Universidade do Minho
Escola de Direito

Ana Helena França Azevedo

Burlas Informáticas: Modos de Manifestação

Tese de Mestrado

Mestrado em Direito e Informática

Trabalho efetuado sob a orientação do

Professor Doutor Fernando Eduardo Batista Conde Monteiro

Professor Doutor Victor Francisco Mendes de Freitas Gomes da Fonte

Janeiro de 2016

DECLARAÇÃO

Nome: Ana Helena França Azevedo

Endereço eletrónico: anahelenafranca@gmail.com Telefone: 912950477

Bilhete de Identidade/Cartão do Cidadão: 13771561

Título da dissertação: Burlas Informáticas: Modos de Manifestação

Orientador/a/es:

Professor Doutor Fernando Eduardo Batista Conde Monteiro

Professor Doutor Victor Francisco Mendes de Freitas Gomes da Fonte

Ano de conclusão: 2016

Mestrado em Direito e Informática

Universidade do Minho, _____/_____/_____

Assinatura

AGRADECIMENTOS

Apesar de um árduo longo trabalho de reflexão e investigação, nada seria possível sem algumas pessoas.

Agradeço e dedico este trabalho à minha mãe, Helena França e irmã Beatriz França pelo incentivo nas horas difíceis e de cansaço. Sem vocês nada seria possível. Isto é por vocês! Ao meu companheiro António Ribeiro, que nos meus momentos de ausência, sempre foi compreensivo. Obrigada pela paciência e amor. Ao meu grande amigo Dr.º Carlos Sá Correia pela sabedoria, palavras de amizade, de incentivo, de esperança e que sempre me fez entender que o futuro é feito a partir da constante dedicação no presente. E a todos os meus amigos que de uma forma ou de outra sempre se preocuparam comigo.

RESUMO

As burlas sempre existiram porém assumem, neste contexto, mecanismos diferentes aos utilizados pela via tradicional.

A difusão das novas tecnologias da comunicação intensificou a prática de «novos crimes» que, pela sua gravidade, constituem uma agressão para determinados valores sociais e juridicamente relevantes.

Fenómeno de neocriminalização, o tipo legal de crime de burla informática, prenunciado no artigo 221.º do C.P., tem vindo a avultar-se enquanto uma nova forma de agressão ao património, através da utilização de meios informáticos. A especificação dos meios utilizados carece de algumas observações. Afigura- se um crime complexo e dissimulado nas mais diversas práticas informáticas.

Hodiernamente, a possibilidade de revermos o crime de burla informática nas mais variadas técnicas informáticas é motivo bastante para nos debruçarmos sobre alguns mecanismos conducentes às mesmas. Essa via possibilita a reunião de elucidações que coadjuvam na consciencialização dos juristas, dos magistrados e que serão favoráveis para servir de melhor modo a justiça Portuguesa e ajudar os tribunais à melhor aplicação do direito.

Palavras-chave: novos crimes; burla informática; práticas informáticas, consciencialização.

Abstract

Frauds have always existed. However, in this context, they assume different mechanisms from those used in the traditional way.

The spread of the new communication and information technologies has intensified the practice of "new crimes" which, due to their weight, are an aggression to certain socially and legally relevant values.

This new type of computer fraud/crime, as in article 221 of the CP, has been increasing as a new form of aggression to patrimony, through the use of electronic means. The specification of the means used lacks some observations. It is a complex and concealed crime, which uses various computer practices.

In our times, the possibility of seeing the computer crime in all possible techniques is reason enough to draw our attention to the mechanisms which lead to those crimes. It enables the gathering of explanations, which may help to raise the jurists and the judges' awareness. It will lead the Portuguese justice and the courts towards a better implementation of the law.

Keywords: new crimes; computer fraud; computer pratices; awareness.

ÍNDICE

ABREVIATURAS UTILIZADAS

ATM – Automated Teller Machine

CC – Código Civil

CFR – Conferir

CP – Código Penal

CNP – Card Not Present

CPE – Código Penal Espanhol

CPI – Código de Propriedade Industrial

CSRF – Cross-site Request Forgery

DNS – Domain Name System

HTML – HyperText Markup Language

HTTP – HyperText Transfer Protocol

LC – Lei do Cibercrime

LCI – Lei da Criminalidade Informática

LO – Lei Orgânica

NSA – National Security Agency

OPC – Órgão de Polícia Criminal

PIN – Personal Identification Number

PJ – Polícia Judiciária

POS – Point of Sale

PSTN – Public Switched Telephone Network

SMS – Short Message Service

STJ – Supremo Tribunal de Justiça

TIC – Tecnologias da Informação e Comunicação

TPA – Terminal de Pagamento Automático

ULR – Uniform Resource Locator

XSS – Cross-site Scripting

CAPÍTULO I

1. INTRODUÇÃO

Num mundo tomado de assalto pelas novas tecnologias –"produto da dialética entre a ciência e a engenharia"[1] – com caráter peculiar e até volátil não é de estranhar que a nossa vida seja pautada e realizada, em grande medida, via Internet.

Nas últimas décadas, temos assistido de forma incontornável a um desenvolvimento e avanço das novas tecnologias, consubstanciadas no progresso da informática e na globalização. A realidade rapidamente sofreu uma evolução com a massificação do acervo de dispositivos e de bens informáticos e com a globalização da informação, que têm vindo a reformular o nosso quotidiano de forma quase irreversível. A utilização da informática e telemática estendeu-se de forma invasiva a grande parte das atividades humanas que, atualmente são cada vez mais caraterizadas pela informatização e automatização.

O fácil acesso à Internet, paralelamente com a criação de dispositivos móveis com capacidade de comunicação, veio espoletar uma mudança de paradigma na forma como se desenvolveram as aplicações informáticas e na expetativa que os utilizadores depositaram na utilização dos mesmos.

As tecnologias e a Internet, com uma veloz projeção mundial, são hoje a representação cultural da contemporaneidade.

1.1. O aparecimento da Internet e da Sociedade da Informação

The Internet is becoming the town square for the global village of tomorrow.[2]

Bill Gates

O aparecimento da Internet veio revolucionar de forma dramática o mundo. É um novo mundo ainda por explorar. A Internet é mais utilizada do ponto de vista estratégico e académico, enquanto ferramenta de trabalho de comunicação, que fomenta o conhecimento. A sua génese

[1] Freitas, Pedro Miguel. "Breves nótulas sobre o crime de acesso ilegítimo previsto na Lei do Cibercrime". In *Estudos em comemoração dos 20 anos da Escola de Direito da Universidade do Minho*, ed.Mário Ferreira Monte, et al., pp. 565-585, Coimbra Editora, 2014, p. 568.

[2] Tradução: "A Internet está a tornar-se a praça da cidade para a aldeia global de amanhã."

é, na realidade, tudo menos lúdica ou amadora. Não obstante, a sua projeção mundial fez-se notar a todos os níveis como também na sua vertente mais lúdica, como por exemplo, através da utilização de ferramentas assíncronas, como é o caso do correio eletrónico. Porém, *a posteriori*, pese embora o facto de parecer um fenómeno desconcertante, começa a ganhar um caráter cada vez mais significativo, acabando por estender-se freneticamente a todo o tipo de relações e sendo considerado, atualmente, como a maior ferramenta do mundo dos negócios.

Importa, antes de mais, frisar a importância do aparecimento da Internet propriamente dita, a fim de ilustrar a relevância astronómica que tem nas nossas vidas e a sua preponderância na matéria que estamos a abordar.

A era da revolução tecnológica culminou, no nosso entendimento, com a II Guerra Mundial que permitiu explorar potencialidades a fim de dar respostas ao governo norte-americano. Em 1957 o Departamento de Defesa norte-americano, designado por DoD – *Department of Defense* –, criou uma agência para os projetos de pesquisa avançada, a ARPA – *Advanced Research Project Agency*. Esta última teve como objetivo o reforço dos progressos científicos suscetíveis de serem utilizados para fins militares. A história da Internet começa nos Estados Unidos, na década de 60, com a instalação de uma rede de grande distância de comutação de pacotes.[3] Em 1969, ocorreu a primeira experiência de computadores em rede, entre a Universidade da Califórnia – Los Angeles –, SRI – *Stanford Research Institute*, a Universidade de Utah e a Universidade da Califórnia – Santa Barbara, dando origem à ARPANET.[4] Em 1990, a ARPANET foi desmantelada pelo Departamento de Defesa dos E.U.A. tendo a mesma sido substituída pela rede da NSF, rebatizada NSFNET, e popularizada, em todo o mundo, com a denominação de Internet.

A Internet é uma rede aberta de interligação mundial de computadores que providencia a transmissão, receção, produção e registo de informações entre indivíduos das mais diversas posições geográficas. A rede é, segundo Manuel Castells[5], um conjunto de nós interligados,

[3] Comutação de pacotes traduz-se na técnica de transmissão de informação de informação que consiste em segmentar a mensagem a transmitir numa série de pacotes que são transportados pela rede.

[4] ARPANET é o acrónimo da palavra da expressão inglesa *Advanced Research Projects Agency* – agência norte-americana financiada pelo governo.

[5] Castells, Manuel. *A Era da Informação: Economia, Sociedade e Cultura, Vol. I A Sociedade em Rede*. Lisboa: Fundação Calouste Gulbenkian, 2005, p. 605.

constituindo deste modo a nova morfologia das sociedades. A estrutura descentralizada da Internet leva a que esta seja muitas vezes designada como a "rede das redes", pois permite que os utilizadores de qualquer computador – independentemente do seu ponto geográfico no globo – consigam aceder a informações contidas noutro qualquer computador ligado à rede, desde que para tanto estejam autorizados. As duas formas mais populares de utilização desta "nova" infraestrutura são o correio eletrónico[6] e a *World Wide Web.*[7]

Este movimento, que se processa à escala mundial, não conhece fronteiras espaciais, temporais, linguísticas, raciais, culturais ou económicas, sendo o mesmo visto, muitas das vezes, como um espaço desgovernado que desconhece regras e onde as «boas» condutas são desconsideradas.

A Internet enquanto fenómeno dinâmico, portador de inúmeras vantagens e presente nas nossas rotinas de forma quase imperativa, impõe-se, segundo José de Oliveira Ascensão como uma "infraestrutura básica" já constituída, que assegura a veiculação permanente da comunicação[8]. Subscrevemos o douto entendimento na íntegra, porque atualmente existem serviços que, para funcionarem plenamente, necessitam de recurso à Internet. Naturalmente que a Internet e a informática vieram desencadear, com a sua invasão progressiva nos setores da Administração Pública, a gradual desburocratização e desmaterialização do sistema. A comunicação fácil e acessibilidade a serviços que estes fenómenos têm colocado à disposição de uma sociedade da informação cada vez mais submissa a esta realidade, caraterizada ainda pelo desmantelamento de determinados modelos de negócio existentes, sustentam também esta perspetiva.

---

[6] *E-mail* ou *eletronic mail*, comumente designado, em língua portuguesa por correio eletrónico, permite uma troca assíncrona – os dois polos não necessitam de estar simultaneamente presentes para comunicar – de mensagens, não exclusivamente textuais, entre duas ou mais pessoas ligadas à Internet. Segundo o artigo 2.º, alínea b) da Lei n.º46/2012 de 29 de Agosto, correio eletrónico é definido como *"qualquer mensagem textual, vocal, sonora ou gráfica enviada através de uma rede pública de comunicações que possa ser armazenada na rede ou no equipamento terminal do destinatário até que este a recolha".*

[7] A título de curiosidade, o WWW foi inicialmente desenvolvido em 1989 no CERN – *Centre Euripéen de Recherce Nucléaire* – com sede em Genebra, por Tim Berners-Lee. No entanto, foi o *software* cliente Mosaic da NCSA – *National Center for Supercomputing Applications* – em 1993, que conferiu à Web a simplicidade de utilização e as capacidades multimédia que estão na origem do seu grande sucesso. Denominado também por "3W", o WWW é uma forma de acesso e visualização de informação através da Internet, tendo como base a utilização do protocolo HTTP – *Hypertext Transfer Protocol.*

[8] Ascensão, José de Oliveira. "Sociedade da Informação". In *Direito da Sociedade da Informação – Vol. I*, Associação Portuguesa do Direito Intelectual. Coimbra Editora, 1999, p. 165.

Institui-se assim uma nova leitura do mundo. A sociedade contemporânea encontra-se em constante mutação, sendo particularmente relevante aquela que se prende com a utilização das novas tecnologias, "na qual as distâncias físicas são uma realidade em revisão, porque deixaram de fazer sentido"[9]. Vivemos hoje num mundo dominado pela máquina, num real ciberambiente. Parece-nos que a sociedade gira em torno da rede. Aliás, a forte dependência da máquina e dos sistemas atesta essa mesma pretensão e vem a verificar-se desde cedo[10]. Embora não se encontre definido, em bom rigor o ciberambiente a que aludimos compreende não só os suportes informáticos como também a Internet. Com a mobilização intensa dos recursos científicos, as máquinas inteligentes ganham impulso dando origem à sociedade da informação. Consequentemente, atendendo ao Relatório Geral sobre as Atividades da Europol de 2010, dar-se-á origem a "uma economia clandestina digital sofisticada e auto-suficiente".

