamentos efectuados são relativos a outros bens e serviços que não se relacionam com a prestação do trabalho, como são as deslocações de casa para o local de trabalho ou despesas com alimentação, viagens, vestuário ou alojamento, mas tão-somente

[62] Neste sentido *vide* Acórdão do Tribunal da Relação do Porto, proc. 140/10.8PJPRT.P1, de 14-03-2012; Acórdão do Tribunal da Relação de Guimarães, proc. 541/10.1GAPTB.G1, de 18/12/2012, disponíveis em www.dgsi.pt.
[63] Assim Acórdão do Tribunal da Relação de Guimarães, proc. 102/09.8GEBRG.G2, de 29/04/2014, disponível em www.dgsi.pt.
[64] Como se referiu anteriormente: No sentido de que caso seja utilizado PIN se está perante um crime de burla informática: CUNHA, J. M. Damião da, ob. cit., pág. 379; GARCIA, M. Miguez, RIO, J. M. Castela, ob. cit., pág. 952; e defendendo que se está perante um crime de abuso de cartão de garantia ou de crédito quando é utilizado um cartão de crédito com recurso a PIN: GONÇALVES, M. Maia, ob. cit. pág. 829; PEREIRA, Sá e LAFAYETTE, Alexandre, ob. cit., págs. 649-650.
[65] Cfr. ALBUQUERQUE, Paulo Pinto de, ob. cit., pág. 873.
[66] A tipicidade do meio de obtenção de enriquecimento ilegítimo, que implica o prejuízo patrimonial de outrem, consiste na interferência no resultado de tratamento de dados ou mediante a estruturação incorrecta de programa informático, na utilização incorrecta ou incompleta de dados, na utilização de dados sem autorização ou na intervenção por qualquer outro modo não autorizada no processamento - Cfr. Acórdão do Supremo Tribunal de Justiça, proc. 06P1942, 20-09-2006, disponível em www.dgsi.pt.

com a satisfação de gostos e interesses pessoais do agente, os quais podem ser supérfluos ou ostentatórios, prejudicando a situação económico-financeira da empresa[67].

8.2.4. Os crimes de contrafacção de moeda, falsidade informática, falsificação ou contrafacção de documento e furto.

O artigo 267.º, n.º 1, alínea c), do Código Penal, equipara os cartões de crédito a moeda. Quer isto significar que quem praticar a contrafacção (clonagem) de um cartão de crédito, com intenção de o pôr em circulação como sendo legítimo, será punido pelo crime de contrafacção de moeda, previsto no artigo 262.º, n.º 1, com referência ao artigo 267.º, n.º 1, alínea c), ambos do Código Penal.

Contudo, caso o cartão de crédito clonado seja utilizado e, assim, se verifique um prejuízo patrimonial efectivo para o emitente do cartão ou do seu titular, estar-se-á perante um concurso efectivo de crimes, isto é, entre o crime de contrafacção de moeda, o crime de falsidade informática, previsto e punido pelo artigo 3.º, n.ºs 1 e 2, da Lei n.º 109/2009, de 15/09 (Lei do Cibercrime) e o crime de burla informática (artigo 221.º do Código Penal)[68]. Tal acontece, por exemplo, quando o agente consegue através de uma A.T.M. obter a informação existente na banda magnética[69] de um cartão de crédito que aí for inserido, e, posteriormente utilizar e inserir tais dados informáticos num cartão por si fabricado e o utilizar para efectuar levantamentos ou pagamento de bens ou serviços[70].

Entre tais crimes existe concurso efectivo, uma vez que quanto à contrafacção de moeda, o bem jurídico protegido diz respeito à protecção da confiança e da fé pública na moeda e na autenticidade do sistema monetário[71], quanto à burla informática tutela-se o património, e na falsidade informática defende-se a integridade dos sistemas de informação[72].

A somar a isto pode, também, suceder que o agente, ao efectuar o pagamento de bens ou serviços com recurso ao "*cartão de crédito adulterado*" ou de um cartão de crédito não adulterado mas furtado, assine o talão de pagamento ou exiba um documento de identificação por si fabricado, correspondente ao titular do cartão de crédito, o que constituirá, para além

[67] Cfr. Acórdão do Supremo Tribunal de Justiça, proc. 352/01.5TACBR.C1.S1, de 15/06/2011, disponível em www.dgsi.pt.
[68] Cfr. Acórdão do Tribunal da Relação do Porto, proc. 2013/13.3JAPRT.P1, de 17/09/2014, disponível em www.dgsi.pt.
[69] Dispositivo electrónico de segurança no verso do cartão que contém informação associada ao titular, entidade emitente e tipo de cartão. Dados informáticos são qualquer representação de factos, informações ou conceitos sob uma forma susceptível de processamento num sistema informático, incluindo os programas aptos a fazerem um sistema informático executar uma função (artigo 2.º, alínea b), da Lei 109/2009, de 15/09).
[70] Assim Acórdão do Tribunal da Relação de Lisboa, proc. 7876/10.1JFLSB.L1-5, de 10/07/2012, disponível em www.dgsi.pt.
[71] Cfr. COSTA, A. M. Almeida, ob. cit., págs. 749 e 808.
[72] Neste sentido *vide* Acórdão do Tribunal da Relação do Porto, proc. 2013/13.3JAPRT.P1, de 17/09/2014; e Acórdãos do Tribunal da Relação de Lisboa, proc. 189/09.3JASTB.L1-5, de 30/06/2011, e 7876/10.1JFLSB.L1-5, de 10/07/2012, disponíveis em www.dgsi.pt.

dos ilícitos supra referidos, a prática de um crime de falsificação ou contrafacção de documento (artigo 256.º, n.º 1, alínea a), do Código Penal)[73].

É, igualmente, possível suceder que o cartão de crédito (não clonado) seja subtraído ao seu titular e, posteriormente, utilizado para levantar dinheiro em caixa de A.T.M.[74] ou para pagamento de bens ou serviços, o que consubstanciará a prática, em concurso efectivo, de um crime de furto (artigo 203.º, do Código Penal), e outro de abuso de cartão de garantia ou de crédito, se o levantamento / pagamento for a crédito, ou de burla informática (artigo 221.º, do Código Penal), se o levantamento / pagamento for a débito[75].

8.2.5. O Crime de emissão de cheque sem provisão

Pode haver concurso efectivo entre o crime de abuso de cartão de garantia ou de crédito com o crime de emissão de cheque sem provisão, previsto no artigo 11.º, do Decreto-Lei n.º 454/91, de 28/12, nas situações em que o titular do cartão de garantia emite um cheque, de acordo com o valor da garantia que o banco assumiu, mas que já se encontra ultrapassada[76].

8.3. A comparticipação

O crime de abuso de cartão de garantia ou de crédito pode ser cometido por mais de um agente, designadamente quando o titular do cartão actua em conluio com o comerciante, no sentido de prejudicaram o emitente do cartão, de forma a obterem um benefício patrimonial ao mesmo tempo que lesam patrimonialmente aquele. A actuação criminosa pode ocorrer em co-autoria quando dois ou mais agentes decidem actuar de forma concertada e para tal utilizam o cartão de crédito de forma abusiva, nos moldes anteriormente referidos.

9. A pena e o regime punitivo

9.1. A moldura penal

[73] Neste sentido cfr. Acórdão do Tribunal da Relação de Lisboa, proc. 7876/10.1JFLSB.L1-5, de 10/07/2012, disponível em www.dgsi.pt; CUNHA, J. M. Damião da, ob. cit., pág. 382.
[74] A.T.M. ou "*Automated Teller Machine*" é um "*equipamento que permite aos titulares de cartões bancários com banda magnética e/ou chip aceder a serviços disponibilizados a esses cartões, designadamente, levantar dinheiro de contas, consultar saldos e movimentos de conta, efectuar transferências de fundos e depositar dinheiro. Os caixas automáticos podem funcionar em sistema real-time, com ligação ao sistema informático da entidade emitente do cartão ou em on-line, com acesso a uma base de dados autorizada que contém informação relativa à conta de depósitos à ordem associada ao cartão de débito.*" – cfr. Cadernos do Banco de Portugal, n.º 6, Cartões Bancários, pág. 20.
[75] Cfr. Acórdão do Tribunal da Relação de Évora, proc. 90/11.0GCLLE.E1, de 20/01/2015, disponível em www.dgsi.pt.
[76] Assim CUNHA, J. M. Damião da, ob. cit., pág. 382.

O crime de abuso de cartão de garantia ou de crédito é punido consoante o montante do prejuízo, existindo, desse modo, duas agravações em razão do valor (valor elevado e consideravelmente elevado)[77].

Dispõe o artigo 202.º, alíneas a) e b), do Código Penal, que: "*a) Valor elevado: aquele que exceder 50 unidades de conta avaliadas no momento da prática do facto*" e "*b) Valor consideravelmente elevado: aquele que exceder 200 unidades de conta avaliadas no momento da prática do facto.*".

Se o prejuízo for inferior ao valor elevado, o agente é punido com pena de prisão até 3 anos ou com pena de multa (artigo 225.º, n.º 1, do Código Penal).

Se o prejuízo for de valor elevado (superior a € 5.100,00) e inferior ao valor consideravelmente elevado (superior a € 20.400,00), o agente é punido com pena de prisão até 5 anos ou com pena de multa até 600 dias (artigo 225.º, n.º 5, alínea a), do Código Penal).

Já se o prejuízo for de valor consideravelmente elevado, o agente é punido com pena de prisão de 2 a 8 anos (artigo 225.º, n.º 5, alínea b), do Código Penal)[78].

9.2. A reparação e a restituição

Aplicam-se as regras especiais previstas nos artigos 206.º e 207.º, do Código Penal, pelo que a reparação e a restituição do prejuízo causado, sem dano ilegítimo de terceiro, até ao início da audiência de julgamento em 1.ª instância, levam à atenuação especial da pena se forem integrais (artigo 206.º, n.º 2, do Código Penal), ou a essa possibilidade se forem parciais (n.º 3, do mesmo normativo legal) [79].

9.3. O procedimento criminal, a natureza do crime e a prescrição.

O artigo 225.º, n.º 3, do Código Penal, estabelece que o procedimento criminal depende de queixa.

---

[77] A utilização do conceito da UC (actualmente fixada em € 102,00), e do valor elevado e consideravelmente elevado foi proposto pelo Sr. Procurador-Geral da República Dr. Cunha Rodrigues, no âmbito da Revisão do Código Penal de 1995, segundo o qual: "*o conceito de 'valor' passa a referir-se à unidade de conta processual. Com efeito, as alçadas não têm que ver só com a realidade do valor do litígio. E o próprio valor da causa é aleatório e fixado, algumas vezes, em função do direito ao recurso. As alçadas exprimem situações-problema de tipo complexo que estão na base da organização judiciária e em que estão presentes factores e considerações de diversa índole.*" – cfr. Actas, ob. cit., pág. 345.

[78] Neste sentido *vide* PEREIRA, Sá e LAFAYETTE, Alexandre, ob. cit., pág. 650; CUNHA, J. M. Damião da, ob. cit., pág. 383.

[79] Artigo 206.º, n.ºs 2 e 3, do Código Penal: "*2 - Quando a coisa ou o animal furtados ou ilegitimamente apropriados forem restituídos, ou tiver lugar a reparação integral do prejuízo causado, sem dano ilegítimo de terceiro, até ao início da audiência de julgamento em 1.º instância, a pena é especialmente atenuada. 3 - Se a restituição ou a reparação forem parciais, a pena pode ser especialmente atenuada.*"; HENRIQUES, Manuel de Oliveira Leal e SANTOS, Manuel José Carrilho de Simas, ob. cit., pág. 598; PEREIRA, Sá e LAFAYETTE, Alexandre, ob. cit., pág. 650; CUNHA, J. M. Damião da, ob. cit., pág. 383.

Tem legitimidade para apresentar queixa quem for prejudicado pelo abuso do cartão, considerando-se como tal o titular dos interesses que a Lei especialmente quis proteger com a incriminação (artigo 113.º, n.º 1, do Código Penal)[80].

O crime simples (n.º 1) é semipúblico, o crime qualificado (n.º 5) é público e o crime cometido nas circunstâncias previstas no artigo 207.º, do Código Penal, é particular[81].
Será, assim, um crime particular se se verificar uma relação do agente com a vítima (se for cônjuge, ascendente, descendente, adoptante, adoptado, parente ou afim até ao 2.º grau da vítima, ou com ela viver em condições análogas às dos cônjuges) ou se a coisa for de diminuto valor e se destinar a utilização imediata e indispensável à satisfação de uma necessidade do agente ou de pessoa com ele relacionada daquela forma.

Dispõe o artigo 48.º, do Código de Processo Penal, que: "*O Ministério Público tem legitimidade para promover o processo penal, com as restrições constantes dos artigos 49.º a 52.º.*". Assim, e quanto à legitimidade para promover o processo penal quanto a crime dependente de queixa, como é o caso do n.º 1 do artigo 225.º do Código Penal e quando o mesmo é cometido nas circunstâncias previstas no artigo 207.º do mesmo diploma legal, dispõe o artigo 49.º, n.ºs 1 e 2, do Código de Processo Penal, que é necessário que os ofendidos se queixem e dêem conhecimento do facto ao Ministério Público, para que este promova o processo, sendo que se considera feita a queixa dirigida a qualquer outra entidade que tenha a obrigação legal de a transmitir àquele.

O artigo 246.º, n.º 4, do Código de Processo Penal, torna obrigatória para o denunciante do crime particular a declaração de que pretende constituir-se assistente e, neste caso, impõe-se à autoridade judiciária ou ao OPC a quem a denúncia foi feita verbalmente, a advertência ao denunciante da obrigatoriedade de constituição de assistente e dos procedimentos a observar.

Quando o crime tenha natureza semi-pública e particular, nos casos supra-referidos, o procedimento criminal é passível de desistência de queixa, desde que não haja oposição do arguido, até à publicação da sentença da primeira instância (*ex vi* artigo 116.º, n.º 2, do Código Penal).

O direito de queixa é passível de ser exercido no prazo de seis meses a contar da data em que o titular teve conhecimento do facto e dos seus autores (artigo 115.º, n.º 1, do Código Penal).

O crime simples (n.º 1) prescreve no prazo de cinco anos (artigo 118.º, n.º 1, alínea c), do Código Penal), o crime qualificado (n.º 5, alíneas a) e b)) prescreve no prazo de dez anos (artigo 118.º, n.º 1, alínea b), do Código Penal).