A sociedade da informação emerge, enquanto modelo de sociedade, aquando da invasão de meios eletrónicos, tais como o telefone, televisão, rádio ou computador. Por outras palavras, estas são algumas das tecnologias de informação e comunicação que envolvem o armazenamento, processamento, aquisição e distribuição da informação. O ciberambiente é o responsável pela "metamorfose" que a sociedade da informação tem vindo a sofrer. Até aqui não nos restam dúvidas. Segundo Pedro Verdelho, quando nos referimos a sociedade da informação falamos sobretudo de um modelo de sociedade cuja informação está disponível de forma livre e aberta. É certo que a sociedade, não sendo considerada uma realidade estática, se está a adaptar ferozmente a este novo paradigma, fazendo com que não haja soberania sobre a mesma "já que o ciberespaço é independente e anárquico, ingovernável e irreprimível"[11]. Para além disso, segundo o mesmo autor, a sociedade da informação deixou marcas consideráveis na ordem jurídica nomeadamente através da "pulverização de conceitos (...) da dissipação da capacidade para aplicar na prática conceitos jurídicos até agora tidos como universais. Por exemplo, os conceitos de competência jurisdicional ou de competência territorial, têm que

[9] Verdelho, Pedro. " Phishing e outras formas de defraudação nas redes de comunicação". In *Direito da Sociedade da Informação – Vol. VIII,* Associação Portuguesa do Direito Intelectual. Coimbra Editora, 2009, p. 410.

[10] A dependência da informática e da Internet tem-se evidenciado em fatores sociais, designadamente a forte ligação que atualmente os mais jovens vivem em relação aos mesmos. Parece-nos que se avizinha um novo modelo de sociedade.

[11] Verdelho, Pedro. " Cibercrime". In *Direito da Sociedade da Informação – Vol. IV,* Associação Portuguesa do Direito Intelectual. Coimbra Editora, 2003, p. 348.

evidentemente que ser reescritos, face a redes de comunicação globais, que não conhecem fronteiras"[12].

Concomitantemente com a Internet, a disponibilidade de serviços tem vindo a entranhar-se de forma quase impositiva em todos os ramos das nossas vidas, tornando-se cada vez mais assinalável a dependência criada à volta do uso dos mesmos no quotidiano.

Não obstante, paralelamente ao crescimento "saudável" da sociedade da informação, há o revés da moeda, ou seja, os efeitos perversos que acompanham o crescimento da sociedade da informação. Para além disso, e em contraposição com a sociedade da informação, surge a sociedade do risco[13] [14] que se reflete no potencial risco que o progresso tecnológico poderá acarretar, provocando sérias inseguranças. A fim de dar resposta a essas adinamias "refugia-se e recorre-se ao Direito Penal, que na forma de "Direito Penal do Risco" responde numa lógica preventiva e antecipa a tutela dos bens jurídicos supraindividuais considerados essenciais".[15]

Em relação às vantagens do uso da Internet, pese embora o facto de que o que nos releva são os efeitos perversos que a acompanham, julgamos necessário elencar, de forma muito breve, algumas: promove a comunicação entre pessoas, é um instrumento de entretenimento, permite a obtenção de vários conhecimentos, seja através de motores de busca, ou de outras ferramentas, a prestação de serviços na Internet, como o sistema de *homebanking*, possibilita o comércio eletrónico, entre outros. Ao invés, a Internet tem vindo a revelar-se um instrumento de cometimento de alguns crimes, uma vez que viabiliza a prática de atividades delituosas. A novidade reside na escala e automatização!

---

[12] Verdelho, Pedro. " Phishing e outras formas de defraudação nas redes de comunicação". In *Direito da Sociedade da Informação – Vol. VIII,* Associação Portuguesa do Direito Intelectual. Coimbra Editora, 2009, p. 410.

[13] Dias, Vera Marques. "A Problemática da Investigação do Cibercrime". In *DataVenia – Revista Jurídica Digital,* Ano 1, n.°1, ed. Joel Timóteo Ramos Pereira. DataVenia. Julho, 2012, p. 79. http://www.datavenia.pt/ficheiros/edicao01/datavenia01_p063-088.pdf (consultado 20 Novembro, 2015).

[14] A este propósito Vera Marques Dias aponta para o facto de Ulrich Beck ser "um dos primeiros a reconhecer o estranho paradoxo de que o risco pode ser aumentado com o desenvolvimento e progresso da tecnologia, ciência e industrialismo, ao contrário do que seria esperado." Acrescenta ainda que Ulrich Beck afirma que "nos encontramos perante uma modernidade reflexiva ou segunda modernidade reflexiva, que consiste num processo de autoconfrontação com os efeitos da sociedade do risco com os próprios fundamentos do desenvolvimento desmesurado e as antinomias em relação à primeira modernidade", conforme p. 79.

[15] Dias, Vera Marques, op.cit., p. 80.

Há, no entanto, associada aos crimes informáticos a complexa questão das cifras negras que consistem naqueles crimes que não chegam ao conhecimento das autoridades e cujos agentes nunca serão conhecidos, logo nunca julgados. A nossa convicção é a de que nunca teremos um conhecimento efetivo deste cenário criminoso, incluindo em relação ao crime de burla informática, o que dificultará a resolução de medidas de combate e de prevenção aos mesmos.

Em jeito de remate, sejam quais forem os futuros desenvolvimentos da Internet, é indiscutível que estamos a assistir ao desenvolvimento do meio de comunicação e importa salientar que estamos a passar de uma Internet de pessoas para uma Internet de coisas[16]. Desta forma concluímos que a Internet é um palco onde se ensaiam comportamentos.

1.2. A problemática do cibercrime

A este propósito, Helena Moniz refere que "o direito penal debate-se na atualidade com os problemas oriundos da utilização intensa das redes de telecomunicações, de fluxo de dados transfronteiras (...) em suma, das novas tecnologias enquanto novos meios para a prática de velhos crimes"[17]. De facto, as tecnologias da informação, especialmente a Internet potenciam e revelam-se como uma fonte poderosíssima e extremamente facilitadora para o cometimento de "novos" crimes.

Em matéria de legislação, Portugal encontra-se praticamente na "primeira linha". A primeira lei que surgiu em Portugal com objetivo de enfrentar a emergente criminalidade do ciberespaço foi a denominada Lei da Criminalidade Informática (Lei 109/91, de 17 de Agosto), não obstante, não reunia nem dispunha de meios processuais. Fica claro que com o passar do tempo o cibercrime fica mais intrincado. Consequentemente a União Europeia sentiu necessidade de rever estas questões, e desta forma é constituída uma Convenção sobre o Cibercrime do

[16] Internet das coisas ou *Internet of things* (IoT) é o conceito criado para a revolução tecnológica em que os dispositivos estão conectados à Internet. Pensamos, vulgarmente, nos computadores ou *smartphones,* mas hoje em dia existe uma oferta imensa de utensílios que se encontram conectados à Internet, como é o caso de alguns eletrodomésticos, pulseiras que registam a atividade física do utilizador (por exemplo Nike FuelBand SE), entre tantos outros.

[17] Moniz, Helena. "Internet e Globalização – Problemas Jurídico-Penais: notas breves". In *As telecomunicações e o direito na Sociedade de Informação*, coord. António Pinto Monteiro. Coimbra: Instituto Jurídico da Comunicação. 1999, p. 367.

Conselho da Europa a 23 de Novembro de 2001, que para além de ser uma convenção europeia também foi negociada por alguns países tecnologicamente mais desenvolvidos, como é o caso, dos EUA, Canadá e Austrália. Como nota, um outro instrumento pertinente é a Decisão-Quadro 2005/222/JAI do Conselho de 24 de Fevereiro de 2005. Ambos instrumentos internacionais surgiram numa tentativa de dar resposta aos crimes cometidos por via da tecnologia ou informática. A Convenção introduziu, de uma forma inédita, disposições de cariz processual[18]. A mesma foi conseguida partindo de vários pressupostos tais como: haver uma coesão e cooperação entre os membros estando convencidos " da necessidade de prosseguir, com carácter prioritário, uma política criminal comum, com o objetivo de proteger a sociedade contra o cibercrime, *inter alia*, através da adoção de legislação adequada e da melhoria da cooperação internacional", com consciência das mudanças levadas pelo advento dos sistemas informáticos e pela preocupação com o "risco de que as redes informáticas e a informação eletrónica sejam igualmente utilizadas para cometer infrações criminais e de que as provas dessas infrações sejam armazenadas e transmitidas através dessas redes".

Por sua vez, Portugal aprovou com algum atraso a Lei 109/2009 de 15 de Setembro, a Lei do Cibercrime que revoga a LCI e transpõe para a ordem jurídica interna a Decisão-quadro n.º 2005/222/JAI do Conselho de 24 de Fevereiro, sendo que a mesma estabelece as disposições penais materiais e processuais, bem como as disposições relativas à cooperação internacional em matéria penal, relativas ao domínio do cibercrime e de recolha de prova ou suporte eletrónico, tendo a mesma como base a Convenção de Budapeste.

No entanto, foi apenas com a LC que foi possível alcançar medidas processuais aplicáveis à investigação criminal do cibercrime. A LC prevê tipos legais de crime onde a informática surge como meio para a prática do crime. Mas qual o critério que permite distinguir os crimes previstos no CP dos crimes previstos na LC? Parece-nos que o critério diferenciador é o bem jurídico. No CP, para além de se tipificarem crimes em sentido estrito, tipificam-se crimes cujos bens jurídicos protegidos incidem na natureza iminentemente patrimonial, ao passo que na LC incidem essencialmente na integridade dos sistemas informáticos. Por seu turno, segundo alguns autores (tal como Pedro Dias Venâncio e Oliveira Ascensão), consideram-se tipos de

[18] Venâncio, Pedro Dias. "Relatório Explicativo da Convenção sobre o Cibercrime" (versão portuguesa). In *Lei do Cibercrime*. Coimbra Editora, 2011, p. 202.

atividade criminosa: crimes relacionados com o conteúdo, crimes relativos à proteção de dados pessoais ou de privacidade, crimes informáticos em sentido estrito (crimes previstos na LC) e os crimes que recorrem a meios informáticos que não alteram o tipo penal comum, sendo os mesmos uma especificação ou qualificação deste, como é o caso da burla informática.

Face ao exposto, temos duas observações a fazer. Achamos infundado o crime de burla informática não constar na LC, já que tipifica crimes onde a informática surge como meio para a prática do crime, independentemente do bem jurídico protegido. E talvez, por se considerar que o crime de burla informática decorre do tipo legal comum é que não se incluiu na LC. De todo o modo, é nossa convicção que o crime de burla informática, enquanto fenómeno de criminalidade informática deveria estar prevista na LC, assim como o crime de devassa por meio de informática, prevista e punida no artigo 193.º do CP.

Mas de que se trata o cibercrime? A criminalidade informática ou cibercrime, como é comumente designada, pode assumir diversas terminologias. No que concerne à terminologia adotada, Garcia Marques e Lourenço Martins[19] alertaram para a inexistência de um conceito expressamente consagrado na legislação, ou uniformemente consolidado na doutrina e jurisprudência portuguesa. Acresce Paulo de Sousa Mendes que não é sensato estar em busca de um conceito deste tipo, isto porque as combinações do crime com a informática abrangem maioritariamente todos os domínios da velha criminalidade.[20] Estes velhos crimes apenas ganharam novos meios de execução, ou seja, existe a transposição de crimes já previstos para o ambiente digital. Pese embora o facto de serem cometidos em ambiente virtual, isso não lhes atribui nenhuma especialidade,[21] até porque o crime não foi arquitetado para o contexto informático.

Ainda assim, Garcia Marques e Lourenço Martins prosseguem dizendo que dever-se-á "encarar a criminalidade informática como 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

[19] Garcia Marques, A. J. e A.G. Lourenço Martins. *Direito da Informática.* 2.ª edição. Coimbra: Almedina, 2006.

[20] Mendes, Paulo de Sousa. "A responsabilidade de pessoas coletivas no âmbito da Criminalidade Informática em Portugal. "In *Direito da Sociedade da Informação – Vol. IV,* Associação Portuguesa do Direito Intelectual. Coimbra Editora, 2003, p. 385.

[21] Verdelho, Pedro. " Cibercrime". In *Direito da Sociedade da Informação – Vol. IV,* Associação Portuguesa do Direito Intelectual. Coimbra Editora, 2003, p. 348.

computador é objeto do crime"[22]. Esta definição, desenvolvida por estes dois autores, é acarinhada por muitos outros. No entanto, levanta as principais dicotomias que dificultam a previsão de um conceito homogéneo de "criminalidade informática". É "incontornável reconhecer que as realidades sociológicas de tipo criminógeno atualmente discutidas a propósito do cibercrime estão muito para lá daquilo que na lei portuguesa se consagrou como criminalidade informática"[23].

De facto, tem sido integrada no fenómeno da criminalidade associada às tecnologias da informação e comunicação uma diversidade de comportamentos violadores de valores fundamentais e de natureza distinta. A propósito, a doutrina tem vindo a distinguir os crimes informáticos em sentido amplo e os crimes informáticos em sentido estrito. Nos primeiros, a criminalidade informática engloba toda a atividade criminosa que pode ser levada a cabo por meios informáticos, ainda que estes não sejam mais do que um instrumento para a sua prática, mesmo que esses meios informáticos não façam parte do tipo legal, pelo que o mesmo crime poderá ser praticado por recurso a outros meios, ou seja, dogmaticamente nada os distingue da sua forma tradicional, tendo apenas de diferente o recurso utilizado. Nestes casos, as tecnologias de informação e comunicação constituem mais um modo de execução para a prática de crimes cujo tipo legal se encontra previsto no CP, sem ter em consideração a utilização de meios tecnológicos enquanto elemento integrador do crime; a título de exemplo, enunciamos o crime de difamação (artigo 181.º do CP) e o crime de injúria (artigo 180.º do CP). No âmbito destes dois crimes, a interferência que o uso de meio tecnológico tem sobre o tipo legal é o meio utilizado para divulgação de expressões injuriosas ou difamatórias como também leva à agravação da moldura abstrata da pena. Os segundos, *maxime* crimes relacionados com o *software* e a rede Internet, compreendem aquele conjunto de tipos legais de crime que introduzem um meio informático ou um elemento digital no tipo legal de crime ou em que a informática faz parte do objeto tutelado pelo tipo legal de crime, como é o caso do tipo legal do crime de burla informática.

A problemática da cibercriminalidade não se prende só com a indefinição do próprio conceito, mas também com outras realidades. Assim, a problemática do cibercrime decorre dos

[22] Garcia Marques, A. J. e A.G. Lourenço Martins. *Direito da Informática.* 2.ª edição. Coimbra: Almedina, 2006, p. 641.

[23] Verdelho, Pedro, op.cit., 347.

seus apanágios que poderão acarretar impedimentos ao nível da sua prevenção, investigação e punição. Veremos de seguida algumas características da cibercriminalidade.

Quanto à transnacionalidade, o caráter transfronteiriço ou de extraterritorialidade da Internet fomenta a criação de um espaço inexistente dentro de quaisquer fronteiras estaduais, bem como uma total falta de controlo.[24] A transnacionalidade surge como um dos principais problemas no combate e repressão do cibercrime, nomeadamente na dificuldade de aplicação de forma estanque de uma única jurisdição. Por sua vez, a-temporalidade corresponde ao hiato temporal entre a "prática da inicial ação ilícita pelo autor e a sua materialização final através da produção do resultado".[25] Ambas as características são proveitosas para a conduta criminosa, pois, por um lado, podem atingir um número massivo de pessoas e, por outro lado, permitem uma preparação mais deliberada.

Uma outra particularidade refere-se à deslocalização; e nas palavras de Pedro Venâncio, o facilitismo associado ao uso da Internet e meios tecnológicos veio desencadear uma "deslocação criminosa para a Internet".[26] Isto significa que o crime deixou de ser praticado na rua para ser cometido, ao invés, à distância de um clique, em zona de conforto. Esta deslocalização de práticas criminosas, antes cometidas por métodos tradicionais, é agora promovida por instrumentos em ambiente digital, fatores que, aliados ao anonimato e potencial impunidade, aliciam à consumação dos crimes, promovendo assim "exponencialmente a internacionalização da criminalidade informática"[27]. Paralelamente à deslocalização para a Internet, a deslocalização criminosa na Internet abrange a deslocalização de conteúdos de um servidor para outro. Isto quer dizer que, a partir do momento em que se deteta atividade ilícita ou conteúdos ilícitos, os agentes criminosos transferem esses mesmos para outros pontos localizados na Internet, nomeadamente para um servidor localizado noutro país, acedendo deste modo ao tão desejado "paraíso cibernético". Estes "paraísos cibernéticos" favorecem normalmente os agentes

[24] A título de curiosidade consultar a Declaração de Independência do Ciberespaço, disponível em http://www.dhnet.org.br/ciber/textos/barlow.htm (consultado 20 Novembro 2015).

[25] Cfr. Dias, Vera Marques. "A Problemática da Investigação do Cibercrime". In *DataVenia – Revista Jurídica Digital,* Ano 1, n.º1, ed. Joel Timóteo Ramos Pereira. DataVenia. Julho, 2012, p. 71. http://www.datavenia.pt/ficheiros/edicao01/datavenia01_p063-088.pdf (consultado 20 Novembro, 2015).

[26] Venâncio, Pedro Dias. "Investigação e Meios de Prova na Criminalidade Informática". In *Compilações doutrinais Verbo Jurídico*. Verbo Jurídico, 2006,p. 6 http://www.verbojuridico.net/doutrina/tecnologia/meiosprovacriminalidadeinformatica.pdf (consultado 20 Novembro 2015).

[27] Idem.

criminosos, ou porque, a instrumentalização de investigação é diminuta, ou a sua conduta não se encontra tipificada, ou então porque a legislação o favorece. Deparamo-nos com a problemática da competência territorial, isto é, é juridicamente difícil e improvável que as autoridades dos países de onde saíram os conteúdos imponham a sua decisão perante os países para onde se alojaram os conteúdos.

Um outro problema com que nos deparamos é a diversidade de ordens jurídicas e aplicabilidade do princípio da territorialidade. A natureza "multi-jurisdicional" da Internet e da cibercriminalidade levanta novos problemas quanto à aplicação da lei penal nas diversas ordens jurídicas envolvidas. Por conseguinte, deparamo-nos com um problema de jurisdição na internet. Concludentemente, o mesmo acontece à qualificação do crime, cuja moldura penal se torna diferente ou até inexistente. A informática encontra-se intrinsecamente ligada à ideia de globalização através da Internet, dificultando a determinação do lugar onde determinado crime foi perpetrado e, em consequência, a competência para o julgar. Fica explicito que o agente do crime informático, na maioria da esmagadora das vezes, não estará fisicamente presente no local da prática do crime. Dada a especificidade do cibercrime, persiste a dúvida de saber qual a lei a aplicar. Na verdade, a questão do cibercrime tem vindo a enquadrar-se na problemática dos delitos à distância, isto é, crimes cujo lugar onde o autor cometeu o crime difere do lugar onde é produzido o resultado. Questionamo-nos sobre as circunstâncias em que se considera que um crime informático é punível em Portugal. Ao analisar a letra da lei (artigo 4.º do CP) relativa à aplicação da lei penal no espaço, a lei portuguesa aplica-se a todos os factos cometidos em território português, independentemente da nacionalidade do agente, e também, a todos os factos praticados a bordo de navios ou aeronaves portuguesas. Por seu turno, o artigo 7.º do CP prevê "a teoria da ubiquidade que resulta da conjugação da teoria da atividade (em que o lugar do crime é aquele em que o agente realizou o processo executivo (...)), com a teoria do efeito (em que o lugar do crime é aquele onde se produziu o resultado típico) e a teoria do efeito intermédio (em que o lugar do crime é aquele em que a energia posta em movimento pelo agente atinge o objeto ou alcança a vítima) "[28]. E portanto, o facto considera-se praticado, tanto no lugar em que o agente atuou, como naquele em que o resultado foi produzido. Como atesta Joel Timóteo Ramos Pereira para determinação do *sedes delicti* terá que se ter em linha de

[28] Santos, M.Simas e M.Leal Henriques. *Noções Elementares de Direito Penal*. 2.ª edição. Editora Rei dos Livros, 2003, p. 47.

conta qualquer um dos elementos de conexão previstos no artigo 7.º do CP, designadamente a ação, omissão ou resultado típico e, segundo o mesmo autor, "em qualquer uma destas circunstâncias considera-se o crime como praticado em Portugal e, consequentemente, aplicável o direito português"[29]. Acrescenta ainda o mesmo autor que " se um utilizador da Internet, situado no nosso país, recebe uma informação proveniente de território estrangeiro, que constitua crime à luz do CP e produz resultado típico em Portugal, o crime considera-se praticado em Portugal".[30] E por esse motivo Helena Moniz estabelece um duplo grau de conexão, isto é, deve-se aplicar o direito português quando o facto é praticado em território português, mas também quando o resultado se produz em território português.[31] A deslocalização criminosa na internet levanta algumas dificuldades em relação à aplicação da lei penal no espaço, em matéria de litígios relativos à Internet. Além disto, estes obstáculos conduzem-nos a grandes delimitações e ineficiência da investigação e julgamento deste tipo de crimes, suscitando dúvidas sobre se o local do crime é o país onde está instalado o servidor que contém a informação, ou o país onde reside o agente que coloca a informação naquele servidor. Com efeito, não se poderá valer de critérios que classicamente localizam o ilícito no espaço, no local onde a ação se desdobra ou onde são produzidos os resultados do crime.[32]

A fim de solucionar dificuldades práticas, o artigo 27.º, n.º1 da LC, para além do disposto no CP, prevê ainda as situações de aplicabilidade da lei penal portuguesa, resolvendo-se a questão.[33] Por essa via decidir-se-á qual dos Estados terá legitimidade e competência para o julgamento em questão. Desta forma, pretende-se que sejam colmatadas todas as lacunas

---

[29] Pereira, José Timóteo Ramos. *Direito da Informação e Comércio Eletrónico.* Lisboa: *Quid Juris* Sociedade Editora, 2001, p. 240.

[30] Idem.

[31] Moniz, Helena. "Internet e Globalização – Problemas Jurídico-Penais: notas breves". In *As telecomunicações e o direito na Sociedade de Informação*, coord. António Pinto Monteiro. Coimbra: Instituto Jurídico da Comunicação. 1999, p. 371.

[32] Verdelho, Pedro. "A nova Lei do Cibercrime." *Scientia Ivridica n.º 320. Revista de Direito* (2009), pp. 748 e 749.

[33] ***Artigo 27.º da Lei n.º 109/2009 de 15 de Setembro***

Aplicação no espaço da lei penal portuguesa e competência dos tribunais portugueses

1 — Para além do disposto no Código Penal em matéria de aplicação no espaço da lei penal portuguesa, e salvo tratado ou convenção internacional em contrário, para efeitos da presente lei, a lei penal portuguesa é ainda aplicável a factos:

a) Praticados por Portugueses, se aos mesmos não for aplicável a lei penal de nenhum outro Estado;

b) Cometidos em benefício de pessoas coletivas com sede em território português;

c) Fisicamente praticados em território português, ainda que visem sistemas informáticos localizados fora desse território; ou

d) Que visem sistemas informáticos localizados em território português, independentemente do local onde esses factos forem fisicamente praticados.

evitando-se que se caia num vazio jurídico, daí que terá de se determinar qual o direito aplicável e qual o tribunal competente.

Quanto à permanência, automatismo e repetição, a autora Vera Marques Dias explicita a permanência do facto como "a característica preponderante na ajuda à comissão do crime", determinando assim o caráter automático e repetitivo do comportamento levado a cabo pelo agente. Por outro lado, o automatismo e repetição – inerente aos computadores e sistemas informáticos – demonstram, por sua vez, ser características aliciantes e que potenciam o crescimento exponencial de condutas criminosas.[34]

On the Internet, nobody knows you're a dog (Peter Steiner)[35]*.* Esta citação emblemática vem ilustrar facilmente de que se trata o anonimato. Contrariamente ao que acontece no mundo físico, no mundo digital, os cibercriminosos conseguem manter-se anónimos. Como nota, apesar de haver uma maior facilidade em manter-se anónimo, a realidade tem demonstrado que o anonimato é mais difícil de se garantir do que se pensava. Também é nossa convicção que "o anonimato é lícito, quando usado para proteger que determinadas informações caiam em mãos erradas e periguem a segurança e provoquem prejuízos irreparáveis"[36]. Em bom rigor o anonimato depende do adversário; tome-se como exemplo o caso do Google ou da NSA, em relação às mesmas não existe grande anonimato pois têm acesso às comunicações. No entanto temos que admitir que o anonimato é um agente potenciador do cometimento de crimes. O anonimato é tão antigo quanto a Internet. Todavia, do ponto de vista mediático, foi através do grupo de ativismo social "Anonymous" que este começou a ser mais preponderante. A utilização de *software* de anonimato não tem de ser encarada forçosamente enquanto uso malicioso[37]. O anonimato traduz-se, incontestavelmente, numa dissimulação ou na utilização de uma

[34] Dias, Vera Marques. "A Problemática da Investigação do Cibercrime". In *DataVenia – Revista Jurídica Digital,* Ano 1, n.º1, ed. Joel Timóteo Ramos Pereira. DataVenia. Julho, 2012, p. 72 http://www.datavenia.pt/ficheiros/edicao01/datavenia01_p063-088.pdf (consultado 20 Novembro 2015).

[35] Expressão retirada e disponibilizada em: https://en.wikipedia.org/wiki/On_the_Internet,_nobody_knows_you%27re_a_dog (consultado a 20 Novembro 2015).

[36] Pereira, Joel Timóteo Ramos. *Direito da Internet e Comércio Eletrónico*. Lisboa: *Quid Juris* Sociedade Editora, 2001, p. 20.

[37] A este propósito, tomemos como exemplo, o Tor que consiste num *software* que estabelece uma comunicação anónima entre dois pontos de uma rede. Equiparado às camadas de uma cebola, tem como funcionalidades disponibilizadas a navegação anónima (esta aplicação é excelente para esconder a identidade, mas como todo o programa é falível; Não previne a entrega dos dados em sites, nem encripta as comunicações entre o nó de saída do circuito e o site do destino), *hidden services* (ou servidores escondidos, são servidores configurados para receber conexões de entrada através do TOR e neste caso em vez de revelar o endereço IP do servidor e, portanto a sua localização na rede, um serviço oculto é acedido através do seu "endereço cebola").

identidade falsa, ou seja, ser anónimo significa que a verdadeira identidade de uma pessoa é desconhecida. É uma característica muito apreciada no mundo digital. A este propósito, citando as palavras de Vera Marques Dias, esta é a "característica mais aliciadora, tentadora e propulsionadora", que permite que o agente possa visitar, conversar e navegar na rede sem que seja identificado[38]. O anonimato, um corolário do direito à reserva da intimidade da vida privada, é uma das características mais usuais, mais aliciadoras e mais instigadoras para a prática criminosa no mundo digital. Com efeito, a liberdade de navegação propiciada pela Internet veio trazer novas questões ao nível do direito à privacidade de cada um de nós. Indissociavelmente ligado à despersonalização, os agentes criminosos procuram minorar ou dizimar os rastos que deixam pela Internet a fim de não serem descobertos ou condenados. Portanto, o anonimato apresenta-se como um dos principais problemas associados à efetivação das responsabilidades dos agentes que cometem ilícitos, tanto criminais como civis, no ciberespaço[39]. Por conseguinte, o anonimato na rede constitui-se como um problema de difícil resolução, sendo que não é fácil obter um equilíbrio entre a proteção da privacidade e a necessidade de condenar os agentes que, protegidos pelos anonimatos, praticam os denominados "special oportunity crimes", isto é, condutas ilícitas.