[80] Assim ALBUQUERQUE, Paulo Pinto de, ob. cit. pág. 874; PEREIRA, Sá e LAFAYETTE, Alexandre, ob. cit., pág. 650.
[81] Artigo 207.º, n.º 1, alíneas a) e b), do Código Penal: "*a) O agente for cônjuge, ascendente, descendente, adoptante, adoptado, parente ou afim até ao 2.º grau da vítima, ou com ela viver em condições análogas às dos cônjuges; ou b) A coisa ou o animal furtados ou ilegitimamente apropriados forem de valor diminuto e destinados a utilização imediata e indispensável à satisfação de uma necessidade do agente ou de outra pessoa mencionada na alínea a).*"; neste sentido cfr. HENRIQUES, Manuel de Oliveira Leal e SANTOS, Manuel José Carrilho de Simas, ob. cit., pág. 599; ALBUQUERQUE, Paulo Pinto de, ob. cit. pág. 874.

Capítulo II – Prática e gestão processual

1. O Inquérito

1.1. A aquisição da notícia do crime e a definição do objecto do processo

A aquisição da notícia do crime de abuso de cartão de garantia ou de crédito, nos termos do disposto no artigo 241.º, do Código de Processo Penal, pode acontecer de três formas, isto é, por conhecimento próprio, por intermédio dos órgãos de polícia criminal e transmitida posteriormente ao Ministério Público mediante auto de notícia ou denúncia, e, ainda, por denúncia efectuada verbalmente ou por escrito junto do Ministério Público.

O Estatuto do Ministério Público consagra, no seu artigo 3.º, n.º 1, alíneas h) e n), que lhe cabe "*dirigir a investigação criminal, ainda quando realizada por outras entidades"* e *"fiscalizar a actividade processual dos órgãos de polícia criminal*", orientado pelo princípio da legalidade e da objectividade (artigos 219.º, n.º 1, da Constituição da República Portuguesa, 3.º, n.º 1, alíneas c), h) e i), do Estatuto do Ministério Público).

Assim, recebida a notícia do crime, o Ministério Público, tendo em consideração os factos relatados, procede à abertura de inquérito, nos termos do disposto nos artigos 53.º, n.ºs 1 e 2, alíneas a) e b), 262.º, n.ºs 1 e 2, 267.º, do Código de Processo Penal. O inquérito compreende o conjunto de diligências que visam investigar a existência de um crime, determinar os seus agentes e a sua responsabilidade, descobrir e recolher provas, em ordem à decisão sobre a acusação (artigo 262.º, n.º 1, do Código de Processo Penal), sendo que o Ministério Público pratica os actos e assegura os meios de prova necessários à realização das referidas finalidades (artigo 267.º, do Código de Processo Penal), devendo, desde logo:

a) Verificar se o procedimento legal se encontra prescrito (artigos 118.º a 126.º, do Código Penal);
b) Conferir a natureza do crime - particular, semipúblico ou público - (artigos 48.º, 49.º, n.º 1, e 50.º, n.º 1, do Código de Processo Penal);
c) Aferir da tempestividade da queixa (artigo 115.º, do Código Penal);
d) Apreciar a competência territorial (artigos 19.º a 23, 264.º, do Código de Processo Penal;
e) Ponderar a sujeição do inquérito a segredo de justiça (artigo 86.º, do Código de Processo Penal);
f) Ordenar a realização de diligências urgentes, designadamente relacionadas com a preservação da prova (ex: preservação das imagens de videovigilância).

Sendo o Ministério Público o titular da acção penal incumbe-lhe a direcção do inquérito, pelo que, para o efeito, é coadjuvado pelos órgãos de polícia criminal, que actuam sobe a sua directa orientação, e na sua dependência funcional com vista à realização das finalidades do processo (*ex vi* artigos 9.º, n.º 2, 55.º, n.º 1, 56.º, 263.º, do Código de Processo Penal), nos

quais podem ser delegadas a realização de "*quaisquer diligências e investigações relativas ao inquérito*" (artigo 270.º, n.º 1, do Código de Processo Penal).

Ab initio cumpre ao Ministério Público definir as orientações investigatórias, ordenando, designadamente, a recolha de imagens de videovigilância do local onde o cartão foi utilizado, o exame dactiloscópico efectuado ao cartão no caso de o mesmo ter sido deixado no local do pagamento dos bens ou serviços, quando utilizado por terceira pessoa cuja identidade se desconhece, solicitar informações ao emitente do cartão sobre a identificação do titular do mesmo e respectivas condições contratuais, questionando sobre qual o limite de crédito, crédito até então utilizado, crédito abusivamente utilizado, data de validade do cartão, se o pagamento foi efectuado a crédito ou a débito, entre outras que casuisticamente se mostrem adequadas.

1.2. A Investigação

O Ministério Público durante a investigação deverá diligenciar pela recolha de meios de prova que forneçam indícios suficientes da prática de crime e de quem foi o seu autor (artigo 283.º, n.º 1, do Código de Processo Penal). A investigação do crime em análise é, necessariamente, posterior ao evento lesivo do património, motivo pelo qual a notícia do crime e a recolha de prova se mostram fulcrais para a boa condução e conclusão do inquérito.

Assim, face aos poderes de direcção do inquérito por parte do Ministério Público, cumpre salientar os contornos que estes podem assumir, salientando-se a necessidade de existir um reforço da direcção da investigação através da criação de um plano de investigação, em coordenação com o Órgão de Polícia Criminal, no caso de ser delegada a competência para a investigação criminal, devendo o Magistrado realizar pessoalmente as diligências mais relevantes, principalmente o interrogatório do(s) arguido(s).

Deverá exigir-se dos OPC's a rápida comunicação da notícia do crime (artigos 243.º, n.º 3, 245.º e 248.º, do Código de Processo Penal), de forma, por exemplo, a se conseguir preservar as imagens de videovigilância[82], e a se emitir emitir directivas, ordens ou instruções sobre o modo processual de realização da investigação criminal, com indicação de diligências a realizar; apreciar o resultado das investigações levadas a cabo pelo OPC; bem como fiscalizar a realização da investigação.

Os órgãos de polícia criminal apesar de assistirem, actuaram sob a directa orientação e na dependência funcional do Ministério Público, sendo esta dependência absoluta no que concerne às actividades processuais, dispõem de autonomia na sua actuação, quando lhes é delegada a investigação dos inquéritos, designadamente por força dos meios e das capacidades técnicas de que dispõem[83].

[82] Cfr. Artigos 4.º, n.º 4, da Lei n.º 67/98, de 26/10, e 31.º, n.ºs 1 e 2, da Lei n.º 34/2013, de 16/05.
[83] Na investigação deste tipo de criminalidade, poderá ser aplicável a Lei n.º 5/2002, de 11/01 (Medidas de Combate à Criminalidade Organizada), quando se verifique e seja utilizado um cartão de crédito contrafeito, portanto exista contrafacção de moeda e de títulos equiparados a moeda, nos moldes anteriormente explicados, por força do

Quanto ao estatuto coactivo do arguido, o cometimento deste crime, desde que desacompanhado de outros tipos legais e o agente seja primário, não exigirá a necessidade de aplicação de uma medida de coacção mais gravosa do que o Termo de Identidade e Residência.

1.3. As medidas cautelares, de polícia e da recolha de prova

Na investigação do crime em estudo, como em qualquer outro, deve ser tomada em consideração a liberdade que é dada ao investigador pelo artigo 124.º, do Código de Processo Penal, segundo o qual "*constituem objecto da prova todos os factos juridicamente relevantes para a existência ou inexistência do crime, a punibilidade ou não punibilidade do arguido e a determinação da pena ou da medida de segurança aplicáveis*" e, ainda, pelo artigo 125.º do mesmo diploma, que define serem "*admissíveis as provas que não forem proibidas por lei*".

O Código de Processo Penal, nos artigos 124.º a 190.º, prevê os meios de obtenção da prova (os exames, as revistas e a busca, as apreensões e as escutas telefónicas) e os meios de prova típicos, como são: a prova testemunhal; as declarações do arguido, do assistente e das partes civis; a acareação; a prova por reconhecimento (pessoas e de objectos); a reconstituição do facto; a prova pericial; e a prova documental.

A investigação deverá ser, como em todas, efectivamente controlada e dirigida de perto pelo Magistrado, sendo que a mesma poderá passar, numa primeira fase, pela preservação expedita de dados, pelo exame de vestígios deixados no cartão de crédito e do local do crime, quando o cartão seja utilizado por terceira pessoa cuja identidade se desconhece, mormente em caso de furto, e manutenção do estado de coisas e dos lugares (e preservação de vestígios de modo a que não se apaguem ou alterem), nos termos dos artigos 249.º, n.º 2, alínea a), 171.º, n.º 2, e 173.º do Código de Processo Penal; Registo fotográfico; Recolha de materiais ou substâncias para posterior análise técnica de forma a identificar o agente que tenha utilizado o cartão, elaborando-se os respectivos relatórios e autos (artigos 253.º, n.º 1, e 275.º, n.º 1, do Código de Processo Penal).

---

disposto no artigo 1.º, alínea o), do referido diploma legal, e 262.º, n.º 1, com referência ao artigo 267.º, n.º 1, alínea c), do Código Penal. Tal possibilitará a admissibilidade de outros meios de prova, mormente, a quebra de segredo relativamente a instituições de crédito , sociedades financeiras, instituições de pagamento e instituições de moeda electrónica (artigos 2.º a 5.º do referido diploma legal) e, ainda, o registo de voz e de imagem como meio de obtenção de prova (artigo 6.º, da referida Lei n.º 5/2002).
Tal diploma poderá ter aplicação, não concretamente quanto ao crime de abuso de cartão de garantia ou de crédito, mas por crime conexo, sendo certo que o recurso a este meio de obtenção de prova depende da verificação cumulativa dos requisitos seguintes: a existência de uma investigação criminal em curso, que o crime em investigação seja de catálogo previsto no artigo 1.º, da Lei n.º 5/2002, que o recurso a esta Lei seja necessário para a investigação do crime, cujo sucesso não conseguiria ser alcançado com o recurso a outros meios menos invasivos e existir prévia ordem ou autorização do juiz.
O artigo 6.º, n.º 3, da Lei n.º 5/2002, de 11/01, faz uma remissão expressa para as formalidades previstas no artigo 188.º, do Código de Processo Penal, relativas à intercepção e gravação de conversações telefónicas e equiparadas, as quais terão de ser observadas. Logo, como o registo de voz e imagem (artigo 6.º, da Lei n.º 5/2002) contende com direitos fundamentais, como são o direito à privacidade, à imagem e à liberdade de movimentos, independentemente de ocorrerem dentro ou fora da esfera da vida privada ou da intimidade dos visados, pelo que a restrição destes e outros direitos apenas se mostra admissível nos casos expressamente previstos na lei, e sempre na estrita medida em que se limitem à salvaguarda de outros direitos ou interesses constitucionalmente protegidos (artigo 18.º, da Constituição da República Portuguesa).

Segue-se a inquirição de testemunhas e recolha de informações de pessoas que facilitem a descoberta do agente do crime e a sua reconstituição, nomeadamente a descoberta e a conservação de meios de prova que poderiam perder-se antes da intervenção da Autoridade Judiciária (artigos 249.º, n.º 2, alínea b), e 250.º, n.º 8, do Código de Processo Penal), a que se seguirá a identificação do suspeito (artigo 250.º, n.ºs 1 a 7 e n.º 9, do Código de Processo Penal) e colheita de informação (artigo 249.º, n.º 2, alínea b), do mesmo diploma legal). Deverá ser solicitado à instituição de crédito informações sobre quais os locais onde foi utilizado o cartão, se foi utilizado a crédito ou a débito e qual o montante utilizado.

Caso o abuso de cartão de crédito seja levado a cabo através da utilização de meio de sistema informático, importará ter em conta, entre outros, os artigos 12.º e 14.º, da Lei n.º 109/2009, de 15/09 (Lei do Cibercrime)[84]. Os mesmos regulam, respectivamente, a preservação expedita de dado e a forma de obtenção de dados informáticos armazenados num determinado sistema informático, atribuindo-lhe a designação de "injunção" e cominando o incumprimento com o crime de desobediência (artigo 348.º, n.º 1, alínea a), do Código Penal). Estabelecem os n.ºs 1 e 4 do referido artigo 14.º que o pedido para a revelação dos dados é formulado pela autoridade judiciária competente (portanto, o Ministério Público na fase de inquérito e o juiz nas restantes) e é dirigido a quem tenha a disponibilidade ou o controlo desses dados, o que, por norma, corresponde aos fornecedores do serviço de Internet[85], devendo o pedido identificar claramente os dados pretendidos (n.º 2, do citado artigo).

Na investigação de um crime de abuso de cartão de crédito com recurso à internet poderá ser necessário o conhecimento do respectivo *Internet Protocol Address* (IP)[86], de forma a se tentar identificar o agente[87]. É certo que a identificação do endereço IP não conduz ao autor do crime, mas apenas ao cliente que contratou o serviço de internet, cuja ligação gerou esse

[84] A Lei do Cibercrime permite a utilização de vários instrumentos processuais que permitem a recolha de prova em ambiente digital, designadamente, as que se encontram plasmadas nos Capítulos III e IV, nomeadamente, a preservação expedita de dados (artigos 12.º e 22.º), a revelação expedita de dados de tráfego (artigos 13.º e 22.º) a injunção para apresentação ou concessão do acesso a dados (artigo 14.º), a pesquisa e apreensão de dados informáticos (artigos 15.º, 16.º e 24.º), a apreensão de correio electrónico e registo de comunicações de natureza semelhante (artigo 17.º), a intercepção de comunicações (artigos 18.º e 26.º) e as acções encobertas (artigo 19.º). Os referidos instrumentos processuais (com excepção da intercepção de comunicações, prevista nos artigos 18.º e 26.º e das acções encobertas, e no artigo 19.º), aplicam-se, nos termos do artigo 11.º, aos crimes previstos na Lei do Cibercrime, aos crimes cometidos por meio de um sistema informático ou em relação aos quais seja necessário proceder à recolha de prova em suporte electrónico.

[85] "*Fornecedor de serviço*" é "*qualquer entidade, pública ou privada, que faculte aos utilizadores dos seus serviços a possibilidade de comunicar por meio de um sistema informático, bem como qualquer outra entidade que trate ou armazene dados informáticos em nome e por conta daquela entidade fornecedora de serviço ou dos respetivos utilizadores*" – artigo 2.º, alínea d), da Lei do Cibercrime.

[86] O IP é um dado de base: "*qualquer número de acesso*" (artigo 14.º, n.º 1, alínea b), da Lei do Cibercrime), que pode ser pedido através do procedimento da injunção.