Uma outra característica prende-se com a alta tecnicidade. É exigido ao investigador um alto grau de tecnicidade, para que seja viável a descodificação da origem das operações informáticas e a identificação do agente criminoso. A parca formação por parte do investigador potencia a prática de crimes de natureza informática. A insuficiência de meios e de colaboração por parte de outros ordenamentos jurídicos dificultam a investigação, bem como a recolha de provas digitais aceitáveis em sede de julgamento, isto porque, como os crimes são levados a cabo em ambiente digital, as provas são geralmente inatingíveis. Existe ainda um outro aspeto que torna a tarefa das autoridades mais difícil: o anonimato referido no ponto anterior.

E para terminar, a disseminação e potenciação dos danos. A autora Vera Marques Dias aponta para o facto de o cibercrime ser ainda mais prejudicial e perigoso, quando comparado

[38]Dias, Vera Marques, op.cit., 73.

[39] "Ciberespaço. Uma alucinação consensual diariamente experimentada por biliões de operadores legítimos, em cada país, por crianças a quem são ensinados conceitos matemáticos... Uma representação gráfica de dados extraídos de bancos de cada computador do sistema humano. Complexidade impensável. Linhas de luz alinhadas no não-espaço da mente, *clusters* e constelações de dados. Como luzes da cidade, afastando-se..." - William Gibson, *Neuromance.* http://www.citi.pt/homepages/espaco/html/william_gibson.html. (consultado 20 Novembro 2015).

com muitos crimes cometidos pela via tradicional. Por via do cibercrime é possível rentabilizar e potenciar os danos e efeitos lesivos que o crime comporta, gerando-se um círculo vicioso onde um efeito é a causa de outro efeito, originando uma sucessão de acontecimentos idênticos. Os prevaricadores utilizam a automação para potenciar os seus lucros, mesmo "não dando nas vistas", sendo mais evidente a prática da técnica do salame (revelada no filme do "Superman III"), que consiste numa operação que visa a subtração de pequenas quantias (até de cêntimos), de um grande número de vítimas, podendo obter quantias consideravelmente exorbitantes. Esta operação efetua-se sem grandes complicações e é de difícil deteção, principalmente quando envolve sistemas informáticos que processam quantidades elevadas de operações de empresas ou instituições financeiras.[40]

Estas dificuldades contribuem eficazmente para a propagação da internacionalização da criminalidade, principalmente daquela levada a cabo por via de sistemas informáticos. Na realidade propicia a prática de crimes. Um possível perfil desenhado para um autor do crime burla informática é: homem entre os 18 e 40 anos de idade; Introvertido, Socialmente isolado, arrogante, ambicioso; Frequentou ou frequenta o Ensino Superior, obtendo notas escolares acima da média; Os seus pais estão separados ou divorciados; Bom trabalhador: é um funcionário que entra antes dos outros, sai depois dos outros; não goza férias ou fica relutante em afastar-se do cargo; Tecnicamente competente; e não apresenta antecedentes criminais.[41]

[40] Prada, Ignacio Flores. *Criminalidad Informática (Aspectos sustantivos y procesales)*. Valencia:Tirant lo blanch, 2012, p. 208.

[41] Cunha, Soraia Daniela Rodrigues. " Características faciais e a interpretação de perfis criminais". Dissertação de Mestrado, Universidade de Aveiro, 2011, anexo 4.

CAPÍTULO II

1. ENQUADRAMENTO JURÍDICO-LEGAL DO CRIME DE BURLA INFORMÁTICA

1.1. Regime Jurídico da Burla Clássica

Apesar de não concordarmos na íntegra com a tese de que o tipo legal de crime de burla informática é estruturalmente uma burla ou que parte da génese da mesma, grande parte da doutrina entende que sim. Por esse motivo e também devido à pertinência de distinção das burlas informáticas das burlas cometidas pela Internet, determinamos a inclusão deste ponto.

Comete o referido crime de burla simples do artigo 217.º, n.º1 do CP "quem com intenção de obter para si ou para terceiro enriquecimento ilegítimo, por meio de erro ou engano sobre factos que astuciosamente provocou, determinar outrem à prática de atos que lhe causem ou causem a outra pessoa, prejuízo patrimonial é punido com pena de prisão até três anos ou com penal de multa". O aspeto nuclear do crime de burla materializa-se na indução em erro de alguém, isto é, implica a colaboração da vítima, resultando da mesma uma viciação da vontade de que foi objeto. Apenas é censurado a título de dolo, ou seja, para verificação do dolo é necessário, por parte do agente, a prática voluntária dos factos e o conhecimento do carater ilícito da sua conduta.

O bem jurídico protegido por esta incriminação consiste no património globalmente considerado.[42] A burla, não é portanto, crime contra a propriedade. Diferentemente do que ocorre com os crimes contra a propriedade, nos crimes contra o património em geral tem de resultar um prejuízo patrimonial enquanto elemento de crime.[43] É operado um critério de prejuízo, em que o agente atua com o ânimo de enriquecimento, resultando uma desvantagem

[42] Para este efeito cfr. Almeida Costa, A.M., *Comentário Conimbricense*, II. Coimbra Editora, 1999, p. 275.

[43] O conceito jurídico-penal de património levanta alguns problemas. Existem várias conceções em busca de um conceito "perfeito" de património. É no âmbito da burla que se evidencia a necessidade de uniformização deste conceito, isto porque, no crime de burla pressupõe-se a exigência de uma disposição de onde decorre um prejuízo. Embora não seja nosso propósito a reflexão profunda sobre a uniformização do conceito de «património», apenas ressalvamos que o conceito não deverá ser reduzido unicamente a uma soma abstrata de dinheiro. Terá que se ter em linha de conta a capacidade económica do sujeito de direito, derivada do seu domínio sobre as coisas que a ordem jurídica reconhece como elemento autónomo do tráfico económico. Com um maior rigor património será "o complexo de relações jurídicas encabeçadas por um sujeito que tem por objeto ultimo *coisa*s dotadas de *utilidade*, isto é, de capacidade de satisfazer necessidades humanas, *materiais ou espirituais*." Faria Costa. In *Comentário Conimbricense*, II. Coimbra Editora, 1999, p. 29, citando Mantovani.

patrimonial na esfera patrimonial do lesado. A burla comum é um crime de enriquecimento intencionado, sem o emprego de meios coativos. O mesmo se aplica para a burla informática.

São elementos constitutivos do crime de burla simples: erro ou engano sobre factos astuciosamente provocados, que determinem a outrem à prática de factos que lhe causem, ou a terceiro, um prejuízo patrimonial e que tenha intenção de obter para si ou para terceiro um enriquecimento ilegítimo entendido segundo o conceito de enriquecimento sem causa do artigo 473.º do CC.[44] O prejuízo patrimonial relevante corresponde, assim, a um empobrecimento do lesado, que vê a sua situação económica diminuída, e efetivamente diminuída quando comparada com a situação em que se encontraria se não tivesse ocorrido a situação determinante da lesão.[45]

A burla escreve-se no Comentário Conimbricense do Código Penal Tomo II[46] como um crime material ou de resultado, cuja consumação depende da verificação de um evento que se traduz na saída dos bens ou valores da esfera de "disponibilidade fáctica" do legítimo detentor dos mesmos ao tempo da infração. E prossegue, dizendo que, "por outro lado, a burla integra um delito de execução vinculada, em que a lesão do bem jurídico tem de ocorrer como consequência de uma muito particular forma de comportamento"[47]. Apresenta, por sua vez, contornos especiais "uma vez que se está perante algo que já se apelidou de *crime com participação da vítima*, isto é, de um delito onde a saída dos valores da esfera de disponibilidade fáctica do legítimo titular decorre, em último termo, de um comportamento do sujeito passivo, a referida autonomização do evento reporta-se tanto à conduta do agente como à ação do próprio burlado".[48]

Ao nível do processo enganatório, haverá que considerar o seguinte: a burla terá lugar aquando a utilização de um meio enganoso conducente a induzir outra pessoa num erro

---

[44] ***Artigo 473.º do CC***

1. Aquele que, sem causa justificativa, enriquecer à custa de outrem é obrigado a restituir aquilo com que injustamente se locupletou.

2. A obrigação de restituir, por enriquecimento sem causa, tem de modo especial por objeto o que for indevidamente recebido, ou o que for recebido por virtude de uma causa que deixou de existir ou em vista de um efeito que não se verificou.

[45] Dias, Jorge, relat. – Acórdão no processo 522/01.6TACBR.C2. Tribunal da Relação de Coimbra. [Em linha]. Coimbra (08-02-2012). [Consultado 20 Novembro 2015] Disponível em http://goo.gl/HO4Fcx.

[46] Almeida Costa. *Comentário Conimbricense*, II. Coimbra: Coimbra Editora, 1999, p. 277.

[47] Ibidem, p. 293.

[48] Lima, António Clemente, relat. – Acórdão no processo 4275/11.1TASTB.E1. Tribunal da Relação de Évora. [Em linha]. Évora (11-03-2014). [Consultado a 20 Novembro 2015] Disponível em http://goo.gl/M76jMe.

levando-a a praticar atos de que resultam prejuízos patrimoniais próprios ou alheios. E, portanto, é necessária a verificação de uma intercessão intersubjetiva. Mas não basta o simples emprego do meio enganoso. Deve existir uma relação causal entre os requisitos enunciados, pois que, o erro ou engano deve ser gerado através de astúcia, sendo esta um instrumento necessário para que se alcancem aqueles. Por engano ou erro deverá entender-se como a "provocação de uma falsa representação da realidade" e terá lugar "quando o agente refira factos falsos ou dissimule factos verdadeiros relevantes".[49]

Afigura-se necessário que ele "consubstancie a causa efetiva da situação de erro em que se encontra o indivíduo. De outra parte, também não se mostra suficiente a simples verificação do estado de erro: requer-se, ainda, que nesse engano resida a causa da prática, pelo burlado dos atos de que decorrem os prejuízos patrimoniais".[50] Deste modo verifica-se um duplo nexo de causalidade objetiva entre a conduta do sujeito ativo aquando o emprego do engano e a prática, pelo sujeito passivo, de atos tendentes a uma diminuição de património (próprio ou alheio) atestando-se a efetiva verificação do prejuízo patrimonial.

Exige-se impreterivelmente um ato ardiloso/astucioso por parte do agente e terá que resultar dessa ação um prejuízo patrimonial. Sem a verificação efetiva de astúcia, a conduta do agente é anómala uma vez que omitiu a prática de um ato típico instrumental, fundamental para obter um efeito legalmente relevante. Por outro lado, erro ou engano relevante, não é apenas aquele que logra o convencimento da vítima. Relevante é apurar se a vítima, sujeita ao processo enganatório, atuou conforme os desígnios do agente. Por erro, deve entender-se a falsa ou nenhuma representação da realidade concreta, que funcione como vício do consentimento da vítima. O engano, por sua vez, equipara-se à simples mentira.

Mais difícil é a definição da noção de astúcia. A mesma se poderá definir como o "aproveitamento de uma vantagem cognitiva do agente sobre o burlado que lhe permite manipular a vontade do burlado"[51]. A astúcia deverá ser reconstituída a partir de atos materiais que a revelem e evidenciem e não por referência a estados de espirito ao nível da mera motivação do agente. Na sua formulação ordinária, registada por qualquer dicionário, ela é

[49] Albuquerque, Paulo P. de. *Comentário do Código Penal.* 2.ª edição Lisboa: Universidade Católica Editora, 2010, p. 599-600.

[50] Almeida Costa. *Comentário Conimbricense*, II. Coimbra: Coimbra Editora, 1999, p. 293.

[51] Albuquerque, Paulo P. de. *Comentário do Código Penal.* 2.ª edição Lisboa: Universidade Católica Editora, 2010, p. 600.

comparada à habilidade para o mal, à manha, à sagacidade, à habilidade para enganar, à subtileza para defraudar, ao ardil, ao embuste, e à maquinação. Mais árdua, todavia, é a sua formulação jurídica. Porém, e não obstante esta dificuldade, sempre que ocorra uma atuação engenhosa por parte do agente do crime, algo ao nível do estratagema ardiloso, da encenação orientada a ludibriar que, psiquicamente, manipula o intelecto da vítima, tratar-se-á de atuação astuciosa relevante.

O segundo momento do crime de burla traduz-se na prática de atos que causem à vítima, ou a terceiro, prejuízo patrimonial e que, lhe causem empobrecimento, sendo este o momento em que o crime se consuma.

Feita esta imprescindível análise das condicionantes doutrinais gerais é altura de apreciar em concreto o crime de burla informática.

1.2. Análise Dogmática do tipo legal de crime de Burla Informática

O panorama sócio criminal tecnológico tem viabilizado um número significativo de burlas informáticas, aliás as motivações económicas fazem disparar as estatísticas referentes a crimes informáticos, sendo que o cometimento de crimes de índole económica ocupam um lugar de destaque. Os processos de burlas informáticas são de "factualidade extremamente complexa"[52], que exigem perícias e pessoal altamente especializado.

Na verdade, na última década o número de casos de crimes de índole informática tem sofrido um aumento substancial. No que respeita a alguns modos de execução, salienta o Relatório de Segurança Interna de 2014[53], o seguinte:

" Os meios de pagamento, abrangendo-se aqui as áreas de banca *online* e do *phishing*, pela ameaça que constitui ao património de empresas e de particulares, à credibilidade do sistema financeiro e ao financiamento de outras atividades criminosas;

[52] Verdelho, Pedro. " Cibercrime". In *Direito da Sociedade da Informação – Vol. IV,* Associação Portuguesa do Direito Intelectual. Coimbra Editora, 2003, p. 354.

[53] Disponível em http://goo.gl/23r2ea, p. 114, (consultado 20 Novembro 2015).