[87] Estando apenas em causa a obtenção da identificação de um utilizador de um endereço IP ou o número de IP usado por um determinado indivíduo, em circunstâncias temporais determinadas, a competência para a respectiva obtenção é do Ministério Público – cfr. Acórdão do Tribunal da Relação de Lisboa, proc. 1695/09.5PJLSB.L1-9, de 19/06/2014.
Em igual sentido *vide* Nota prática n.º 2/2013 do Gabinete de Cibercrime da Procuradoria-Geral da República, "*A obtenção do endereço IP – súmula de jurisprudência*".

endereço. Apesar disso, será sempre um primeiro passo investigatório que poderá apontar no sentido da descoberta da identidade do criminoso[88].

Podem surgir várias dificuldades na investigação, entre as quais o conhecimento tardio do crime e a recolha de prova se revelar já difícil ou impossível; a prova recolhida sobre a identidade do agente do crime ser insuficiente ou contraditória; a pouca e/ou lenta colaboração com a investigação por parte das instituições de crédito e dos estabelecimentos comerciais onde o mesmo foi utilizado, ou até dos prestadores de serviço de Internet, através dos quais o cartão de crédito foi utilizado.

1.4. O Encerramento do inquérito

1.4.1. A aplicação das medidas de oportunidade e consenso

Ao invés da clássica acusação poderá lançar-se mão dos instrumentos de celeridade, simplificação, oportunidade, consenso ou de mera concordância no processo penal, os quais deverão ser aplicados no tratamento da pequena e média criminalidade[89].

A aplicação da suspensão provisória do processo[90] e do processo sumaríssimo depende da verificação dos respectivos requisitos para que tal seja possível, desde logo no que diz respeito à moldura penal, visto que o crime não pode ser punível com pena de prisão superior a cinco anos (artigos 281.º, n.º 1, e 392.º, n.º 1, do Código de Processo Penal).

Assim, a suspensão provisória do processo e o processo sumaríssimo poderão ser utilizados nas situações previstas no artigo 225.º, n.ºs 1 e 5, alínea a), do Código Penal, já que são puníveis, respectivamente, com pena de prisão até 3 anos ou com pena de multa, e com pena de prisão até 5 anos ou com pena de multa até 600 dias.

---

[88] No caso de o fornecedor do serviço a quem se dirige a injunção para a obtenção de qualquer dado de base ser uma das empresas operadoras de telecomunicações a operar em Portugal, devem ser utilizados os formulários acordados entre aquelas empresas e a PGR, por força do disposto na Circular n.º 12/2012, de 25/09, da PGR. Quando o operador é internacional, o pedido de informação é efectuado através do pedido de cooperação judiciária internacional, carta rogatória a encaminhar pela PGR (Lei da Cooperação Judiciária Internacional em Matéria Penal, mormente artigos 21.º, 145.º e ss., que regulam o auxílio judiciário mútuo em matéria penal), ou poderão ser dirigidos directamente pelo Magistrado do Ministério Público ao fornecedor de serviço, através do envio do formulário respectivo preenchido e assinado, face aos protocolos celebrados pela PGR com as entidades a quem se dirigem o maior número de solicitações (Microsoft e seus serviços associados, Hotmail, Outlook), Google (Gmail), entre outros. Estes formulários estão disponíveis no SIMP, bem como os contactos a utilizar e as informações específicas que cada fornecedor disponibiliza através desta via. – cfr. Notas práticas n.ºs 3 e 4/2014 do Gabinete de Cibercrime da Procuradoria-Geral da República, "*Pedidos de informação à Google, à Facebook e à Microsoft – experiência prática*".

[89] Cfr. Directiva n.º 1/2014, de 15/01/2014, da PGR, alterada pela Directiva n.º 1/15 de 30/04/2015 da PGR, segundo a qual "*1) Os magistrados do Ministério Público devem optar, no tratamento da pequena e média criminalidade, pelas soluções de consenso previstas na lei, entre as quais assume particular relevo a suspensão provisória do processo.".*

[90] A suspensão provisória do processo é um instituto processual que tem subjacente a ideia de consenso, oportunidade, não publicidade, ressocialização e diversão que permite que a tramitação do processo penal seja suspensa, sob condição de o arguido cumprir injunções e/ou regras de conduta, evitando a sujeição a acusação e a, eventual, julgamento potenciando a sua reintegração na sociedade. Com a aplicação de injunções e/ou regras de conduta afasta-se a ideia de impunidade, indesejável do ponto de vista da prevenção geral, e asseguram-se as funções equivalentes às da sanção penal típica, garantindo a prevenção especial.

Concretamente quanto à suspensão provisória do processo é, ainda, necessário que se verifiquem os demais requisitos, previstos no mencionado artigo 281.º, n.º 1, alíneas a) a f), do Código de Processo Penal[91]. Será, ainda, essencial que se inclua nas injunções a aplicar ao arguido a indemnização ao lesado(s) (artigo 281.º, n.º 2, alínea a), do Código de Processo Penal), sempre tendo em consideração se o juízo de oportunidade assegura os interesses públicos e privados em causa, uma vez que a imposição de injunções terá de satisfazer as expectativas da comunidade quanto à norma violada.

Concretamente quanto à necessidade de ausência de um grau de culpa elevado, será fulcral aferir, casuisticamente, qual o comportamento adoptado pelo arguido aquando da prática dos factos e, posteriormente, bem como valorar o prejuízo patrimonial, as consequências do crime, para daí se retirar qual o grau de ilicitude e de culpa do arguido. Ter-se-á em consideração o caso concreto e os critérios que se aplicam à determinação do grau de culpa para aplicação de uma pena (artigo 71.º, n.º 2, do Código Penal).

O processo sumaríssimo é uma das formas de processo especial, regulada nos artigos 392º a 398º, do Código de Processo Penal, e representa um mecanismo de simplificação, aceleração e consenso, quanto à pequena e média criminalidade, devendo ser equacionada a sua aplicação relativamente ao crime em análise. Reflexo desse mecanismo de consenso é a exigência, segundo a qual, para além da concordância do juiz, haja aceitação por parte do arguido em relação ao requerimento previsto no artigo 394.º e 395.º, do Código de Processo Penal[92].

1.4.2. O arquivamento e a acusação

Determina o artigo 276.º, do Código de Processo Penal, que "*o Ministério Público encerra o inquérito, arquivando-o ou deduzindo acusação [...]*.".

O inquérito é arquivado quando se tiver recolhido prova bastante de se não ter verificado crime, de o arguido não o ter praticado a qualquer título ou de ser legalmente inadmissível o procedimento, bem como quando não tiver sido possível ao Ministério Público obter indícios suficientes da verificação de crime ou de quem foram os agentes (artigo 277.º, n.ºs 1 e 2, do Código de Processo Penal).

[91] Como são a concordância do arguido e do assistente, a ausência de condenação anterior por crime da mesma natureza, a ausência de aplicação anterior de suspensão provisória de processo por crime da mesma natureza, não haver lugar a medida de segurança de internamento, ausência de um grau de culpa elevado e ser de prever que o cumprimento das injunções e regras de conduta responda suficientemente às exigências de prevenção que no caso se façam sentir.

[92] Tal notificação contém o requerimento do Ministério Público e concretiza o direito de o arguido se opor à sanção proposta e a forma de o fazer; a indicação do prazo para a oposição e o seu termo final; o esclarecimento dos efeitos da oposição e da não oposição. Em consequência dessa necessidade de aceitação do arguido criou-se um mecanismo de notificação pessoal daquele, apenas por contacto pessoal (artigo 396.º, n.º 2, do Código de Processo Penal), tendo em vista garantir um exercício consciente do direito de oposição e assegurar todas as garantias de defesa (artigo 32º, da Constituição da República Portuguesa).

De outro modo, se no decurso do inquérito tiverem sido recolhidos indícios suficientes, sempre que deles resultar uma possibilidade razoável de ao arguido vir a ser aplicada, por força deles, em julgamento, uma pena ou medida de segurança, de se ter verificado o crime e de quem foi o seu agente, o Ministério Público deduz acusação (artigo 283.º, n.º 1, do Código de Processo Penal).
Para que haja dedução de acusação, para além de se terem que verificar os elementos objectivos supra referidos, é necessário, também, que o elemento subjectivo se mostre preenchido, demonstrando-se o dolo.

É necessário, ainda, que se indique toda a prova obtida, mormente documental, pericial e testemunhal, de forma a que se consigam depoimentos directos de ordens dadas pelo arguido, ou das indicações dadas pelo titular do cartão ao utilizador do mesmo, ou que tenham presenciado os factos criminosos e relatem a sucessão de factos, e que sejam passíveis de demonstrar a utilização do cartão, respectivos montantes e locais onde foi usado.
No que concerne à prova documental poderão ser fundamentais os registos fotográficos e de videovigilância, talões de pagamento, condições contratuais, listagens de valores utilizados e locais de utilização do cartão, entre outros elementos apurados caso a caso, que serão essenciais para sustentar a acusação em julgamento. As testemunhas poderão ser confrontadas com tais elementos probatórios, o que se poderá revelar fundamental para a boa produção de prova.

A presença em julgamento dos peritos poderá ser necessária para responderem a pedidos de esclarecimentos dos relatórios periciais, por si elaborados.

Caso a investigação tenha sido levada a cabo pelo Polícia Judiciária, o Ministério Público comunica, pelo meio considerado mais adequado, o teor do despacho de encerramento dos inquéritos ao departamento da Polícia Judiciária que realizou a investigação, nos casos previstos nos artigos 4.º (competência reservada) e 5.º, n.º 2 (competência deferida), por força do disposto no ponto 1 da Circular n.º 4/2008, de 06/03/2008, da PGR[93].

IV. Hiperligações e referências bibliográficas

Hiperligações

http://www.dgsi.pt/;
http://www.ministeriopublico.pt/;
http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?artigo_id=109A0225&nid=109&tabela=leis&pagina=1&ficha=1&nversao=;
https://www.bportugal.pt/.

Referências bibliográficas

[93] A comunicação de despachos de arquivamento é efectuada após o decurso do prazo previsto no artigo 278.º, do Código de Processo Penal, e a a comunicação de despachos de acusação é efectuada após as notificações previstas no artigo 283.º, n.º 5, do Código de Processo Penal (*vide* pontos 2 e 3 da referida Circular).

AA. VV. – Comentário Conimbricense do Código Penal – Parte Especial, Tomo II, Coimbra, Coimbra Editora, 1999;

Cadernos do Banco de Portugal, n.º 6, Cartões Bancários, disponível em http://www.bbs.pt/publicacoes/BancodePortugal/BP6-CartoesBancarios.pdf;

ALBUQUERQUE, Paulo Pinto de, Comentário do Código Penal à luz da Constituição da República e da Convenção Europeia dos Direito do Homem, 3.ª ed. actualizada, Lisboa, Universidade Católica Editora, 2015;

BARREIROS, José António, Crimes contra o património, Lisboa, Lisboa: Universidade Lusíada, 1996;
BELEZA, Teresa Pizarro, e PINTO, Frederico Lacerda da Costa, *in* "*A tutela penal do património após a revisão do código penal de 1995*", Lisboa, Associação Académica da Faculdade de Direito de Lisboa, 1998;

Código Penal, Actas e Projecto da Comissão de Revisão, Rei dos Livros, 1993;

CORDEIRO, António Menezes, Manual de Direito Bancário, 3ª Edição, Coimbra, Almedina, 2006;

HENRIQUES, Manuel de Oliveira Leal e SANTOS, Manuel José Carrilho de Simas, Código Penal Anotado, 3.ª Ed., II Vol., Rei dos Livros, 2000;

PEREIRA, Sá, e LAFAYETTE, Alexandre, Código Penal Anotado e Comentado, Legislação Conexa e Complementar, Quid Juris, Sociedade Editora, 2014;

SANTOS, António Carlos dos, GONÇALVES, Maria Eduarda, MARQUES, Maria Manuel Leitão, Direito Económico, 7.ª edição, Almedina, 2014;

SILVA, Germano Marques da, Direito Penal Português - Teoria do Crime, Lisboa, Universidade Católica Portuguesa Editora, 2015;

VASCONCELOS, Joana de, *in* Revista de Direito e de Estudos Sociais, Coimbra, Outubro-Dezembro 1992.

Aviso do Banco de Portugal, n.º 11/2001, que define cartões de crédito e de débito, e as condições de utilização destes instrumentos de pagamento, pág. 1, disponível em https://www.bportugal.pt/sites/default/files/anexos/cartas-circulares/11-2001a.pdf;

Nota prática n.º 2/2013 do Gabinete de Cibercrime da Procuradoria-Geral da República, "*A obtenção do endereço IP – súmula de jurisprudência*", disponível em http://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/nota_pratica_2_jurispridencia_sobre_ip.pdf;

Directiva n.º 1/2014, de 15/01/2014, da PGR, alterada pela Directiva n.º 1/15 de 30/04/2015 da PGR, disponível em
https://simp.pgr.pt/circulares/mount/files/1389784021_directiva_1_2014.pdf;

Notas práticas n.ºs 3 e 4/2014 do Gabinete de Cibercrime da Procuradoria-Geral da República, "*Pedidos de informação à Google, à Facebook e à Microsoft – experiência prática*", disponíveis em:http://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/nota_pratica_3_isp_eua.pdf
e http://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/nota_pratica_4_pedidos_a_isp_eua.pdf.