O *hacking*, em particular o que tem como alvo instituições do Estado, com consequências ao nível da proteção de dados pessoais da gestão de serviços públicos, da credibilidade do próprio Estado de Direito.

O *malware*, nomeadamente com a produção e utilização de programas maliciosos e a possibilidade de utilização em todo o tipo de dispositivos móveis, com implicação nos dois pontos anteriores. "

Respeitante ao tipo legal de crime em análise:

Verifica-se um acréscimo bastante significativo de cometimento de burlas informáticas e nas telecomunicações, com mais de 580 casos registados segundo os dados registados no Relatório Anual de Segurança Interna respeitante a 2011 (aumento de 27,4% relativamente a 2010). Relativamente ao ano de 2012, verifica-se, de igual forma, um aumento significativo de burlas informáticas e nas telecomunicações, com mais de 923 casos, ou seja, um acréscimo de 34,2%. No ano de 2014, relativamente à subida de participações, a burla informática apresenta um aumento de 30.4%.

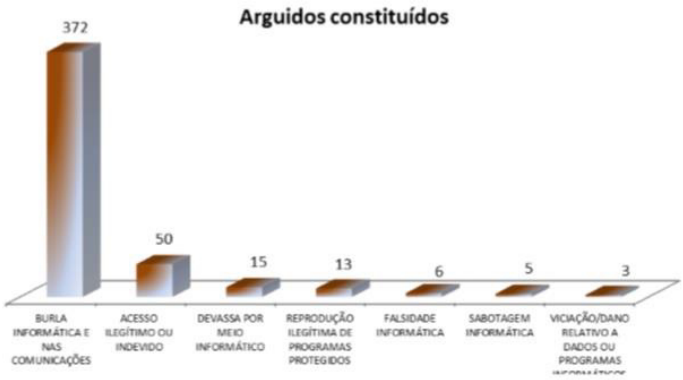

Figura i

Imagem retirada do Relatório Anual de Segurança Interna 2014

O gráfico supra apresentado corrobora o que temos vindo a afirmar acerca do tipo legal do crime de burla informática ser o delito informático com maior incidência dentro do leque dos crimes informáticos.

Tendo em consideração o gráfico supra apresentado há a tendência, e bem, de equiparar o crime de burla informática com os crimes de colarinho branco[54] ou *white-collar crime.* Pese embora o facto de ser um conceito ambíguo, é frequente considerar-se enquanto crimes geralmente cometidos por pessoas com um elevado *status* social, sem violência cujo desiderato passa pelo lucro financeiro e de difícil perceção pelo homem comum dado a alta destreza que caracteriza tão bem os criminosos mais sofisticados. Segundo Shapiro um crime de colarinho branco é um crime de índole económico cometido através da combinação de fraude, engano ou conluio.[55] Acresce Figueiredo Dias que o crime de colarinho branco "invalidou definitivamente a representação tradicional do crime como exclusivo das classes deserdadas ou desqualificadamente inseridas na sociedade"[56]. Morgado e Vegar[57] na sua obra catalogaram os crimes de colarinho branco em três classes. A primeira respeita aos crimes tributários, nomeadamente crimes aduaneiros, crimes fiscais e crimes contra a Segurança Social. O segundo, e o que nos importa, refere-se às burlas informáticas, pornografia infantil na Internet e intrusão de piratas informáticos. A terceira e última reporta-se ao peculato e corrupção, incluindo o tráfico de influências e branqueamento de capitais. Estamos inteiramente de acordo, com a categorização das burlas informáticas nos crimes de colarinho branco, pelos argumentos já expostos, por se tratar de um crime *clean*, deveras astucioso, do qual ninguém, ou quase ninguém se apercebe.

No que concerne à análise dogmática e enquadramento jurídico-penal, o crime de burla informática foi introduzido na versão do Código Penal de 1995 na senda do direito alemão, com correspondência na *Computerbetrug* (burla de computadores) do § 263-a do StGB germânico, o que decorre dos trabalhos preparatórios, onde se declara, que o tipo legal visa dotar a ordem

---

[54] O termo teve a sua origem em 1939 durante um discurso de Edwin Sutherland e o mesmo define-os como aqueles que são praticados por pessoas de grande estatuto social e de alta respeitabilidade.

[55] Santos, Cláudia Maria Cruz. *O crime de colarinho branco: da origem do conceito e sua relevância criminológica à questão da desigualdade na administração da Justiça Penal.* Coimbra Editora, 2001, p. 64.

[56] Dias, Jorge de Figueiredo e Manuel da Costa Andrade. *Criminologia: O Homem Delinquente e a Sociedade Criminógena.* Coimbra Editora, 1997, p. 33.

[57] Morgado, Maria José e José Vegar. *O inimigo sem rosto, fraude e corrupção em Portugal.* Edições D.Quixote, 2003.

jurídica portuguesa de uma disciplina idêntica à existente nos direitos germânicos e austríaco. Na verdade de acordo com José António Choclán Montalvo "na base do artigo 263-a do StGB germânico terá estado a utilização abusiva de ATMs e as dificuldades dos tipos penais tradicionais de conteúdo patrimonial, designadamente a burla, para proteger adequadamente o bem jurídico face a novas modalidades de ataque"[58].

Os motivos que levaram à inclusão do tipo legal do crime de burla informática no CP, segundo Lopes da Rocha, foram: "frequência com que semelhantes crimes são cometidos; a difícil deteção das condutas lesivas, que merecem uma repulsa social enérgica; e a insuficiência dos meios clássicos tradicionais para proteção dos interesses em jogo".[59]

Em primeiro lugar, os computadores bem como outros dispositivos eletrónicos não podem ser ludibriados e deste modo a manipulação informática propriamente dita, tendente ao enriquecimento ilegítimo do agente ou de terceiro, afasta-se do tipo clássico da burla (art. 217.º). Almeida Costa atenta no facto de a burla informática não contemplar a intervenção de outrem, no sentido de não se dirigir à manipulação da vontade de uma pessoa, tratando-se antes de um atentado direto ao património, que é, por sua vez, levado a cabo através da utilização de meios informáticos, de onde advém a sua especificidade.[60] A sua especificidade reside no facto de a burla informática só ter lugar aquando verificação de uma qualquer das condutas previstas no artigo 221.º e Rita Coelho Santos acrescenta, dizendo "(...) só relevam as ofensas que sejam cometidas através de uma das modalidades típicas (...) como formas de ação"[61].

Por um lado, a burla tradicional exige por parte do agente a "(...) realização voluntária de um ato gerador do prejuízo patrimonial por alguém(...) determinado (...) pelo comportamento astucioso do agente, induzindo-o em erro ou enganando-o sobre a realidade dos factos."[62] Acresce ainda, dizendo que nunca se poderia fazer uma interpretação extensiva da burla clássica "(...) no sentido de se entender aí incluído o engano ou o erros produzido sobre o próprio

[58] Gaspar, Henriques, relat. – Acórdão no processo 08P2817. Supremo Tribunal de Justiça. [Em linha]. Lisboa (05-11-2008). [Consultado 20 Novembro 2015] Disponível em http://goo.gl/Dvr4Ts.

[59] Monteiro, Armindo, relat. – Acórdão no processo 1008/11.6JFLSB-L1.S1. Supremo Tribunal de Justiça. [Em linha]. Lisboa (12-09-2012). [Consultado 20 Novembro 2015] Disponível em http://goo.gl/KtgLTv.

[60] Almeida Costa. *Comentário Conimbricense*, II. Coimbra Editora, 1999, p. 329.

[61] 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, p. 216.

[62] Ibidem, p. 232.

computador (...). Concordamos na íntegra, esse "alguém" que subsiste indubitavelmente na figura legal clássica não existe na burla informática; poderá eventualmente existir, por intermédio de sistemas informáticos, e que dessa relação decorra uma interferência no resultado de tratamento de dados; não obstante os elementos qualificadores da burla clássica de erro ou engano sobre factos astuciosamente provocados não são elementos integrantes da burla informática e desta forma, podemos rejeitar parcialmente a tese de que a burla informática é estruturalmente uma burla. A nossa convicção é a de que o computador surge apenas como mecanismo da ação do agente, e desta forma não poderá ser alvo de engano ou de comportamentos que classifiquem a particularidade da burla tradicional, possibilitando desta forma uma "apropriação da *pecunia* alheia através da manipulação dos sistemas informáticos"[63].

O bem jurídico protegido é de natureza iminentemente patrimonial, logo o património em geral[64]. Aliás, a proteção do património[65] é "o critério que irá permitir separar este crime de vários crimes previstos na Lei da criminalidade Informática".[66] O lesado é a pessoa que sofre o prejuízo patrimonial e não o proprietário ou utente dos dados ou programas informáticos[67]. O STJ tem seguido a orientação de que no crime de burla informática, o bem jurídico protegido não é só património (mas concretamente, a integridade patrimonial) como, ainda, a fiabilidade dos dados e a sua proteção.[68] Todavia, o STJ[69] parece ter-se inclinado para uma posição mais circunscrita do bem jurídico protegido, sustentando que o bem jurídico protegido com tal incriminação é o património. Poderia também admitir-se que vise igualmente proteger o correto

---

[63] Santos, Rita Coelho. *O Tratamento Jurídico-Penal da Transferência de Fundos Monetários através da Manipulação Ilícita dos Sistemas Informáticos – Studia Jurídica*, n.° 82. Coimbra Editora, 2005, p. 212.

[64] Almeida Costa. *Comentário Conimbricense*, II. Coimbra Editora, 1999, p. 329.

[65] Adotamos a asserção de Rita Coelhos Santos, in *O Tratamento Jurídico-Penal da Transferência de Fundos Monetários através da Manipulação Ilícita dos Sistemas Informáticos – Studia Jurídica*, n.° 82, p. 216, relativamente à qualificação do bem jurídico de património: "O património constitui, (...) um bem jurídico funcionalmente ligado à realização do homem, que merece proteção contra novas formas de ofensas, não acauteladas historicamente pelo legislador, que se encontram relacionadas com a utilização dos meios informáticos (e telemáticos) como instrumentos da ação do agente, com vista à obtenção de um enriquecimento ilegítimo, em prejuízo do titular dos valores patrimoniais atingidos".

[66] Verdelho, Pedro. " Cibercrime". In *Direito da Sociedade da Informação – Vol. IV,* Associação Portuguesa do Direito Intelectual. Coimbra Editora, 2003, p. 358.

[67] Albuquerque, Paulo P. de. *Comentário do Código Penal*. 2.ª edição Lisboa: Universidade Católica Editora, 2010, p. 599.

[68] Santos, Simas, relat. – Acórdão no processo 05P2253. Supremo Tribunal de Justiça. [Em linha]. Lisboa (06-10-2005). [Consultado 20 Novembro 2015] Disponível em http://goo.gl/TFWaq9.

[69] Gaspar, Henriques, relat. – Acórdão no processo 08P2817. Supremo Tribunal de Justiça. [Em linha]. Lisboa (05-11-2008). [Consultado 20 Novembro 2015] Disponível em http://goo.gl/Dvr4Ts.

funcionamento e a inviolabilidade dos sistemas informáticos e de informação.[70] Não obstante, seguimos o douto entendimento de Almeida Costa.

Relativamente à forma de consumação do ataque, trata-se de um crime de resultado, de resultado parcial ou cortado, sendo exigida a produção de uma perda patrimonial de alguém. Acresce-se que é " um delito de intenção ...um delito de resultado parcial ou cortado... caracterizado por uma descontinuidade entre os tipos subjetivo e objetivo, em que se requer o aludido *animus* de enriquecimento, mas que se consuma com o dano patrimonial da vítima, independentemente da efetiva verificação do benefícios económico do sujeito ativo da infração ou de terceiro"[71].

No plano da tipicidade, constitui um crime de execução vinculada. Com isto queremos dizer que a lesão do património produzir-se-á através da intromissão nos sistemas e da utilização de meios informáticos, nos quais está presente e aos quais está subjacente alguma forma de fraude ou de artificio que tenha a finalidade a especifica intenção de obter enriquecimento ilegítimo, causando a outra pessoa prejuízo patrimonial. Neste caso prescinde-se o erro ou engano em relação a uma pessoa, ou seja, a máquina não pode ser ludibriada, tal como sucede no crime de burla do artigo 217.º. Há-de estar sempre presente um erro direto com finalidade determinada, um engano ou um artifício sobre dados ou aplicações informáticas.

Acrescentamos ainda que "a coordenação entre a natureza do bem jurídico protegido e a especificidade típica como crime de execução vinculada supõe que a produção do resultado tenha de ser determinada por procedimentos e ações que sejam tipicamente vinculados na descrição específica da norma que define os elementos materiais da infração."[72] Mas prescindindo do erro ou engano em relação a uma pessoa, prevê, no entanto, atos com conteúdo material e final idêntico: manipulação dos sistemas informáticos, ou utilização sem autorização ou abusiva determinando a produção dolosa de prejuízo patrimonial.

---

[70] Graça, Pires da, relat. – Acórdão no processo 78/07.6JAFAR.E2.S1.Supremo Tribunal de Justiça. [Em linha]. Lisboa (20-10-2010). [Consultado 20 Novembro 2015] Disponível em http://goo.gl/ZT5AAk.

[71] Almeida Costa. *Comentário Conimbricense*, II. Coimbra Editora, 1999, p. 331.

[72] Gaspar, Henriques, relat. – Acórdão no processo 08P2817.Supremo Tribunal de Justiça. [Em linha]. Lisboa (05-11-2008). [Consultado 20 Novembro 2015] Disponível em http://goo.gl/Dvr4Ts.

As condutas típicas referidas no artigo 221.º, n.º1 do CP "constituem, assim, na apreensão intrínseca e na projeção externa, modos de descrição de modelos formatados de prevenção da integridade dos sistemas contra interferências, erros determinados, ou abusos de utilização que se aproximem da fraude ou engano contrários ao sentimento de segurança e fiabilidade dos sistemas."[73] Destarte, o legislador estabeleceu uma enumeração de algumas formas possíveis de conduta de ação criminosa traçando, desta forma, o *iter criminis* da burla informática.

E portanto, é nossa convicção que o tipo legal pretendeu, de igual modo, abranger a utilização indevida de máquinas automáticas de pagamento (ATM), incluindo os casos de manipulação ou utilização indevida no sentido de utilização sem a vontade do titular. Tem entendido grande parte da jurisprudência que há burla informática, aquando um agente, à revelia do legítimo titular e sem autorização deste, furta e utiliza indevidamente o seu cartão de multibanco, levanta dinheiro em ATM[74] ou faz pagamentos em POS[75]. Aliás essa é a posição de Paulo Pinto de Albuquerque que afirma dizendo 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 eletrónica (*smart card, pay before card*) com o PIN de outrem" constitui também conduta típica prevista no artigo 221.º do CP. Seguimos o douto entendimento de Paulo Pinto de Albuquerque. No entanto, para Pedro Verdelho, a questão é mais difícil. No caso em apreço, Pedro Verdelho[76] entende haver crime de furto, porque para que a situação ora descrita consubstanciasse o crime de burla informática seria necessário que houvesse uma interferência no resultado do tratamento de dados ou houvesse uma utilização incorreta ou incompleta de dados, utilização de dados sem autorização ou intervenção por qualquer outro modo não

[73] Gaspar, Henriques, relat. – Acórdão no processo 06P1942.Supremo Tribunal de Justiça. [Em linha]. Lisboa (20-09-2006). [Consultado 20 Novembro 2015] Disponível em http://goo.gl/8aAkVU.

[74] As siglas denominam-se como *Automated Teller Machine* que é comumente designada por caixa automática, que faculta diversos serviços para além do levantamento automático. Segundo informação disponibilizada pelo Banco de Portugal, CA ou ATM é um terminal de uma rede do sistema bancário que permite ao cliente efetuar diversos tipos de operações que variam consoante as características do cartão de que se é detentor. Mas, de grosso modo, permitem operações correntes, tal como levantamentos, consultas, pagamentos e depósitos, entre outras.

[75] POS, designação para *Point of Sale,* que corresponde ao Terminal de Pagamento Automático – TPA. Consiste num dispositivo de aceitação de cartões que permite realizar pagamentos por via eletrónica que faz a leitura dos dados constantes do cartão para autorização da operação e recolha de elementos de transação para processamento. Através do mesmo, há a emissão de talões com informações sobre os dados da transação após efetuar a digitação do código PIN.

[76] Verdelho, Pedro. " Cibercrime". In *Direito da Sociedade da Informação – Vol. IV,* Associação Portuguesa do Direito Intelectual. Coimbra Editora, 2003, p. 360.

autorizada no processamento. Perguntamos nós... Se afigurarmos um caso como o descrito no parágrafo anterior, não haveria utilização de dados sem autorização? Ora tendo acesso à conta bancária, por via de uma ATM, não estaria o criminoso a interagir no processamento de dados? Julgamos que sim! Deste modo, preencheria a conduta típica de utilização de dados sem autorização. Estamos em desconformidade com a opinião de Pedro Verdelho.

Quanto à utilização do PIN, afirma o mesmo autor que é necessário saber se o mesmo é ou não abrangido pelo conceito de dados informáticos, porém a definição ainda não se encontra descrita na lei portuguesa. O mesmo autor refere que, o código PIN não se inclui no conceito de dados informáticos, que vem definido na Convenção sobre o Cibercrime, no artigo 1.º, alínea b)[77] e portanto que não preenche os elementos tipo do crime de burla informática. Ainda que considerando que o código PIN não se inclui no conceito de dados informáticos,[78] a utilização do mesmo por pessoa não autorizada em caixa automática não preenche o tipo de «utilização de dados sem autorização»? Achamos nós que sim, bem como a grande parte da jurisprudência, portanto quanto a esse aspeto não teceremos mais considerações. A integração (ou não) do conceito de PIN no conceito de dados informáticos não é, a nosso ver, relevante para a aferição da atividade delituosa na conduta prevista no preceito legal.

Relativamente ao tipo de ilícito objetivo do crime previsto no n.º 1, é exigido que "(...) a ofensa ao património se realize através da utilização de meios informáticos (...)[79]" e consiste na interferência no resultado de tratamento de dados, através da: 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, causando desse modo, prejuízo patrimonial.

---

[77] «Dados informáticos» qualquer representação de factos, informações ou conceitos numa forma adequada para o processamento informático, incluindo um programa que permita a um sistema informático executar uma função;

[78] Pelo contrário, entendemos admitir que o conceito de Código PIN poderá integrar a definição de «dados pessoais» constantes no artigo 2.º, al.a) da *Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados*, através de interpretação extensiva porque só assim é que o espirito da lei se verifica na totalidade. Consideramos que o Código PIN (*Personal Identification Number*) além de ser uma senha numérica (com quatro algarismos) é um número de identificação pessoal que permite ao respetivo titular aceder a um determinado terminal de multibanco. O nosso entendimento é o de que o Código PIN consiste de facto num número de identificação pessoal, logo tratar-se-á de um dado pessoal.

[79] 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, p. 239, citando Almeida Costa.

Uma das características diferenciadoras em relação à burla tradicional, que consiste na afetação direta em relação a uma pessoa que pode ser cometida por via de qualquer erro ou engano quanto ao que o agente provocou de forma astuciosa, é a de que na burla informática só poderá haver consumação do crime aquando a verificação e por qualquer um dos meios previstos na norma incriminadora. Desse modo, a ofensa ao património terá que se consumar através da utilização de meios informáticos, desde que, não subsumíveis ao *modus operandi* típico da burla tradicional.[80] Assim, "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".[81]

Relativamente às modalidades típicas de manipulação informática:

A interferência no resultado do tratamento de dados é, "por um lado, a consequência necessária da interferência no processamento de dados através dos modos de execução do crime-referidos na norma-, e, por um lado, a causa do prejuízo patrimonial"[82]. Melhor dizendo que a interferência no resultado do tratamento de dados não se consubstancia como uma das modalidades típicas previstas no modelo normativo, mas antes a consequência necessária através de uma das "condutas geradoras de prejuízo patrimonial"[83].Para o efeito, exige-se a verificação de um nexo de causalidade entre a manipulação informática e a interferência no resultado do tratamento de dados e entre a última e o prejuízo patrimonial que dela decorre.

Refere ainda Paulo P. de Albuquerque que a estruturação do programa informático é incorreta, quando ela é "contrária à finalidade do programa informático, produzindo as novas instruções resultados objetivamente contrários à finalidade do programa. A estruturação pode ter lugar pela manipulação de um programa já existente quer pela criação de um programa que não produz resultados falsos". Por exemplo, por manipulação do *browser*. Acresce ainda Rita Coelho Santos que "a configuração incorreta do programa pode concretizar-se na sua total ou parcial reestruturação, no aditamento, alteração ou supressão de fases do programa, na introdução de

[80] Idem.

[81] Albuquerque, Paulo P. de. *Comentário do Código Penal.* 2.ª edição Lisboa: Universidade Católica Editora, 2010, p. 609.

[82] Idem.

[83] Santos, Rita Coelho, op. cit., 242.

novas instruções, (...) na alteração das condições de validade do controlo ou na alteração do "running time "do programa"[84].

Por seu turno, refere ainda o mesmo autor que a utilização incorreta de dados "consiste na introdução de dados que não correspondem à realidade, como por exemplo na introdução de dados de pessoas que não existem", " 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 informático ou em suportes digitais móveis, como disquetes, CD-ROM, cartões magnéticos ou eletrónicos". Por outro lado, a utilização incorreta de dados poderá consistir, segundo Rita Coelho Santos[85], numa manipulação do *input* da qual poderá resultar um acréscimo, modificação ou eliminação de dados.

Quanto à utilização de dados sem autorização traduz-se na utilização de dados alheios com vista a obtenção de uma vantagem patrimonial[86] e "implica a violação de regras de acesso aos dados, sem que a integridade desses dados seja afetada. O exemplo típico consiste na utilização de um cartão de débito e respetivo código em caixas não automáticas por pessoas não autorizadas pelo titular, com intenção de obter um enriquecimento ilegítimo"[87]. Desta forma a burla informática advirá da "interferência no tratamento de dados em consequência da utilização não autorizada de dados"[88]. Por outro lado, José de Oliveira Ascensão afirma que haver ou não utilização é irrelevante, porque o que releva é o meio ardiloso de manipulação de dados ou do resultado.[89]

A intervenção por qualquer modo não autorizado no processamento de dados "inclui a interferência no processo mecânico do sistema informático"[90]. Esta conduta abrange manipulações de *hardware* que se materializam em interferência sobre as instruções de

---

[84] 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, p. 245.

[85] Ibidem, p. 246.

[86] A vantagem patrimonial não significa necessariamente a obtenção de dinheiro na sua conceção tradicional, terá que se considerar para o efeito o dinheiro eletrónico, que é assegurado pelas instituições financeiras assegurando do mesmo modo a sua autenticidade.

[87] Albuquerque, Paulo P. de. *Comentário do Código Penal.* 2.ª edição Lisboa: Universidade Católica Editora, 2010, p. 609.

[88] 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, p. 253.

[89] Ascensão, José de. " Criminalidade Informática". In *Direito da Sociedade da Informação – Vol. II,* Associação Portuguesa do Direito Intelectual. Coimbra Editora, 2001, p. 216.

[90] Albuquerque, Paulo P. de. *Comentário do Código Penal.* 2.ª edição Lisboa: Universidade Católica Editora, 2010, p. 610.

processamento de dados ou na alteração do processo mecânico do programa informático bem como inclui aquela conduta em que se aciona uma caixa automática através de um programa de computador obtido de forma ilegal. Não obstante, terá que se ter em consideração que existe uma certa corrente doutrinal que considera que a Internet constitui um meio através do qual interfere por qualquer modo não autorizado no processamento de dados. [91]

Quanto ao tipo subjetivo admite o mesmo qualquer modalidade de dolo. A consumação do crime verifica-se quando o prejuízo patrimonial efetivo (empobrecimento) ocorre e não quando se interfere nos dados ou programa informático. Sobre a intenção de obter enriquecimento ilegítimo, cabe referir que tal como sucede no crime de burla, " o tipo inclui ainda um elemento subjetivo adicional: a intenção de obter, para si ou para terceiro, um enriquecimento ilegítimo"[92], e portanto, um dolo específico na ação do agente, o *animus lucrandi*. É um crime de resultado cortado, pelo que valorará apenas a vontade obter determinada vantagem patrimonial, isto é, para efetiva consumação do crime não terá que ocorrer necessariamente um enriquecimento por parte do agente ou de terceiro. Por seu turno, enriquecimento patrimonial pode "consistir num aumento do património, numa diminuição dos débitos ou na poupança de encargos ou despesas" Para Taipa de Carvalho a "intenção de enriquecimento" corresponde a um dolo direto ou necessário, em relação ao enriquecimento.[93] Não obstante, terá que se considerar a imprevisibilidade das consequências da manipulação informática, pois nem sempre é possível ao agente prever e controlar o resultado da sua conduta. Posto isto ter-se-ia que considerar a possibilidade de imputar ao agente dolo a título eventual.

Importa salientar que, burla informática não é sinónimo de burla cometida através da Internet, porquanto, para existir burla informática é necessária a verificação dos seus elementos típicos. Dizendo melhor, não obstante serem praticadas com recurso a meios informáticos, não tem correspondência direta com a tipicidade do tipo legal de burla informática, nem lhe confere nenhuma relação de especialidade. A burla informática difere da burla tradicional na medida em que não se verifica o elemento intersubjetivo que qualifica a burla tradicional, e por conseguinte também não existirá participação da vítima. Na verdade, na burla tradicional o instrumento

[91] Santos, Rita Coelho, op.cit., p. 260.

[92] Albuquerque, Paulo P. de, op.cit., p. 602.

[93] Albuquerque, Paulo P. de. *Comentário do Código Penal.* 2.ª edição Lisboa: Universidade Católica Editora, 2010,p. 602, citando Taipa de Carvalho e António Barreiros.

informático é o meio engenhoso para enganar ou induzir em erro, do qual irá resultar um prejuízo patrimonial, tal não sucede no âmbito da burla informática uma vez que" (...) o prejuízo patrimonial decorre diretamente de uma operação informática, totalmente automatizada ou em que a intervenção humana não corresponde a um controlo efetivo e crítico do resultado do tratamento informático dos dados"[94].

1.3. Diferenças entre o crime de burla informática e de burla nas telecomunicações

O artigo 221.º do CP prevê dois crimes, por um lado no n.º 1 o crime de burla informática e por outro lado no n.º 2 o crime de burla nas telecomunicações, que contrariamente ao primeiro foi introduzido na revisão do CP em 1998. O último não é objeto do estudo, mas não poderíamos deixar de o abordar, tecendo, portanto, algumas considerações.

Uma consideração importante subjaz na extensão do tipo ao domínio das telecomunicações. Estão previstos no mesmo preceito legal, mas são crimes que se distinguem não só pela natureza mas pelos diferentes bens jurídicos protegidos, e portanto defendemos que deveria de haver duas construções normativas autónomas para cada um dos crimes.