9.
Crime de abuso de cartão de garantia ou de crédito. Enquadramento jurídico, prática e gestão processual

Rui Miguel Lima Alves (Norte)

Nuno Filipe de Sousa Gonçalves (Centro)

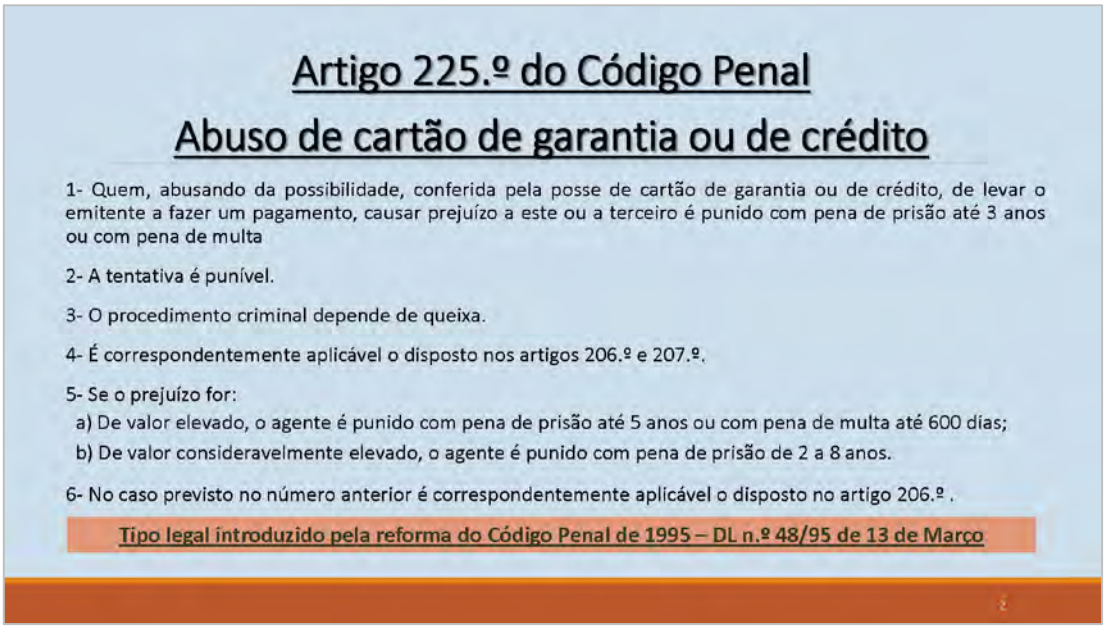
Maria José Clara Sousa (Lisboa)

Rui Miguel Ferreira dos Santos Cruz (Sul)

CENTRO
DE ESTUDOS
JUDICIÁRIOS

9. O CRIME DE ABUSO DE CARTÃO DE GARANTIA OU DE CRÉDITO. ENQUADRAMENTO JURÍDICO, PRÁTICA E GESTÃO PROCESSUAL

Rui Miguel Lima Alves (Norte)
Nuno Filipe de Sousa Gonçalves (Centro)
Maria José Clara Sousa (Lisboa)
Rui Miguel Ferreira dos Santos Cruz (Sul)



- Tal introdução não foi pacífica, porque se levantavam dúvidas sobre a dignidade penal destas condutas, já que as mesmas resultam do facto de se violarem regras contratuais (as quais estão subjacentes à emissão dos próprios cartões), tratando-se, portanto, de uma responsabilização penal por obrigações civis.
- Mas a justificação para tal introdução, aponta, todavia, para outro sentido, que é o de que em causa está um abuso de uma relação de confiança que é concedida ao agente e que tem como escopo causar um empobrecimento no património alheio.
- Teve como objetivo colmatar uma lacuna de punibilidade, uma vez que a conduta do titular do cartão de garantia ou de crédito que o utilizasse conhecendo a sua impossibilidade de pagamento, era atípica.
- Quanto ao terceiro que utilizava um cartão de outrem sem a devida autorização, já era punível pelo crime de burla, nos termos do Artº. 217º do Código Penal, se o enganado fosse uma pessoa, ou pelo crime de burla informática, nos termos do Artº. 221º do mesmo diploma legal, se fosse cometido através de manipulação informática.

3

Fonte

§ 266b, do Código Penal alemão (Missbrauch von Scheck- und Kreditkarten), introduzida em 1986

A previsão legal do Código Penal português é mais abrangente, já que, para além das condutas de abuso praticadas pelos titulares do cartão, previstas naquele ordenamento jurídico, inclui a responsabilização criminal de terceiros que usem um cartão de garantia ou de crédito de outrem, prevendo-se agravações em função do valor.

4

Cartão de garantia - é um cartão destinado a garantir, até um determinado montante, cheques que foram validados por um comerciante, quer com base num cartão emitido ao titular do cheque ou através de uma base de dados central, à qual os comerciantes têm acesso. Os cheques validados são garantidos pela entidade emissora do cartão de garantia, o banco sacado ou pelo operador do sistema. Este cartão pode acumular outras funções, como, por exemplo, a de cartão de caixa ou de cartão de débito.

Cartão de crédito - é um cartão que indica que foi concedida uma linha de crédito ao seu titular, permitindo-lhe efectuar compras e/ou levantar dinheiro ("cash-advance") até um limite acordado previamente; o crédito concedido pode ser liquidado na sua totalidade no final de um período específico ou pode ser liquidado parcialmente, sendo o saldo considerado como uma extensão do crédito. São cobrados juros sobre o montante de qualquer extensão do crédito e, por vezes, é cobrada uma comissão anual ao respectivo titular.

Há, por isso, que fazer a distinção entre cartões de crédito e cartões de débito. Enquanto o primeiro difere o pagamento no tempo, o segundo implica um débito directo na conta do titular.

Estamos, assim, perante um tipo criminal que pune a utilização abusiva de um cartão de crédito, desde que o mesmo seja utilizado no âmbito da sua real função, ou seja, aquela para a qual foi emitido.

E a utilização deste cartão de crédito tanto poderá ser física como em ambiente digital.

O **bem jurídico** tutelado por esta incriminação é o património de outra pessoa. O património inclui, numa conceção jurídico-económica, todos os direitos, as posições jurídicas e as expetativas com valor económico compatíveis com a ordem jurídica. Podemos ainda acrescentar que paralelamente, também o crédito em geral e a confiança que merecem os cartões como meios de pagamento são aqui acessoriamente defendidas.

Elementos objetivos:

- O abuso da possibilidade conferida pela posse do cartão de garantia ou de crédito

- Leve o emitente a fazer um pagamento

- Causando prejuízo a este ou a terceiro

7

Elementos subjetivos

Só admite o dolo (em qualquer das suas modalidades)

- Elemento volitivo

- Elemento cognitivo:

– é necessário que se encontrem reunidos:

- representação do abuso

- representação do prejuízo

8

A Pena e o Regime Punitivo

A Moldura Penal

- O crime de abuso de cartão de garantia ou de crédito é punido consoante o montante do prejuízo,
- Existem duas agravações em razão do valor (valor elevado e consideravelmente elevado).
- Dispõe o artigo 202.º, alíneas a) e b), do Código Penal, que:
- "***a) Valor elevado***: *aquele que exceder 50 unidades de conta avaliadas no momento da prática do facto*" **+ de € 5.100,00**
- ***"b) Valor consideravelmente elevado***: *aquele que exceder 200 unidades de conta avaliadas no momento da prática do facto.".* **+ de € 20.400,00**

9

A Pena e o Regime Punitivo

- Se o **prejuízo for inferior ao valor elevado**, o agente é punido com **pena de prisão até 3 anos ou com pena de multa** (artigo 225.º, n.º 1, do Código Penal);
- Se o **prejuízo for de valor elevado** (superior a € 5.100,00) e **inferior ao valor consideravelmente elevado** (superior a € 20.400,00), o agente é punido com **pena de prisão até 5 anos ou com pena de multa até 600 dias** (artigo 225.º, n.º 5, alínea a), do Código Penal);
- Já se o **prejuízo for de valor consideravelmente elevado**, o agente é punido com **pena de prisão de 2 a 8 anos** (artigo 225.º, n.º 5, alínea b), do Código Penal).

10

A atenuação especial da pena e a extinção da responsabilidade criminal

Artigo 225º, nº.4 do Código Penal

É correspondentemente aplicável o disposto nos artigos 206.º e 207.º do Código Penal.

- **Atenuação especial da pena** por força da aplicação do artigos. 206º, nº.2 do Código Penal, se houver restituição ou reparação. Tal atenuação, é aplicável ao crime simples (nº.4), bem como aos crimes agravados (nº.6). Funciona, por isso, em conexão com os artigos 72º e 73º do Código Penal.

- **Extinção da responsabilidade criminal**, por força do seu nº.1 daquele preceito.

Causas de exclusão da ilicitude e da culpa

Para que se possa afirmar que o agente verdadeiramente cometeu um crime, é necessário a verificação do preenchimento dos pressupostos da ilicitude e da culpa, ou seja, para que um facto seja punível, para além de ser necessariamente típico, terá que ser ainda ilícito e culposo.

Quer isto dizer e, desde logo, no que concerne ao pressuposto da ilicitude - que consiste na desconformidade da conduta com o direito ou lesão de interesses juridicamente protegidos -, ser necessário verificar se existe alguma causa de justificação ou de exclusão da ilicitude.

Causas de exclusão da ilicitude e da culpa

Por seu lado, a culpa, enquanto elemento do crime - que assenta na capacidade do agente em avaliar a ilicitude no momento da prática do facto ou de se determinar de acordo com essa avaliação e se traduz num juízo de censurabilidade dirigido ao agente por ter actuado daquela forma -, é um pressuposto indispensável à aplicação de uma pena, pois não basta que o agente tenha praticado um facto ilícito-típico para que lhe seja aplicável uma pena, é necessário ainda que tenha agido com culpa.

Causas de exclusão da ilicitude e da culpa

A declaração de inimputabilidade exclui a culpa do agente e, portanto, a possibilidade de lhe ser aplicada uma pena. Porém, essa circunstância não afasta a possibilidade de ser aplicado uma medida de segurança sempre que aquele for considerado perigoso – ou seja, **houver fundado receio de que venha a cometer outros factos da mesma espécie** - (cfr. artigos 20.º, n.º 1 e 91.º, n.º 1 do Código Penal).

A culpa tem assim como função político-criminal a limitação do intervencionismo estatal, impedindo que, numa situação em que o agente pratica um facto ilícito-típico não censurável, o Estado lhe aplique uma pena.

Causas de exclusão da ilicitude e da culpa

Por isso, a determinação da medida da pena, dentro dos limites definidos na lei, é sempre feita em função da culpa do agente, tendo em conta as exigências de prevenção, nos termos do artigo 71.º, n.º 1 do Código Penal e bem assim o disposto no artigo 40.°, n.º 2 do mesmo diploma, atendendo-se a todas as circunstâncias que, não fazendo parte do tipo, depuserem a favor do agente ou contra ele, conforme também dispõe o n.º 2 do referido artigo 71°.

Sobre o tema Damião da Cunha afirma serem de aplicar as regras gerais das causas de exclusão da ilicitude e da culpa, incluindo o direito de necessidade, bem como hipóteses de actuação com base num estado de necessidade desculpante.

15

Causas de exclusão da ilicitude e da culpa

Todavia, para que assim seja, o agente tem de conhecer os elementos do tipo justificador e, em alguns casos, exige-se ainda que o agente tenha actuado com uma certa direcção de vontade.

Nos casos em que o agente actua numa situação objectiva de justificação sem que dela tenha conhecimento, deverá ser punido a título de tentativa. Nos casos inversos, em que o agente configura de forma errada estar numa situação objectiva de exclusão ou justificação quando na verdade não está, este deverá ser punido a título de negligência caso o seu erro pudesse ter sido evitado através de uma cuidadosa comprovação da situação justificadora. Caso contrário o seu erro é em si mesmo uma causa de exclusão (cfr. artigo 16.º, n.º 2 e 3 do Código Penal).

16

Tentativa

A tentativa é punível, por força do disposto nos artigos 225.º, n.º 2, e 23.º, n.º 1, do Código Penal, com a pena aplicável ao crime consumado, mas especialmente atenuada nos termos do disposto nos artigos 72.º e 73.º do mesmo diploma.

A punibilidade da tentativa não estava inicialmente pensada pela Comissão Revisora do Código Penal de 1995, tendo sido acrescentada mediante proposta do Professor Doutor Figueiredo Dias, uma vez que o regime de punição criado para o abuso de cartão de garantia e de crédito era semelhante ao do crime de burla.

17

Tentativa

Tendo em atenção a segurança (informática) inerente ao uso de cartões de garantia ou de crédito, é natural que possam ocorrer situações em que o agente queira usar (abusivamente) o cartão, sem conseguir no entanto a produção do resultado, por motivos alheios à sua vontade, ficando-se assim apenas pela tentativa.

A tentativa só não é punível quando for manifesta a inaptidão do meio empregado pelo agente ou a inexistência do objecto essencial à consumação do crime - tentativa impossível ou inidónea - (cfr. artigo 23.º, n.º 3 do Código Penal).

18

Comparticipação

A comparticipação na consumação deste crime, porque se trata de um crime comum que pode ser praticado por qualquer pessoa, rege-se pelas regras gerais previstas no artigo 26º do Código Penal.

Aplicam-se, por isso, os regimes dos artigos 25.º e 28.º do mesmo diploma.

Como tal, se um dos comparticipantes decidir desistir da tentativa, tal tentativa não é punível se o mesmo voluntariamente impedir a consumação ou que se esforce seriamente para que tal não aconteça. Também no caso de a ilicitude ou grau da ilicitude do facto dependerem de certas qualidades ou relações especiais do agente, tal comunica-se aos demais.

19

Crime continuado

O crime continuado encontra-se previsto no artigo 30.º, n.º 2, do Código Penal, segundo o qual:

"*2 — Constitui um só crime continuado a realização plúrima do mesmo tipo de crime ou de vários tipos de crime que fundamentalmente protejam o mesmo bem jurídico, executada por forma essencialmente homogénea e no quadro da solicitação de uma mesma situação exterior que diminua consideravelmente a culpa do agente.*"

20

Crime continuado

Constituem-se assim, como pressupostos da ocorrência de crime continuado:

a) A realização plúrima do mesmo tipo de crime ou de vários tipos que protejam fundamentalmente o mesmo bem jurídico.

b) A homogeneidade da forma de execução.

c) A persistência de uma "situação exterior" que facilita a execução e que diminui consideravelmente a culpa do agente.

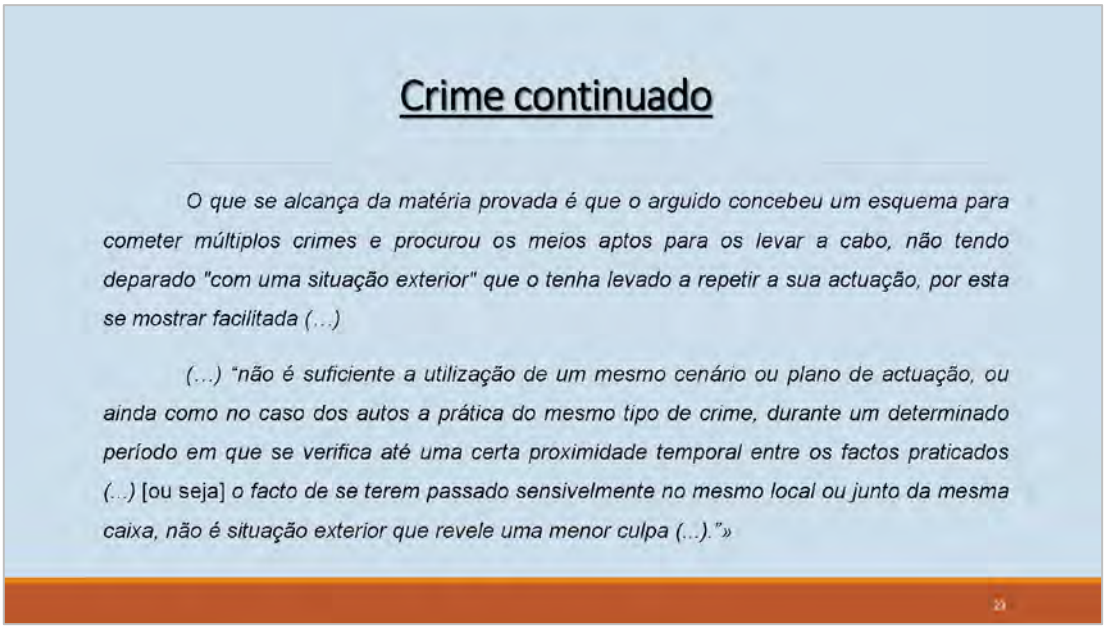
21

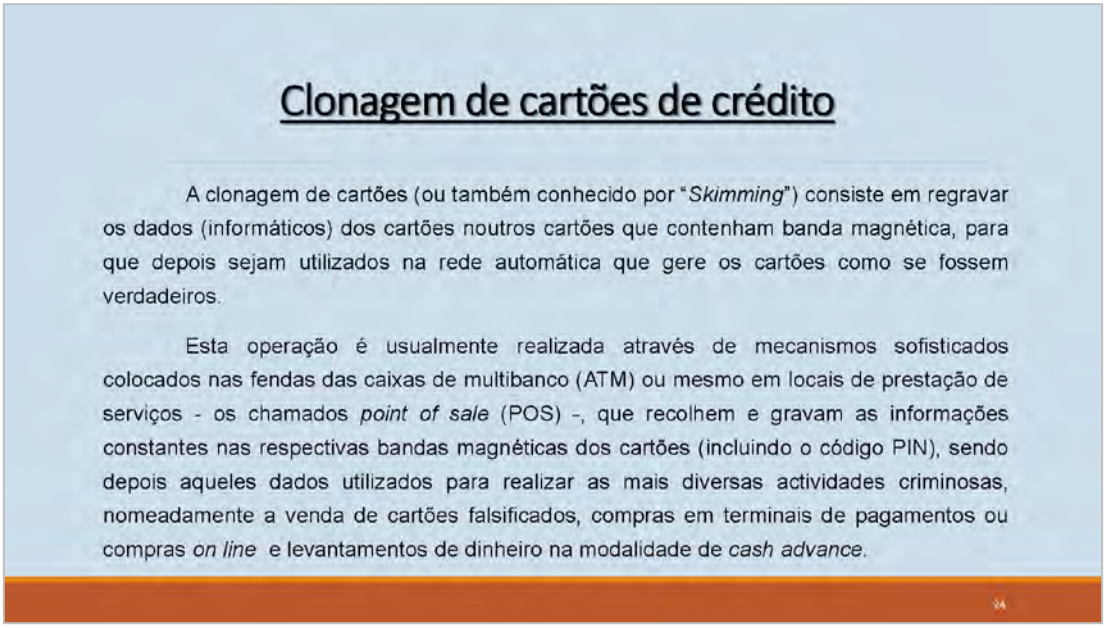
Crime continuado

Segundo o Acórdão do STJ de 20/10/2010, proc. n.º 78/07.6JAFAR.E2.S1, relatado por Pires da Graça, relativo à utilização de cartões de crédito falsificados em operações de levantamento de dinheiro em caixas multibanco (ATM), e onde se discutia a prática do crime de burla informática, na forma continuada, este afastou essa continuação, dizendo:

«Da matéria de facto provada não resulta, efectivamente, configurada a actuação do arguido no "quadro da solicitação de uma mesma situação exterior", que lhe tenha propiciado e facilitado a repetição das suas acções.

22


Crime continuado
O que se alcança da matéria provada é que o arguido concebeu um esquema para cometer múltiplos crimes e procurou os meios aptos para os levar a cabo, não tendo deparado "com uma situação exterior" que o tenha levado a repetir a sua actuação, por esta se mostrar facilitada (…)
(…) "não é suficiente a utilização de um mesmo cenário ou plano de actuação, ou ainda como no caso dos autos a prática do mesmo tipo de crime, durante um determinado período em que se verifica até uma certa proximidade temporal entre os factos praticados (…) [ou seja] o facto de se terem passado sensivelmente no mesmo local ou junto da mesma caixa, não é situação exterior que revele uma menor culpa (…)."»


Clonagem de cartões de crédito
A clonagem de cartões (ou também conhecido por "Skimming") consiste em regravar os dados (informáticos) dos cartões noutros cartões que contenham banda magnética, para que depois sejam utilizados na rede automática que gere os cartões como se fossem verdadeiros.
Esta operação é usualmente realizada através de mecanismos sofisticados colocados nas fendas das caixas de multibanco (ATM) ou mesmo em locais de prestação de serviços - os chamados point of sale (POS) -, que recolhem e gravam as informações constantes nas respectivas bandas magnéticas dos cartões (incluindo o código PIN), sendo depois aqueles dados utilizados para realizar as mais diversas actividades criminosas, nomeadamente a venda de cartões falsificados, compras em terminais de pagamentos ou compras on line e levantamentos de dinheiro na modalidade de cash advance.

Clonagem de cartões de crédito

A captura da informação existente na banda magnética de cartão de crédito constitui a prática do crime de falsidade informática, p. e p. pelo artigo 3.º n.ºs 1 e 2 da Lei n.º 109/2009, de 15 de Setembro (Lei do Cibercrime), que diz:

"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" – **Cfr. Ac. do TRP de 17.04.2014, proc. n.º 2013/13.3JAPRT.P1, relatado por Coelho Vieira.**

25

Clonagem de cartões de crédito

A falsificação de cartão em si mesmo, ou seja, o fabrico de cartão de crédito falso com inserção de banda magnética clonada de um cartão verdadeiro, constitui a prática do crime de contrafacção de moeda falsa, p. e p. pelas disposições conjugadas dos artigos 262.º, n.º 1 e 267.º, n.º 1, al.ª a), do Código Penal, que dizem:

"1 - Quem praticar contrafacção de moeda, com intenção de a pôr em circulação como legítima, é punido com pena de prisão de três a doze anos", e *"1 - Para efeitos do disposto nos artigos 262.º a 266.º, são equiparados a moeda: (...) c) Os cartões de garantia ou de crédito"* - **Cfr. Ac. do TRP de 17.04.2014, proc. n.º 2013/13.3JAPRT.P1, relatado por Coelho Vieira.**

26

Clonagem de cartões de crédito

Já a utilização destes "cartões" falsificados por pessoas não autorizadas, com a introdução do código PIN ou com a introdução do número de cartão de crédito em transacções *on line*, constitui a prática do crime de burla informática, p. e p. pelo artigo 221.º, n.º 1 do Código Penal, que diz:

"1 - Quem, com intenção de obter para si ou para terceiro enriquecimento ilegítimo, causar a outra pessoa prejuízo patrimonial, interferindo no resultado de tratamento de dados ou mediante estruturação incorrecta de programa informático, utilização incorrecta ou incompleta de dados, utilização de dados sem autorização ou intervenção por qualquer outro modo não autorizada no processamento, é punido com pena de prisão até 3 anos ou com pena de multa".

27

Clonagem de cartões de crédito

Por seu lado, sendo os cartões de crédito equiparados a moeda previsto pelo artigo 267.º, n.º 1, al.ª c) do Código Penal, a venda destes "cartões" falsificados constitui a prática do crime de passagem de moeda falsa de concerto com o falsificador, p. e p. pelo artigo 264.º do Código Penal, que diz:

"1 - Nas penas indicadas nos artigos 262.º e 263.º incorre quem, concertando-se com o agente dos factos neles descritos, passar ou puser em circulação por qualquer modo, incluindo a exposição à venda, as ditas moedas" - **Cfr. Ac. do STJ de 12.09.2012, proc. n.º 1008/11.6JFLSB-L1.S1, relatado por Armindo Monteiro**.

28

Clonagem de cartões de crédito

Aos quais pode acrescer ainda o crime de falsificação de documento, nos termos do disposto no artigo 256.º, n.º 1, al.ª c), do Código Penal, quando haja lugar à utilização do cartão "falso" com recurso à assinatura em talão de pagamento por terceiro não autorizado, como se fosse o seu legítimo titular. Com efeito, em certos terminais automáticos de pagamento, para além da introdução do código PIN, é ainda emitido um talão com os dados da operação que deve ser assinado pelo apresentante do cartão e corresponder ao seu titular – **Cfr. Ac. do TRL de 10.07.2012, proc. n.º 7876/10.1JFLSB.L1-5, relatado por Luís Gominho**.

29

O Concurso
Crimes Conexos

- Artigo 30.º, n.º 1, do Código Penal prevê que: "*O número de crimes determina-se pelo número de tipos de crime efectivamente cometidos, ou pelo número de vezes que o mesmo tipo de crime for preenchido pela conduta do agente.*".

- Diversas possibilidades de obtenção e utilização dos cartões de garantia e de crédito:
  - Leva a que a mesma conduta possa constituir a prática de vários crimes ou de várias vezes o mesmo crime.

30

Os Crimes de Abuso de cartão de garantia ou de crédito e de Burla

- O crime de burla levanta dúvidas face à relação e possibilidade de cometimento dos dois crimes - abuso de cartão de garantia ou de crédito e burla;
- A verificação de ambos os crimes;
- Relação de especialidade do crime de abuso de cartão de garantia ou de crédito em relação ao crime de burla;
- Exemplo:
  - agente utiliza o cartão de crédito (de mera assinatura), cujo montante máximo permitido ("*plafond*") se encontra ultrapassado;
  - disso tem conhecimento,
  - convence, através de algum logro ou artifício, o comerciante a aceitar o pagamento, sem obter a necessária autorização do emitente do cartão;

= Preenchimento dos dois tipos de crime (concurso aparente com o crime de abuso, o qual se aplica, por ser especial em relação à burla).

31

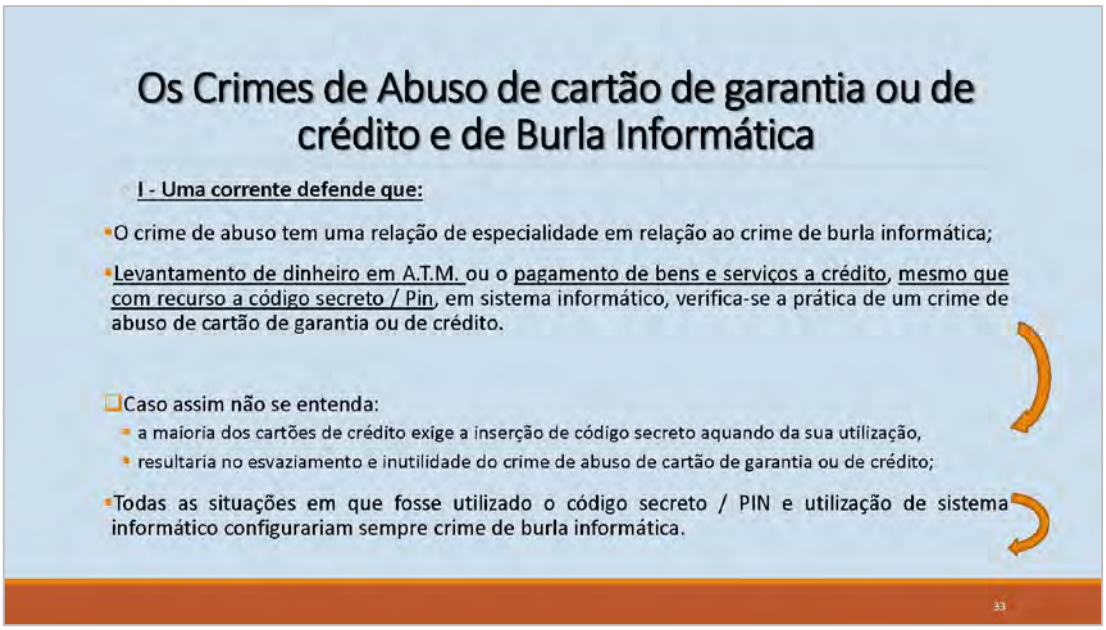
Os Crimes de Abuso de cartão de garantia ou de crédito e de Burla Informática

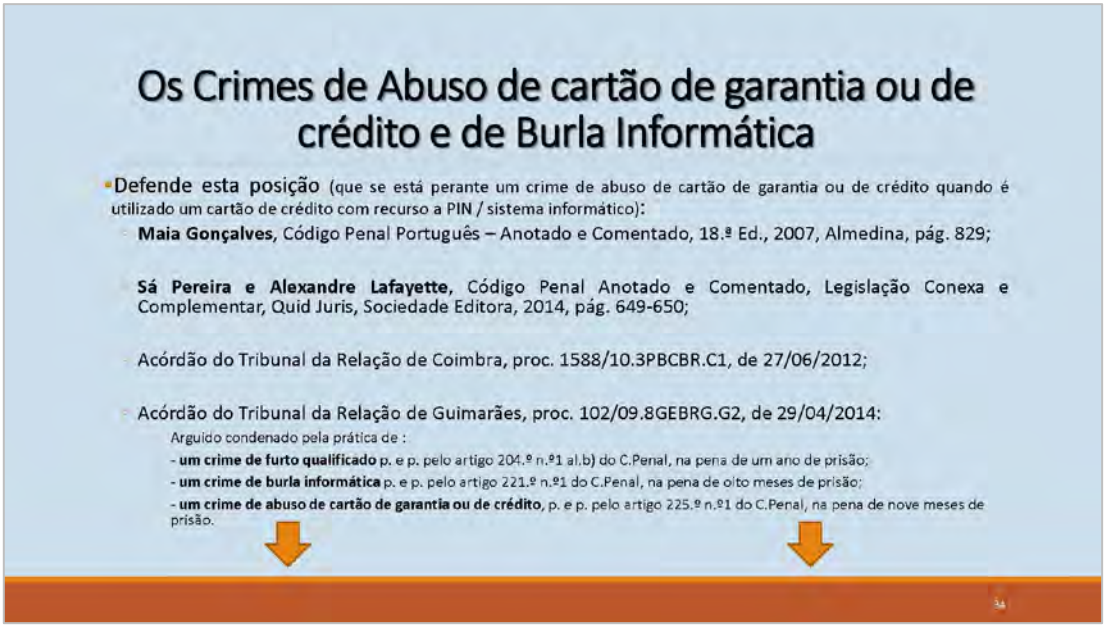
Situações em que se verifica a:

- Utilização de um cartão de crédito, como meio de pagamento de bens ou serviços ou levantamento de dinheiro, através da utilização do sistema informático das A.T.M.;
- Com a introdução do cartão e digitação do código secreto;
- Obtendo um enriquecimento ilegítimo (pagamento / levantamento);
- Causando um correspondente prejuízo patrimonial ao titular do cartão;

==» Verifica-se a prática de um crime de burla informática ou de abuso de cartão de garantia ou de crédito ?