Segundo o entendimento de Pedro Verdelho[95], a vertente patrimonial é um dos critérios que vai permitir diferenciar o crime de burla informática do da burla nas telecomunicações, isto porque, tendo em conta o elemento subjetivo, a burla informática prevê um enriquecimento ilegítimo e portanto da atuação criminosa advirá uma vantagem patrimonial, já a burla nas telecomunicações prevê um benefício ilegítimo. Etimologicamente, ambos termos não são coincidentes, tome-se como exemplo "a utilização imediata pelo agente de sistemas de comunicações, sem para isso ter que suportar o respetivo custo". No caso em apreço, o benefício não corresponde nem poderá ser considerado enriquecimento e não pode considerar-se haver necessariamente enriquecimento através do valor do custo da comunicação. Segundo o mesmo autor "só haverá efetivo enriquecimento se o agente do crime, não sendo bem-sucedido,

[94] 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, p. 214.

[95] Verdelho, Pedro. " Cibercrime". In *Direito da Sociedade da Informação – Vol. IV,* Associação Portuguesa do Direito Intelectual. Coimbra Editora, 2003, p. 358.

estiver disponível para suportar o custo da comunicação, o que em boa parte desses casos não acontece"[96].

Quanto à diferença de bens jurídicos: na burla nas comunicações o bem jurídico engloba não só o património como também o "normal funcionamento ou exploração de serviços de comunicações".

As condutas típicas também diferem do n.º 1 para o n.º 2, isto é, incluem-se, no n.º 2 dispositivos eletrónicos ou outros meios. A burla de comunicações, diferentemente do que sucede na burla informática, pode verificar-se através da manipulação de *hardware* [97] ou outras estruturas físicas de telecomunicações. A burla de comunicações assenta, ainda no facto, de só poder ser consumida nos casos em que se utilizem programa ou outros dispositivos ou meios que tenham como desígnio a perturbação de um serviço de comunicações. Tal não sucede na burla informática, que não se encontra inscrita por um critério restritivo, pois a mesma pode ocorrer em relação a qualquer atividade humana.

Quanto ao lesado pelo crime, resulta da leitura da lei que o mesmo não tem de ser necessariamente o operador das telecomunicações; sê-lo-á no caso de resultar de um impedimento ou dificuldade na normal faturação de serviços; pode ser o respetivo utilizador de um serviço, nos casos em que se existe interferência entre o utilizador e o servidor.

1.4. Crimes aparentados: questão de concurso?

Na senda do pensamento de Figueiredo Dias "sempre que no mesmo processo penal (...) o comportamento global imputado ao agente – traduza-se ele numa unidade ou pluralidade de ações – preenche mais do que um tipo legal de crime, previsto em mais que uma norma concretamente aplicável, ou preenche várias vezes o mesmo tipo legal de crime previsto pela mesma norma concretamente aplicável: artigo 30,º, n.º1 do CP"[98].

---

[96] Idem.

[97] *Hardware* compõe-se por componentes/suportes físicos; É a parte física de um computador incluindo os componentes elétricos/eletrónicos, os componentes eletromecânicos e os componentes mecânicos. Por seu turno, entende-se por *software* entende-se, em sentido lato, como todos os programas e procedimentos relacionados que se podem utilizar num dado sistema de computador para sua exploração.

[98] Figueiredo Dias, Jorge. *Direito Penal: parte geral, tomo I*. 2.ª edição. Coimbra Editora, 2007, p. 1005.

Através da unidade ou pluralidade de ações é possível delimitar o concurso efetivo de crimes das situações em que não existe concurso efetivo de crimes. No primeiro caso, existe uma pluralidade de crimes através da mesma ação violadora de várias normas penais ou da mesma norma repetidas vezes (concurso ideal) ou de várias ações que preenchem automaticamente vários crimes ou várias vezes o mesmo crime (concurso real). No segundo, são os casos de concurso aparente e de crime continuado.[99]

1.4.1. Burla

Não faz muito sentido fazer este tipo de abordagem, pelo simples facto de subsistir uma relação de exclusão dados os diferentes modos de execução, e porque entre ambos existe uma relação de exclusividade ou de alternatividade[100].

1.4.2. Furto

Este concurso respeita àqueles casos em que um terceiro se apodera de cartão bancário contra a vontade do respetivo titular, fazendo-o coisa sua, sem consentimento e à revelia do ofendido. Tendo na sua posse o cartão bancário furtado, e agindo de forma deliberada, livre e consciente e tendo perfeito conhecimento de que, para tanto, não estava autorizado, o agente tendo conhecimento do código PIN (muitos encontram o código PIN escrito em suporte físico junto do cartão ou memorizando o mesmo nas mais variadas circunstâncias) efetua levantamentos em numerário, ou procede a pagamentos em POS, não estando para tal autorizado, resultando de tais transações um prejuízo ao ofendido.

---

[99] Gaspar, Henriques, relat. – Acórdão no processo 06P1942. Supremo Tribunal de Justiça. [Em linha]. Lisboa (20-09-2006). [Consultado 20 Novembro 2015] Disponível em http://goo.gl/8aAkVU.

[100] Segundo a doutrina dominante existem três categorias acerca das formas de unidade de lei, a da especialidade, a da subsidiariedade e a da consumpção. "Na opinião de Klug, existem unicamente três formas lógicas de relacionamento dos tipos legais enquanto "conceito de classes": a relação de exclusão (ou alternatividade), a da inclusão (ou subordinação) e a de interferência (ou sobreposição). Sendo certo que a primeira dessas relações – a de exclusão – acaba por conduzir à aplicabilidade de uma só das normas, apenas as relações de inclusão e de interferência podem suscitar o problema da unidade da lei (...) isto é, no sentido de encontrar uma norma prevalecente cuja aplicação afasta a aplicação das restantes". *In* Figueiredo Dias, Jorge. *Direito Penal: parte geral, tomo I*. 2.ª edição. Coimbra Editora, 2007, pp. 993-994.

Afigura-se, portanto a consumação de dois crimes, por um lado o crime de furto (subtração de cartão bancário da esfera do respetivo titular) e o crime de burla informática (o agente logrou efetuar os aludidos levantamentos em numerário e pagamentos em POS, operados por via de programa informático, mediante a utilização de um cartão bancário).

Se a sua conduta preencheu os elementos típicos do crime de furto e do crime de burla informática, entendemos haver nestes casos uma relação de concurso efetivo entre o crime de furto e o crime de burla informática.

1.4.3. Roubo

Nesta hipótese afiguram-se aquelas situações em que o lesado ao recear pela sua vida e integridade física, acaba por fornecer os cartões bancários e respetivos código de acesso. Os agentes do crime agem com o propósito de se apropriarem de bens e valores, logrando de benefícios que não lhes eram devidos, pertencentes aos lesados através do emprego da força física e cientes de que a sua conduta era contrária à lei e que aquelas importâncias não lhes pertenciam, através da utilização ilegítima de dados informáticos.

No crime de roubo os bens jurídicos assegurados pelo tipo são de natureza patrimonial (direito de propriedade e de detenção) e a liberdade individual, a integridade física e a vida no crime de burla informática os bens jurídicos tutelados é o património e a fiabilidade dos dados e a sua proteção. O conhecimento do código e obtenção do respetivo cartão resulta de uma ameaça séria contra a integridade física das pessoas e não de uma ação que se destinava à manipulação, intervenção ou engano do sistema informático.

Considerando estes dois tipos, consideramos haver concurso efetivo quando o agente obriga a vítima a entregar-lhe o cartão bancário e a revelar-lhe o Código PIN tendo de seguida levantado dinheiro em caixas ATM, ou então pagamentos em POS, sem para tal estar autorizado, com a intenção de obter uma vantagem patrimonial.

1.4.4. Acesso ilegítimo

Por seu turno, o acesso ilegítimo consubstancia um crime de natureza informática, o que tal não sucedia até aqui. Não se encontra previsto no nosso CP, mas no artigo 6.º da LC, diz respeito à infração relativa às ameaças à segurança (confidencialidade, integridade e disponibilidade) dos sistemas informáticos, sendo que o bem jurídico protegido é a segurança do sistema informático. Note-se, porém, que o conceito uniforme do bem jurídico tem "(...) motivado discórdia entre autores e os tribunais"[101], no entanto, segundo Pedro Freitas "(...) a incriminação vai no sentido de perspetivar como matéria protegida a inviolabilidade dos sistemas informáticos(...)"[102].

O *modus operandi* típico assenta naqueles casos em que o agente consegue " (...) aceder ao sistema informático da vítima à sua revelia e sem o seu conhecimento, podendo controlar remotamente o seu computador, através da disseminação de um vírus informático, desenvolvido especificamente para uma finalidade bem definida, que se irá traduzir na captura dos elementos de segurança bancários do lesado, mas que concomitantemente "abre as portas" aos prevaricadores para extraírem todo o tipo de informação que pretenderem."[103]

Posto isto, suscita-nos a questão de eventual existência de concurso de normas entre os crimes de acesso ilegítimo e burla informática.

Por um lado, haverá quem entenda que, entre os dois crimes existe uma relação de concurso aparente (consumpção), como é a douta opinião de Paulo Pinto de Albuquerque, e de Rita Coelho Santos. Seguimos o entendimento destes últimos pois considera-se que a concretização do crime de burla informática (nem sempre, mas em grande parte) pressupõe, inicialmente, aceder ilegitimamente a determinado sistema, pelo que seria absorvido pelo consagrado no artigo 221.º, n.º1 do CP - consumpção pura. Na verdade, para efetivar o desejo dos agentes do crime, que se traduz, na maioria das vezes na subtração de parcelas de dinheiro,

[101] Freitas, Pedro Miguel. "Breves nótulas sobre o crime de acesso ilegítimo previsto na Lei do Cibercrime". In *Estudos em comemoração dos 20 anos da Escola de Direito da Universidade do Minho*, ed.Mário Ferreira Monte, et al., pp. 565-585, Coimbra Editora, 2014, p. 574.

[102] Ibidem, p. 578.

[103] Teixeira, Paulo Alexandre Gonçalves. " O Fenómeno do Phishing – Enquadramento Jurídico-Penal". Dissertação de Mestrado, Universidade Autónoma de Lisboa, 2013, p. 34.

terão de numa fase inicial "infecionar" o computador de forma a conseguir aceder aos dados pessoas do lesado, logo a burla informática só se verificaria caso se verifique a consumação do crime de acesso ilegítimo. Poder-se-á pensar que o acesso ilegítimo tratar-se-á de atos de execução prévios, na medida que houve necessidade na criação de um programa informático para o efeito, bem como de *malware* (nomeadamente cavalo de Tróia).

No entanto segundo outro autor[104], o mesmo considera que entre o tipo legal de crime de burla informática e acesso ilegítimo existe uma relação de concurso efetivo, por " (...) no fenómeno ora em apreço (*phishing* (...) não se poder reduzir o efeito do ilícito do art. 6º a um mero ato de execução da burla informática e nas comunicações, já que, se por um lado estes atos são essenciais para a consumação da burla, também é certo que os agentes do crime terão efetivamente um acesso livre a uma séria de dados pessoais da vítima, guardados no seu computador, que não cessam na mera captura dos seus elementos bancários".

1.4.5. Falsidade Informática

Também neste caso, há divergências quanto a relação de concurso entre a burla informática e falsidade informática. Para Rita Coelho Santos [105], à luz da antiga redação do art. 4º da LCI (...) a falsidade informática (atualmente art. 3º da LC)[106] pode constituir uma forma de

---

[104] Teixeira, Paulo Alexandre Gonçalves. " O Fenómeno do Phishing – Enquadramento Jurídico-Penal". Dissertação de Mestrado, Universidade Autónoma de Lisboa, 2013, p. 36 e ss.

[105] 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, p. 288.

[106] ***Artigo 3.º***

Falsidade Informática

1 — Quem, com intenção de provocar engano nas relações jurídicas, introduzir, modificar, apagar ou suprimir dados informáticos ou por qualquer outra forma interferir num tratamento informático de dados, produzindo dados ou documentos não genuínos, com a intenção de que estes sejam considerados ou utilizados para finalidades juridicamente relevantes como se o fossem, é punido com pena de prisão até 5 anos ou multa de 120 a 600 dias.

2 — Quando as ações descritas no número anterior incidirem sobre os dados registados ou incorporados em cartão bancário de pagamento ou em qualquer outro dispositivo que permita o acesso a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado, a pena é de 1 a 5 anos de prisão.

3 — Quem, atuando com intenção de causar prejuízo a outrem ou de obter um benefício ilegítimo, para si ou para terceiro, usar documento produzido a partir de dados informáticos que foram objeto dos atos referidos no n.º1 ou cartão ou outro dispositivo no qual se encontrem registados ou incorporados os dados objeto dos atos referidos no número anterior, é punido com as penas previstas num e noutro número, respetivamente.

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 efetivo de crimes".

É também nossa convicção, bem como de Paulo Pinto de Albuquerque que subsiste entre estes dois tipos legais de crime uma relação de concurso aparente, mais propriamente de consumpção pura.

Ao invés, e tendo em conta que ocorre aquando a criação de uma página web falsa em tudo idêntica à página oficial da instituição bancária, e ao acederem ao mesmo julgando que se trata da página legítima do banco " (...) preenche os elementos objetivos necessários para fazer com que o seu autor incorra na prática do crime de falsidade informática." Segundo este autor, por se tratar de bens jurídicos diferentes não se poderá falar numa relação de concurso aparente. [107]

Terá, porém, que se considerar haver coincidência, ainda que parcial, quanto ao bem jurídico protegido tanto pela burla informática como pela falsidade informática, porquanto a burla informática para além de proteger o património visa proteger, ainda que secundariamente, o correto funcionamento e a inviolabilidade dos sistemas informáticos.

1.4.6. Falsificação de cartão de crédito

Estes casos reportam-se àquelas situações, como veremos mais adiante, da utilização de técnica de *skimming*, que segundo a nossa análise, se trata de um modo de manifestação e

---

4 — Quem importar, distribuir, vender ou detiver para fins comerciais qualquer dispositivo que permita o acesso a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado, sobre o qual tenha sido praticada qualquer das ações prevista no n.º2, é punido com pena de prisão de 1 a 5 anos.