32


Os Crimes de Abuso de cartão de garantia ou de crédito e de Burla Informática
I - Uma corrente defende que:
O crime de abuso tem uma relação de especialidade em relação ao crime de burla informática;
Levantamento de dinheiro em A.T.M. ou o pagamento de bens e serviços a crédito, mesmo que com recurso a código secreto / Pin, em sistema informático, verifica-se a prática de um crime de abuso de cartão de garantia ou de crédito.
Caso assim não se entenda:
a maioria dos cartões de crédito exige a inserção de código secreto aquando da sua utilização,
resultaria no esvaziamento e inutilidade do crime de abuso de cartão de garantia ou de crédito;
Todas as situações em que fosse utilizado o código secreto / PIN e utilização de sistema informático configurariam sempre crime de burla informática.
33


Os Crimes de Abuso de cartão de garantia ou de crédito e de Burla Informática
Defende esta posição (que se está perante um crime de abuso de cartão de garantia ou de crédito quando é utilizado um cartão de crédito com recurso a PIN / sistema informático):
Maia Gonçalves, Código Penal Português – Anotado e Comentado, 18.ª Ed., 2007, Almedina, pág. 829;
Sá Pereira e Alexandre Lafayette, Código Penal Anotado e Comentado, Legislação Conexa e Complementar, Quid Juris, Sociedade Editora, 2014, pág. 649-650;
Acórdão do Tribunal da Relação de Coimbra, proc. 1588/10.3PBCBR.C1, de 27/06/2012;
Acórdão do Tribunal da Relação de Guimarães, proc. 102/09.8GEBRG.G2, de 29/04/2014:
Arguido condenado pela prática de :
- um crime de furto qualificado p. e p. pelo artigo 204.º n.º1 al.b) do C.Penal, na pena de um ano de prisão;
- um crime de burla informática p. e p. pelo artigo 221.º n.º1 do C.Penal, na pena de oito meses de prisão;
- um crime de abuso de cartão de garantia ou de crédito, p. e p. pelo artigo 225.º n.º1 do C.Penal, na pena de nove meses de prisão.
34

Os Crimes de Abuso de cartão de garantia ou de crédito e de Burla Informática

- **Factos:**
  - Furto de carteira que se encontrava no interior de veículo automóvel estacionado em Braga,
  - A qual continha:
    - Um cartão de crédito
    - Um cartão de débito
    - *"Na **posse do cartão de débito** n.º 0258... e do seu código o arguido, o Albano e a Maria S... **dirigiram-se à ATM** do BPI, sita na Rua P...onde, após introduzirem o cartão do ofendido, **digitaram o código e levantaram** as quantias de 150€, 200€ e 50€ de que se apropriaram;*
    - *Na **posse do cartão de crédito** n.º 3389..., **na referida ATM** após introduzirem o cartão do ofendido, **digitaram o código e levantaram as quantias** de 200€ e 200€ de que se apropriaram"*
    - Posteriormente deslocaram-se a vários estabelecimentos comerciais (Worten, Nike, Levi's) e adquiriam telemóveis, peças de vestuário, sapatilhas, **com recurso ao cartão de crédito (digitando o código secreto / Pin).**

35

Os Crimes de Abuso de cartão de garantia ou de crédito e de Burla Informática

II – Outra corrente defende que: ≠

- A utilização do cartão de crédito desde que efectuada com recurso a código secreto/Pin e/ou com recurso a sistema informático, configura um crime de burla informática e não de abuso de cartão de garantia ou de crédito:
  - **Damião da Cunha**, Comentário Conimbricense do Código Penal, Tomo II, Coimbra Editora, 1999, pág. 379;
  - **Miguez Garcia, Castela Rio**, Código Penal - Parte geral e especial, Almedina, 2015, pág. 952;
  - **Paulo Pinto de Albuquerque**, Comentário do Código Penal à luz da CRP e da CEDH, 2015, pág. 873;
  - **Comissão de Revisão do Código Penal** parece ter pensado o crime de abuso de cartão de garantia ou de crédito somente quanto à utilização do cartão de crédito sem utilização de Pin; Se utilizado em sistemas automatizados de pagamento parece que esta conduta já integraria o crime de burla informática.
  - Acórdão do STJ, proc. n.º 01P1800, de 27/06/2001,
  - Acórdão do TRG, proc. n.º 541/10.1GAPTB.G1; TRE, proc. n.º 90/11.0GCLLE.E1, de 20/01/2015.

36

Os Crimes de Abuso de cartão de garantia ou de crédito e de Burla Informática

Acórdão do Supremo Tribunal de Justiça, proc. 06P1942, 20-09-2006- Rel. Henriques Gaspar:

"o crime de burla informática remete para a realização de actos e operações especificas de intromissão e interferência em programas ou utilização de dados nos quais está presente e aos quais está subjacente algum modo de engano, de fraude ou de artifício que tenha a finalidade, e através da qual se realiza a específica intenção, de obter enriquecimento ilegítimo, causando a outra pessoa prejuízo patrimonial.".

- Face à factualidade anteriormente referida: em que momento se verificou o engano, o artifício?
- Engano em relação ao emitente do cartão?
- Concurso aparente entre o crime de abuso de cartão de garantia ou de crédito e o crime de burla informática. (relação de especialidade daquele? Mesmo com utilização do PIN e sistema informático?).

37

O Crime de Contrafacção de Moeda

- O artigo 267.º, n.º 1, alínea c), do Código Penal, equipara os cartões de crédito a moeda:
- Quer isto significar que quem praticar a contrafacção (clonagem) de um cartão de crédito ("*Skimming*"), com intenção de o pôr em circulação como sendo legítimo
- será punido apenas pelo crime de contrafacção de moeda, previsto no artigo 262.º, n.º 1, com referência ao artigo 267.º, n.º 1, alínea c), ambos do Código Penal.
- Não há concurso de crimes.

38

Os Crimes de Contrafacção de Moeda e de Falsidade Informática

- Caso o cartão de crédito clonado seja utilizado e se verifique um prejuízo patrimonial para o emitente do cartão ou do seu titular estamos perante um concurso efectivo de crimes:

-» entre o crime de contrafacção de moeda, o crime de falsidade informática (artigo 3.º, n.ºs 1 e 2, da Lei n.º 109/2009, de 15/09 (Lei do Cibercrime) e o crime de burla informática (artigo 221.º, do Código Penal) e não de abuso de cartão de crédito ou de garantia.

- Tal acontece quando:

1. o agente consegue através de uma A.T.M. obter a informação existente na banda magnética de um cartão de crédito que aí foi inserido;
2. posteriormente a utiliza e insere tais dados informáticos num cartão por si fabricado;
3. o utiliza para efectuar levantamentos de dinheiro ou pagamento de bens ou serviços (ATM ou *online*).

39

Os Crimes de Contrafacção de Moeda e de Falsidade Informática

- Entre tais crimes existe concurso efectivo, uma vez que o bem jurídico protegido é:
  - contrafacção de moeda: a protecção da confiança e da fé pública na moeda e na autenticidade do sistema monetário;
  - burla informática: tutela-se o património;
  - falsidade informática: defende-se a integridade dos sistemas de informação.

Neste sentido:

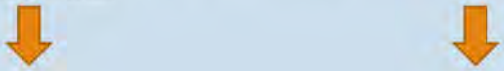
- Acórdão do Tribunal da Relação do Porto, proc. 2013/13.3JAPRT.P1, de 17/09/2014;

- Acórdãos do Tribunal da Relação de Lisboa, proc. 189/09.3JASTB.L1-5, de 30/06/2011, e 7876/10.1JFLSB.L1-5, de 10/07/2012.

40

Os Crimes de Contrafacção de Moeda, Falsidade informática e Passagem de moeda falsa de concerto com o falsificador

- Como os cartões de crédito são equiparados a moeda por força do artigo 267.º, n.º 1 alínea c), do Código Penal:



- A venda destes "cartões" falsificados constitui a prática do crime de passagem de moeda falsa de concerto com o falsificador.
- **Situação em que se verifica concurso efectivo de crimes:**
  - contrafacção de moeda;
  - falsidade informática;
  - burla informática;
  - passagem de moeda falsa de concerto com o falsificador.

41

Os Crimes de Contrafacção de Moeda, Falsidade informática, Passagem de moeda falsa de concerto com o falsificador e Falsificação de Documento

- A somar a isto, se:
  - o agente, ao efectuar o pagamento de bens ou serviços com recurso ao "*cartão de crédito adulterado/falsificado*" ou de um cartão de crédito não adulterado, mas furtado:
  - assinar o talão de pagamento ou exibir um documento de identificação por si fabricado, correspondente ao titular do cartão de crédito.

- Configura, para além dos ilícitos supra referidos, a prática de, em concurso efectivo, um crime de falsificação ou contrafacção de documento (artigo 256.º, n.º 1, alínea a), do Código Penal).
- Neste sentido: Acórdão do Tribunal da Relação de Lisboa, proc. 7876/10.1JFLSB.L1-5, de 10/07/2012; CUNHA, J. M. Damião da, ob. cit., pág. 382.

42

Os Crimes de Abuso de Cartão de Garantia ou de Crédito, Burla Informática e Furto.

- Possibilidade de o cartão de crédito (não clonado) ser subtraído ao seu titular e, posteriormente, utilizado para levantar dinheiro em caixa de A.T.M. ou para pagamento de bens ou serviços:

- o que **consubstanciará a prática, em concurso efectivo, de**:

- Um crime de furto (artigo 203.º, do Código Penal),

- Um crime de abuso de cartão de garantia ou de crédito, se o levantamento / pagamento for a crédito, **OU** de burla informática (artigo 221.º, do Código Penal), se o levantamento / pagamento for a débito
  - (**OU** sempre de burla informática seguindo a 2.ª tese (crédito ou débito / sistema informático).

Os crimes de abuso de cartão de garantia ou de crédito e de emissão de cheque sem provisão

- Pode existir concurso efectivo entre o crime de abuso de cartão de garantia ou de crédito com o crime de emissão de cheque sem provisão (artigo 11.º, do Decreto-Lei n.º 454/91, de 28/12):

- Exemplo:
  - titular do cartão de garantia emite um cheque, de acordo com o valor da garantia que o banco assumiu,
  - mas que já se encontra ultrapassada e se verificam os demais requisitos previstos no referido artigo 11.º (falta de provisão).

O Procedimento Criminal

- O artigo 225.º, n.º 3, do Código Penal, estabelece que o **procedimento criminal depende de queixa**.
- Tem **legitimidade para apresentar queixa** quem for prejudicado pelo abuso do cartão, considerando-se como tal o titular dos interesses que a Lei especialmente quis proteger com a incriminação (artigo 113.º, n.º 1, do Código Penal).
  - os lesados pela conduta abusiva: o titular do cartão, o emitente do cartão ou o comerciante, consoante os casos.
- O direito de queixa pode ser exercido no **prazo de seis meses a contar da data em que o titular teve conhecimento do facto e dos seus autores** (artigo 115.º, n.º 1, do Código Penal).

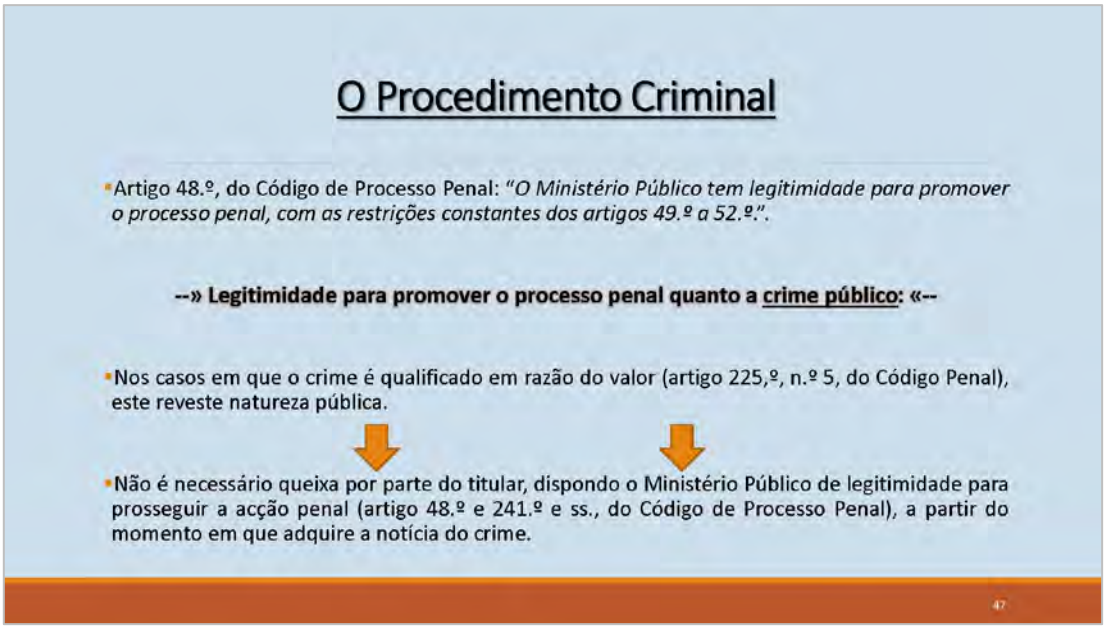
- O crime simples (n.º 1) é semipúblico.
- O crime qualificado (n.º 5) é público.
- O crime cometido nas circunstâncias previstas no artigo 207.º, do Código Penal, é particular.

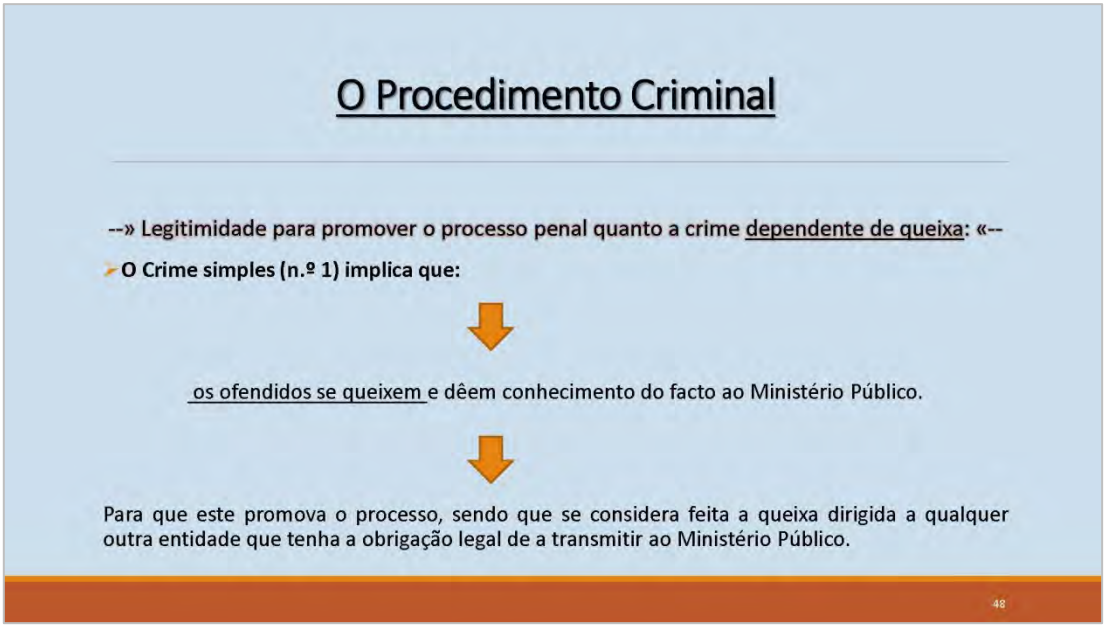
O Procedimento Criminal

- É um **crime particular se se verificar** (Artigo 207.º, n.º 1, alíneas a) e b), do Código Penal):

i. **uma relação do agente com a vítima** (se for cônjuge, ascendente, descendente, adoptante, adoptado, parente ou afim até ao 2.º grau da vítima, ou com ela viver em condições análogas às dos cônjuges)

ii. ou se a **coisa for de diminuto valor e se destinar a utilização imediata e indispensável à satisfação de uma necessidade** do agente ou de pessoa com ele relacionada daquela forma.


O Procedimento Criminal
Artigo 48.º, do Código de Processo Penal: "O Ministério Público tem legitimidade para promover o processo penal, com as restrições constantes dos artigos 49.º a 52.º.".
--» Legitimidade para promover o processo penal quanto a crime público: «--
Nos casos em que o crime é qualificado em razão do valor (artigo 225,º, n.º 5, do Código Penal), este reveste natureza pública.
Não é necessário queixa por parte do titular, dispondo o Ministério Público de legitimidade para prosseguir a acção penal (artigo 48.º e 241.º e ss., do Código de Processo Penal), a partir do momento em que adquire a notícia do crime.
47


O Procedimento Criminal
--» Legitimidade para promover o processo penal quanto a crime dependente de queixa: «--
O Crime simples (n.º 1) implica que:
os ofendidos se queixem e dêem conhecimento do facto ao Ministério Público.
Para que este promova o processo, sendo que se considera feita a queixa dirigida a qualquer outra entidade que tenha a obrigação legal de a transmitir ao Ministério Público.
48

O Procedimento Criminal

--» Legitimidade para promover o processo penal quanto a crime particular: «--

- apenas assiste legitimidade ao Ministério Público para prosseguir com o procedimento criminal se o ofendido/lesado apresentar queixa, se constituir assistente e deduzir acusação particular, conforme estabelece o artigo 50.º, n.º 1, do Código do Processo Penal

49

O Procedimento Criminal

Desistência de Queixa

- O procedimento criminal no crime de natureza semi-pública ou particular:

  é passivel de desistência de queixa, desde que não haja oposição do arguido, até à publicação da sentença da primeira instância (*ex vi* artigo 116.º, n.º 2, do Código Penal).

  se o conhecimento da desistência tiver lugar durante o inquérito, a homologação cabe ao Ministério Público (artigo 51.º , n.º 2 do Código de Processo Penal).

  sendo notificado o arguido para, em cinco dias, declarar, sem necessidade de fundamentação, se a ela se opõe. A falta de declaração equivale a não oposição (artigo 51.º, n.º 3, do Código de Processo Penal).

Prescrição

- O crime simples (n.º 1) prescreve no prazo de cinco anos (artigo 118.º, n.º 1, alínea c), do Código Penal).

- O crime qualificado (n.º 5, alíneas a) e b)) prescreve no prazo de dez anos (artigo 118.º, n.º 1, alínea b), do Código Penal).

  - Sem prejuízo das causas de suspensão ou de interrupção do prazo de prescrição (artigos 120.º e 121.º, do Código Penal).

51

PRÁTICA E GESTÃO PROCESSUAL
O Inquérito

A aquisição da notícia do crime e a definição do objecto do processo

A aquisição da notícia do crime de abuso de cartão de garantia ou de crédito (artigo 241.º, do Código de Processo Penal), pode acontecer de três formas:

1) por conhecimento próprio do Ministério Público,
2) por intermédio dos órgãos de polícia criminal e transmitida posteriormente ao Ministério Público, mediante auto de notícia ou denúncia,
3) por denúncia efectuada verbalmente ou por escrito junto do Ministério Público.

Recebida a notícia do crime, o Ministério Público procede à abertura de inquérito (artigos 53.º, n.ºs 1 e 2, alíneas a) e b), 262.º, n.ºs 1 e 2, 267.º, do Código de Processo Penal, e 3.º, n.º 1, alíneas h) e n), do Estatuto do Ministério Público).

52

PRÁTICA E GESTÃO PROCESSUAL
O Inquérito

O Ministério Público pratica os actos e assegura os meios de prova necessários para determinar os agentes do crime e a sua responsabilidade, em ordem a decidir sobre a acusação (artigo 262,º, 267.º, do Código de Processo Penal), devendo, desde logo:

a) **Verificar se o procedimento legal se encontra prescrito** (artigos 118.º a 126.º, do Código Penal);

b) **Conferir a natureza do crime - particular, semipúblico ou público** - (artigos 48.º, 49.º, n.º 1, e 50.º, n.º 1, do Código de Processo Penal);

c) **Aferir da tempestividade da queixa** (artigo 115.º, do Código Penal);

d) **Apreciar a competência territorial** (artigos 19.º a 23.º, 264.º, do Código de Processo Penal;

e) **Ponderar a sujeição do inquérito a segredo de justiça** (artigo 86.º, do Código de Processo Penal);

f) **Ordenar a realização de diligências urgentes, designadamente relacionadas com a preservação da prova** (ex: preservação das imagens de videovigilância).

53

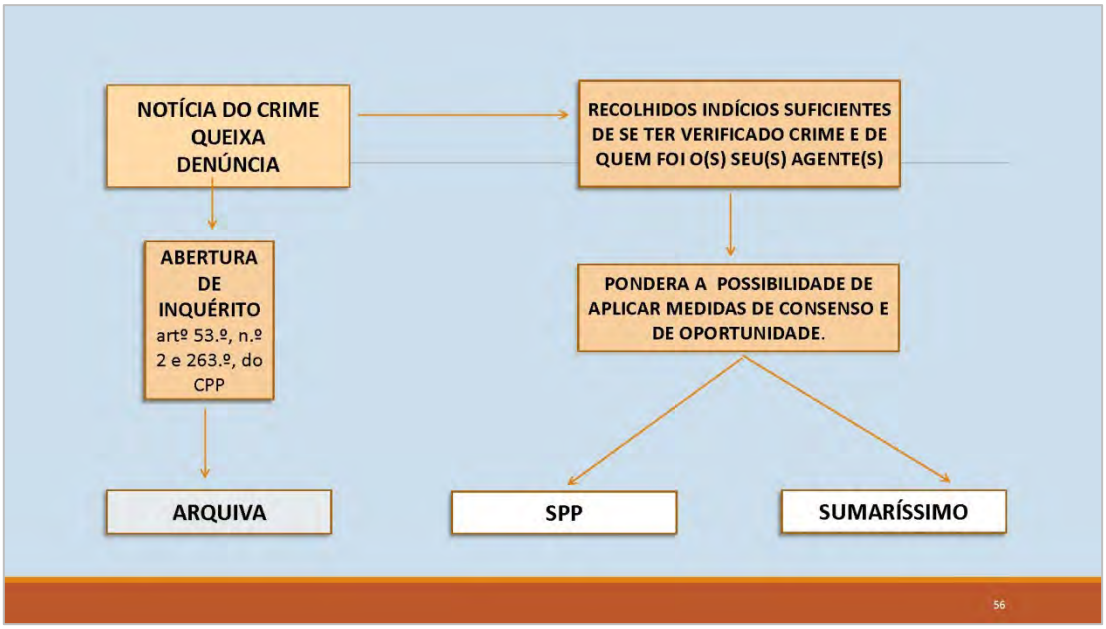
PRÁTICA E GESTÃO PROCESSUAL
O Inquérito

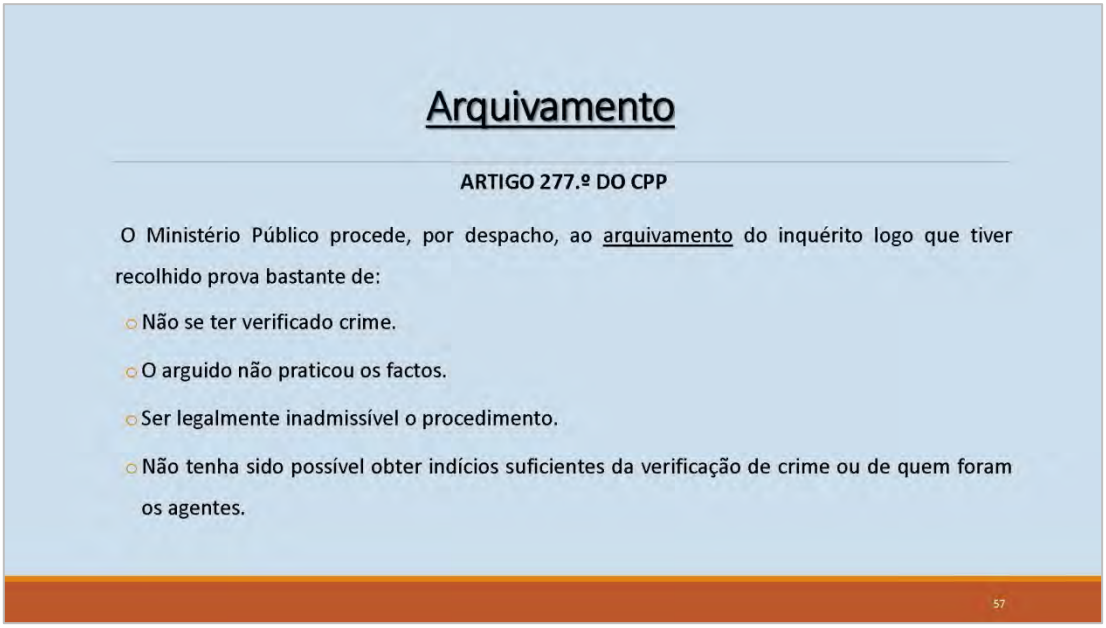
<u>Outras diligências de prova:</u>

A. Solicitar informações ao emitente do cartão relativamente à:

1) identificação do titular do mesmo e respectivas condições contratuais,
2) qual o limite de crédito,
3) crédito até então utilizado,
4) crédito abusivamente utilizado,
5) data de validade do cartão,
6) se o pagamento foi efectuado a crédito ou a débito,
7) entre outras que casuisticamente se mostrem adequadas.

55


NOTÍCIA DO CRIME
QUEIXA
DENÚNCIA
RECOLHIDOS INDÍCIOS SUFICIENTES DE SE TER VERIFICADO CRIME E DE QUEM FOI O(S) SEU(S) AGENTE(S)
ABERTURA DE INQUÉRITO artº 53.º, n.º 2 e 263.º, do CPP
PONDERA A POSSIBILIDADE DE APLICAR MEDIDAS DE CONSENSO E DE OPORTUNIDADE.
ARQUIVA
SPP
SUMARÍSSIMO
56


Arquivamento
ARTIGO 277.º DO CPP
O Ministério Público procede, por despacho, ao arquivamento do inquérito logo que tiver recolhido prova bastante de:
Não se ter verificado crime.
O arguido não praticou os factos.
Ser legalmente inadmissível o procedimento.
Não tenha sido possível obter indícios suficientes da verificação de crime ou de quem foram os agentes.
57

Suspensão Provisória do Processo

ARTIGO 281.º, N.º 1, DO CPP

Crime punível com pena de prisão não superior a cinco anos ou sanção diferente de prisão; situações em que se indicie suficientemente um concurso de crimes punível com pena de prisão superior a 5 anos, mas em que a pena de cada um deles não excede esta medida; não é aplicável aos crimes puníveis com pena de prisão de duração superior, salvo nos casos expressamente previstos na lei, mesmo que o magistrado entenda que, no caso concreto, a pena não deveria exceder os 5 anos de prisão.

Factos que consubstanciem o crime de abuso de cartão de garantia ou de crédito previsto no **artigo 225.º, n.ºs 1 e 5, alínea a), do Código Penal.**, punível com pena de prisão até 3 anos ou com pena de multa, e com pena de prisão até 5 anos ou com pena de multa até 600 dias, respetivamente.

58

Suspensão Provisória do Processo

- Ausência de um grau de culpa elevado será aferida, casuisticamente, tendo em conta, nomeadamente, o comportamento adotado pelo arguido aquando da prática dos factos, o valor do prejuízo patrimonial e as consequências do crime, entre outras, a apreciar À luz do artigo 71.º, n.º 2, do Código Penal.
- No que concerne às injunções e regras de conduta a aplicar, dependerão do caso concreto, porém e tendo em conta o bem jurídico protegido pela norma incriminadora - o património - parece-nos que, a injunção deverá passar sempre pela indemnização do lesado.
- DIRETIVA N.º 1/2014 DA PGR + DIRETIVA N.º 1/2015 DA PGR + INSTRUÇÃO N.º 1/18 DA PGR

59

Processo Sumaríssimo

ARTIGO 392.º DO CPP

Crime punível com pena de prisão não superior a 5 anos; pena de prisão não superior a 5 anos ou pena de multa; pena de prisão não superior a 5 anos e multa; pena de multa; mesmo em caso de concurso desde que não exceda os 5 anos de prisão.

Factos que consubstanciem o crime de abuso de cartão de garantia ou de crédito previsto no **artigo 225.º, n.ºs 1 e 5, alínea a), do Código Penal**

60

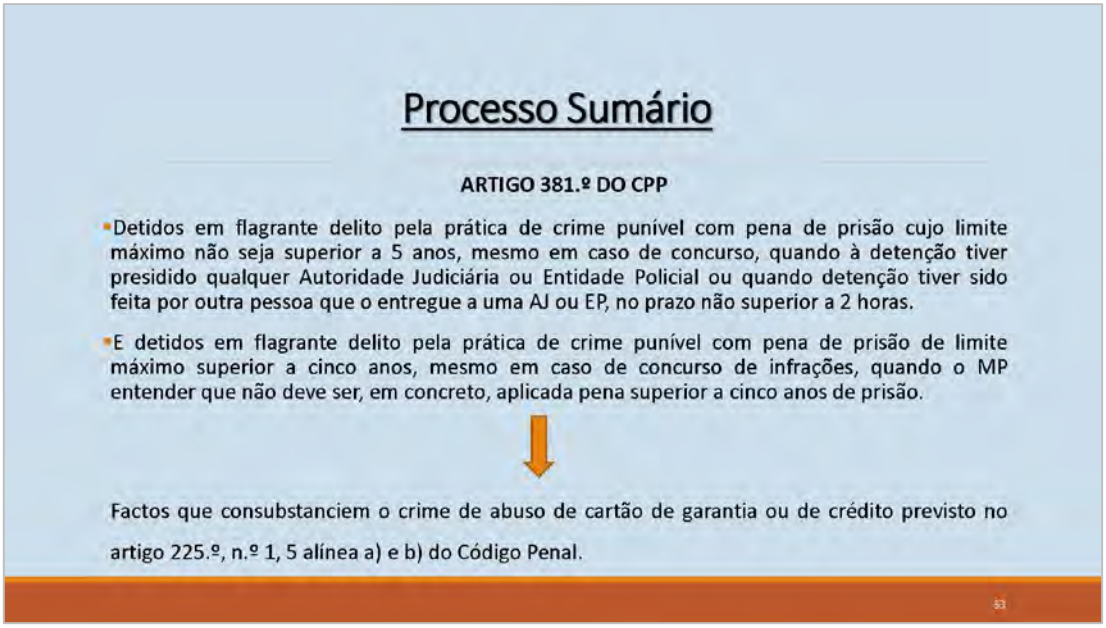
Processo Sumaríssimo

- O Ministério Público por iniciativa do arguido ou depois de o ter ouvido e quando entender ser de aplicar pena ou medida de segurança não privativas da liberdade;
- Se o procedimento depender de acusação particular o requerimento previsto no número anterior depende da concordância do assistente;
- O lesado pode manifestar a intenção de obter reparação dos danos sofridos, caso em que o requerimento deve de conter a indicação da quantia exata a atribuir a título de reparação.

- DIRETIVA N.º 1/2016, DA PROCURADORIA GERAL DA REPÚBLICA.

61


Acusação
Recolhidos indícios suficientes de se ter verificado crime e de quem foi o(s) seu(s) agente(s), não sendo de aplicar a spp ou a forma de processo sumaríssimo, o MINISTÉRIO PÚBLICO DEDUZ ACUSAÇÃO – artigo 283.º, n.º 1 do Código de Processo Penal
SUMÁRIO
ABREVIADO
COMUM
62


Processo Sumário
ARTIGO 381.º DO CPP
Detidos em flagrante delito pela prática de crime punível com pena de prisão cujo limite máximo não seja superior a 5 anos, mesmo em caso de concurso, quando à detenção tiver presidido qualquer Autoridade Judiciária ou Entidade Policial ou quando detenção tiver sido feita por outra pessoa que o entregue a uma AJ ou EP, no prazo não superior a 2 horas.
E detidos em flagrante delito pela prática de crime punível com pena de prisão de limite máximo superior a cinco anos, mesmo em caso de concurso de infrações, quando o MP entender que não deve ser, em concreto, aplicada pena superior a cinco anos de prisão.
Factos que consubstanciem o crime de abuso de cartão de garantia ou de crédito previsto no artigo 225.º, n.º 1, 5 alínea a) e b) do Código Penal.
63

Processo Abreviado

ARTIGO 391.º -A DO CPP

- Crime punível com pena de multa ou com pena de prisão não superior a 5 anos, havendo provas simples e evidentes de que resultem indícios suficientes de se ter verificado o crime e de quem foi o seu agente,
- Os crimes puníveis com pena de prisão de limite máximo superior a 5 anos, mesmo em caso de concurso de infrações, quando o MP, na acusação, entender que não deve ser aplicada, em concreto, pena de prisão superior a 5 anos.

Factos que consubstanciem o crime de abuso de cartão de garantia ou de crédito previsto no artigo 225.º, n.º 1, 5 alínea a) e b) do Código Penal.

Acusação em Processo Comum

ESPECIFICIDADES:

Quando o abuso é cometido pelo próprio titular do cartão:

- Data da validade do cartão;
- Contrato de cartão de crédito e ou garantia (prova dos termos em que o cartão foi emitido e condições, designadamente o limite de crédito concedido);
- Extrato do cartão;
- Valor do cheque/informação acerca do *plafond* do cartão;
- Informação acerca da forma como foi utilizado o cartão (a crédito);

65

Acusação em Processo Comum

ESPECIFICIDADES:

Quando o abuso é cometido por terceiro:

- Recibos assinados pelo terceiro;
- Imagens do terceiro na loja/local onde foi cometido o abuso;
- Informação acerca de forma como entrou na posse do cartão.
- Menção às ordens e instruções dadas pelo legítimo titular do cartão.
- Informação acerca da forma como foi utilizado o cartão (a crédito);

66

Acusação em Processo Comum

A par dos elementos objetivos e subjetivos do tipo e de todos os mencionados no artigo 283.º, n.º 3, do Código de Processo Penal, a acusação deve ainda de:

- Relatar a sucessão de factos passíveis de demonstrar a utilização do cartão, respetivo montantes e locais onde foi usado o cartão, incluindo, quem, dia, data, hora e local.
- Explicitar que o cartão foi usado na sua função típica de servir como meio de pagamento e de concessão de crédito.
- Indicar a prova testemunhal.
- Indicar a prova documental (contrato, cheque, extrato,...).

67

Dificuldades:

- A ausência de provas:
  - Não são deixados os cartões que poderiam eventualmente conter vestígios datiloscópicos;
  - Em caso de "comparticipação" não saber quem utilizou o cartão;
  - Quando o cartão é utilizado por terceiro a quem foi confiado pelo próprio titular, provar que o mesmo foi utilizado de forma abusiva, isto é, de forma diversa daquela para que o mesmo lhe foi confiado.
- Na maioria das vezes a queixa só é feita para acionar o seguro associado, de forma a que o lesado possa ser de alguma forma ressarcido pelo prejuízo patrimonial sofrido.
- Demora na obtenção da informação das entidades bancárias:
  - Violação de dever de colaboração?

Conclusão

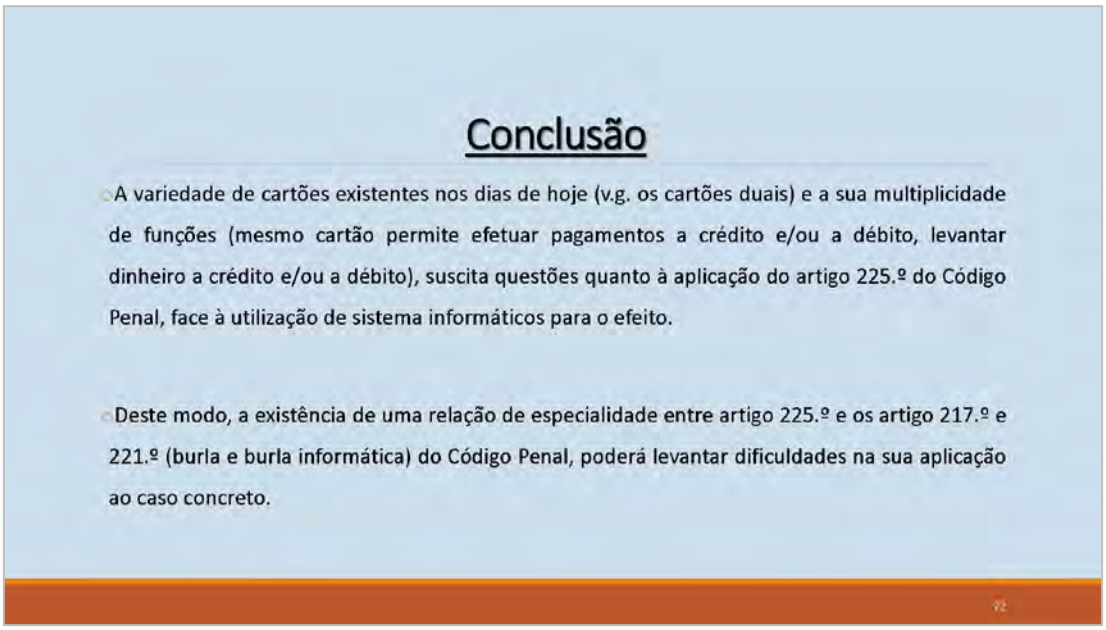
- Quando, em 1995, o legislador introduziu o crime de abuso de cartão de garantia ou de crédito no Código Penal Português, a realidade dos cartões de crédito era muito diferente da atual.
- Inicialmente a utilização do cartão de crédito requeria um terminal de pagamento manual, vulgarmente designado de "ferro de engomar", na qual era colocado o cartão e um impresso.
- Os dados do cartão ficavam gravados num talão, que era passado em triplicado e assinado, e o comerciante comparava a assinatura aposta no talão, com a constante do verso do cartão.
- Posteriormente, o cartão de crédito passou a incluir uma banda magnética que era inserida num terminal de pagamento automático, o talão impresso era assinado pelo titular do cartão, que conferia autenticidade ao ato.

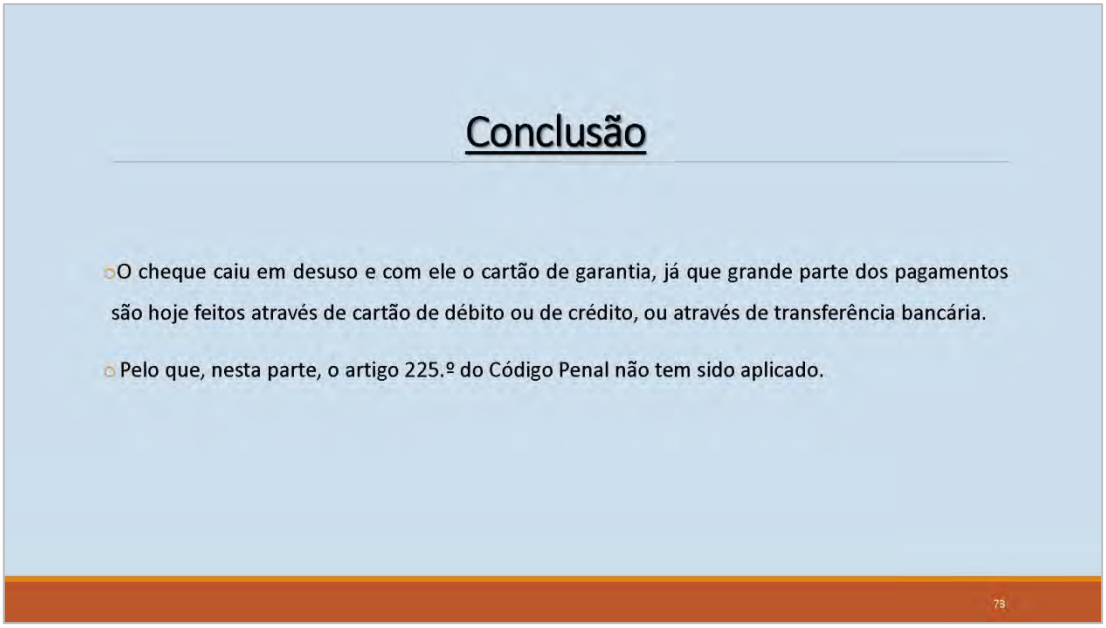
Conclusão

- Mais tarde, o cartão de banda magnética passou a exigir a marcação de um **código PIN**, em substituição da assinatura no talão.
- Recentemente foram introduzidos **CHIPS** nos cartões que armazenam informação (identificação do titular, o seu histórico, o limite de crédito), passando a ser necessário a marcação de um **código PIN** pelo titular, para validar a operação.
- Os terminais de pagamento automático comunicam de forma instantânea com o emitente do cartão, que confirma dos dados do titular, o saldo associado ao cartão, o valor da compra, o tipo de transação, o comerciante (registado e autorizado), o tipo da conexão (que deve obedecer a uma série de protocolos de segurança) e autoriza (ou não) o pagamento.

Conclusão

- Através deste procedimento é difícil imaginar um caso em que o agente consiga realizar um pagamento com o cartão de crédito, sem que disponha de plafond (autorizado) para o efeito, a não ser que o sistema esteja offline como acontece durante a noite quando são feitas as atualizações de software, ou durante uma viagem de avião, ou então que recorra a práticas cibercriminosas.
- Ademais, afigura-se-nos que a utilização abusiva dos cartões de crédito, hoje em dia, se integra quase, exclusivamente, na conduta prevista no crime de burla informática, p. e p. pelo artigo 221.º, n.º 1 do C.P. por implicar a inserção de dados informáticos em sistemas informáticos.


Conclusão
A variedade de cartões existentes nos dias de hoje (v.g. os cartões duais) e a sua multiplicidade de funções (mesmo cartão permite efetuar pagamentos a crédito e/ou a débito, levantar dinheiro a crédito e/ou a débito), suscita questões quanto à aplicação do artigo 225.º do Código Penal, face à utilização de sistema informáticos para o efeito.
Deste modo, a existência de uma relação de especialidade entre artigo 225.º e os artigo 217.º e 221.º (burla e burla informática) do Código Penal, poderá levantar dificuldades na sua aplicação ao caso concreto.
72


Conclusão
O cheque caiu em desuso e com ele o cartão de garantia, já que grande parte dos pagamentos são hoje feitos através de cartão de débito ou de crédito, ou através de transferência bancária.
Pelo que, nesta parte, o artigo 225.º do Código Penal não tem sido aplicado.
73

Conclusão

- No que concerne à tramitação do inquérito, com base nos inquéritos consultados, assistimos a um grande número de desistências/arquivamentos, motivada sobretudo pelo fato de o queixoso não dispor de informação acerca das circunstâncias em que ocorreram os abusos e porque a verdadeira motivação da queixa é, a possibilidade de acionar o seguro associado ao cartão de crédito.

74

CENTRO DE ESTUDOS JUDICIÁRIOS

Obrigado pela vossa atenção!

"Por detrás de uma grande fortuna há um crime!" Honoré de Balzac

Rui Miguel Lima Alves (Norte)
Nuno Filipe de Sousa Gonçalves (Centro)
Maria José Clara Sousa (Lisboa)
Rui Miguel Ferreira dos Santos Cruz (Sul)

75

Título:
O Crime de Abuso de cartão de garantia e crédito e o Crime de Burla Informática

Ano de Publicação: 2019

ISBN: 978-989-8908-58-2

Série: Formação Ministério Público

Edição: Centro de Estudos Judiciários

Largo do Limoeiro

1149-048 Lisboa

cej@mail.cej.mj.pt