5 — Se os factos referidos nos números anteriores forem praticados por funcionário no exercício das suas funções, a pena é de prisão de 2 a 5 anos.

[107] Teixeira, Paulo Alexandre Gonçalves. " O Fenómeno do Phishing – Enquadramento Jurídico-Penal". Dissertação de Mestrado, Universidade Autónoma de Lisboa, 2013, p. 23.

burla informática. *Skimming* permite regravar dados dos cartões bancários noutros cartões que contenham banda magnética que depois permitem as mais variadas operações. É feito normalmente em caixas ATM, ou até em pontos de venda (POS). Os agentes do crime recolhem e gravam as informações constantes nas respetivas bandas magnéticas, isto é a duplicação dos caracteres de identificação eletrónica codificados na banda magnética efetuando assim cópias das mesmas em cartões que contenham banda magnética e até mesmo cartões validamente adquiridos através de uma instituição bancária, para depois serem utilizados em terminais de pagamento.

O acórdão 1008/11.6JFLSB-L1. do STJ profere que" a falsificação de cartões de crédito, em aumento exponencial entre nós desde 2007, origina insegurança e abala a credibilidade desses meios de pagamento, minando os alicerces da vida em comunidade." [108]

A falsificação de cartão bancário inclui-se na segmentação do artigo 256º, nºs 1, als. e) e f) e n.º 3, com referência às als. a) e c) do art. 255º, ambos do CP. A falsificação de cartões origina a insegurança e consequente falta de credibilidade nesses meios de pagamento. Por outro lado, consubstancia o crime de contrafação de título equiparado a moeda, a interferência na banda magnética do cartão bancário.

Acresce dizendo que os agentes tinham "perfeito conhecimento de que ao utilizarem os códigos de acesso ao sistema informático das máquinas/terminais visa/multibanco introduziam no mesmo dados que lhes permitiam desencadear o acesso aos dados bancários constantes da banda magnética manipulada, que pertenciam a instituições bancárias e a terceiros a que estavam adstritos, o que lhes possibilitava o débito dos pagamentos que efetuavam".[109] Utilizando os dados bancários em seu proveito, sem o conhecimento do legítimo titular e sem que para o efeito tivesse autorização, resultando dessa ação uma subtração e uma vantagem patrimonial decorrente de uma deslocação patrimonial indevida conduze-nos à qualificação de um crime de burla informática.

É nosso entendimento, à semelhança do que o pensamento jurídico tem entendido, nomeadamente Paulo P. de Albuquerque, que existe uma relação de concurso efetivo entre o

[108] Monteiro, Armindo, relat. – Acórdão no processo 1008/11.6JFLSB-L1.S1. Supremo Tribunal de Justiça. [Em linha]. Lisboa (12-09-2012). [Consultado 20 Novembro 2015] Disponível em http://goo.gl/CJVIyM.

[109] Idem.

crime de burla informática e falsificação de documento, no caso em que o agente da burla seja também o falsificador do cartão bancário.

1.4.7. Contrafação, imitação e uso ilegal de marca[110]

Através do *phishing* e do *pharming* são técnicas muito apreciadas pelos prevaricadores que, inadvertidamente, acedem aos elementos constantes na respetiva conta, através da introdução das respetivas credenciais pelo próprio utilizador.

A reprodução de uma página de uma instituição bancária é, geralmente, muito credível e fiável; e quando não o é, na grande esmagadora das vezes, o incauto julga que o banco tem uma novo *design* e arquitetura da página do banco. A introdução na página de elementos em tudo semelhantes aos da página oficial, como por exemplo, a introdução de um logótipo praticamente igual ao legítimo, os agentes do crime incorrem na prática do crime referido, por violação do constante das alíneas a),b) e c) do artigo 322.º do CPI.

Convém ter em linha de conta que a marca se traduz numa representação ou um sinal distintivo, de forma a individualizar o serviço, com vista a proteger o consumidor de risco de confusão em relação a outras marcas concorrentes. Ora, a nosso ver, a utilização de logótipo ou marca das instituições financeiras na mensagens de *e-mail* e nas páginas de internet traduziram-se no *modus operandi*, ou em atos de execução para prossecução do crime de burla informática, ou seja, foram um meio necessário para a consumação do crime de burla informática.

---

[110] ***Artigo 323.º do DL n.º36/2003, de 5 de Março- Código da Propriedade Industrial***

Contrafação, imitação e uso ilegal de marca

É punido com pena de prisão até três anos ou com pena de multa até 360 dias quem, sem consentimento do titular do direito:

a) Contrafizer, total ou parcialmente, ou, por qualquer meio, reproduzir uma marca registada;

b) Imitar, no todo ou em alguma das suas partes características, uma marca registada;

c) Usar as marcas contrafeitas ou imitadas;

d) Usar, contrafizer ou imitar marcas notórias cujos registos já tenham sido requeridos em Portugal;

e) Usar, ainda que em produtos ou serviços sem identidade ou afinidade, marcas que constituam tradução ou sejam iguais ou semelhantes a marcas anteriores cujo registo tenha sido requerido e que gozem de prestígio em Portugal, ou na Comunidade Europeia se forem comunitárias, sempre que o uso da marca posterior procure, sem justo motivo, tirar partido indevido do carácter distintivo ou do prestígio das anteriores ou possa prejudicá-las;

f) Usar, nos seus produtos, serviços, estabelecimento ou empresa, uma marca registada pertencente a outrem.

Para concluir, não nos restam dúvidas que tratar-se-á de uma relação de concurso aparente de consumpção, onde o crime de burla informática absorve o crime de contrafação, imitação e uso ilegal de marca.

1.5. Breves considerações do enquadramento do tipo legal de crime de burla informática no Direito Comparado - Alemanha, Espanha, Itália

Resta-nos saber como é desenvolvida a burla informática, em certos ordenamentos jurídicos europeus. Sabemos que, devido à Convenção da cibercriminalidade, existe uma aproximação e harmonização legislativa imposta pela mesma, quanto à legislação de crimes informáticos. Não obstante, verificam-se algumas diferenças.

A maior parte da doutrina do direito europeu continental admite que o crime de burla informática deve ser estudado intimamente ligado ao crime de burla tradicional. No entanto, as opiniões dividem-se na determinação dos "limites" dessa proximidade. Por um lado, Alemanha e Portugal fazem uma descrição "exaustiva" dos comportamentos típicos, por outro lado, Itália e Espanha utilizam "definições gerais"[111].

Na Alemanha, o comportamento verificado na burla informática encontra dificuldades de aplicação da incriminação da burla clássica aos casos de burla informática, porquanto o crime de burla tradicional pressupõe o engano de uma pessoa, o mesmo não sucede nem será aplicável aos casos de manipulação informática. E por isso, introduziu-se um tipo legal destinado a apenas à incriminação da atividade dolosa por via de manipulação de sistemas informáticos totalmente automatizados, em que o prejuízo patrimonial decorre diretamente da manipulação informática. [112] A especificidade deste ordenamento jurídico respeita à descrição enumerativa das condutas típicas que consubstanciam o crime de burla informática. O Código Penal Alemão na § 263a contempla "quatro modalidades". A utilização de uma descrição extensa, detalhada e enumerativa permite a aferição concreta de determinadas ações ao preceituado na lei, sendo

[111] Hoyos, Gustavo Balmaceda. "El delito de estafa informática en el derecho europeo continental." *Revista de Derecho y Ciencias Penales* n.°17 (2011):111-149, p. 118.

[112] Santos, Rita Coelho. *O Tratamento Jurídico-Penal da Transferência de Fundos Monetários Através da Manipulação Ilícita dos Sistemas Informáticos – Studia Jurídica, n.°82*. Coimbra Editora, 2005, p. 237-238.

mais fácil a atribuição de determinado crime a determinada conduta, evitando desta maneira, um vazio legal.

Tendo em conta que a burla informática tem origem na *Computerbetrug*, salienta Rita Coelho Santos que "(...) atualmente, a posição doutrinal e o *Bundesgerichshof* englobam, na utilização não autorizada de dados, a utilização abusiva de cartões de crédito ou de débito por terceiro não autorizado, para efetuar pagamentos, através de terminais de POS ou levantamentos de numerário, através das ATMs"[113]. Na interpretação da doutrina alemã, segundo a mesma autora a expressão "utilização não autorizada de dados" visaria precisamente aplicar-se a estes casos não deixando de satisfazer, do mesmo passo, a exigência legal da interferência no resultado do tratamento de dados, na medida em que o funcionamento de uma ATM exige a introdução de dados, nomeadamente, do número de identificação pessoal.

Relativamente ao modelo previsto em Itália[114], contrariamente, ao que acontece na Alemanha e mesmo em Portugal, prevê um sistema de «definições gerais». A norma prevê duas condutas que consistem em alterar o modo de funcionamento de um sistema informático ou telemático e decorrendo desta prática um enriquecimento patrimonial para si ou para terceiros; ou a intervenção sem autorização, sobre dados, informações ou programas, não elencando discriminadamente as condutas conducentes à prática do crime. Quanto ao bem jurídico protegido, a doutrina italiana considera que é um crime pluri-ofensivo, por entender que o bem jurídico protegido deverá ser alargado, na medida em que vai "*para* além do património, nele englobando, (...) a proteção da regularidade do funcionamento e da reserva da utilização dos sistemas informáticos"[115]. O bem jurídico protegido, tal como decorre do Supremo Tribunal

---

[113] Ibidem, p. 257.

[114] ***Art. 640 ter***

Frode informatica

Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da lire centomila a due milioni. La pena è della reclusione da uno a cinque anni e della multa da lire seicentomila a tre milioni se ricorre una delle circostanze previste dal numero 1) del secondo comma dell'articolo 640, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema. Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze di cui al secondo comma o un'altra circostanza agravante.

[115] Santos, Rita Coelho. *O Tratamento Jurídico-Penal da Transferência de Fundos Monetários Através da Manipulação Ilícita dos Sistemas Informáticos – Studia Jurídica, n.°82*. Coimbra Editora, 2005, p. 215.

Italiano[116], não se reduz ao património incluindo a" *riservatezza e della regolarita' dei sistemi informatici che del patrimonio altrui* .[117] Este delito também pressupõe a obtenção de uma vantagem patrimonial através da alteração do funcionamento de um sistema informático ou intervenção abusiva do sistema, dos dados, programas ou informações, como decorre da Cassazione penale, sez. II, 18 luglio 2003, n. 32440 La Corte Suprema di Cassazione Seconda Sezione Penale.[118][119]

À semelhança do que sucede noutros ordenamentos jurídicos, o crime de burla informática parte da génese, com a mesma estrutura e mesmos elementos constituintes que a burla tradicional, diferindo apenas porque a conduta do agente recai não sobre a pessoa, mas sobre o sistema informático que pertença à mesma, sendo o crime consumado aquando obtenção de vantagem patrimonial, decorrendo da mesma, uma subtração patrimonial por parte da vítima.[120] À semelhança do ordenamento jurídico português, a doutrina italiana rejeitou a equiparação da máquina ao homem.

Quanto ao ordenamento jurídico espanhol, prevê o artigo 248, n.º2,alíena a)[121], uma tipificação ampla deste crime, que não elenca exaustivamente as condutas típicas do crime de burla informática tal como sucede no ordenamento jurídico italiano, conforme o artigo 640.º do Código Penal Italiano. E, portanto, os elementos típicos que integram o crime de burla informática são: a manipulação informática e artifício semelhante, a transferência patrimonial não consentida pelo legítimo titular, ânimo de lucro e da sua ação terá que resultar um prejuízo

[116] Cfr. http://www.penale.it/page.asp?mode=1&IDPag=115 (consultado 20 Novembro 2015).

[117] Amato, Astolfo di. *Codice di Diritto Penale delle Imprese e della Società: annotato com la giurisprudenza*. 1ª edição. Giuffrè Editore, 2001, p. 1642.

[118] " Tale reato presuppone, infatti, che l'agente consegua il profitto alterando il funzionamento di un sistema informatico o "intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi" in quest'ultimo contenuti.". Disponível em http://www.ius-web.it/PUB/allegati_prodotti/457/Cass._pen._sez._II_18.7.03_n._32440.pdf.

[119] Para o efeito, cfr. Cendon, Paolo. *Trattato dei nuovi danni – nformazioni Erronee Soggetti Deboli Illeciti Informatici Danni Ambientali*. Vol. 5. CEDAM, 2011, p. 964.

[120] Amato, Astolfo di. *Codice di Diritto Penale delle Imprese e della Società: annotato com la giurisprudenza*. 1.ª edição. Giuffrè Editore, 2001, p. 1644.

[121] **Artigo 248 do CPE**

1. Cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno.

2. También se consideran reos de estafa:

a) Los que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro.

a terceiro. A sua particularidade reside apenas na não discriminação das condutas, optando assim por incluir no preceito «definições gerais». Aliás pela própria configuração do artigo, o mesmo não se encontra autonomizado, restando para o efeito, apenas o n.º2 do artigo 248.º, cuja epígrafe é «De las estafas». Quanto a sua evolução, Código Penal Espanhol anterior a 1995 apenas alcançava bens que se corporizassem em coisas físicas, visíveis e tangíveis, logo mediante, uma burla informática não haveria aplicação possível, pela impossibilidade de se materializar este tipo de crime. Atualmente, também se prevê, para além dos bens supra mencionados, aqueles bens intangíveis, como por exemplo, os dados. A redação inicial do Código Penal Espanhol de 1995 apenas previa os n.ºs 1 e 2, alínea a), no entanto, com a reforma introduzida pela LO 15/2003[122], acrescentou o n.º3, cuja redação é muito semelhante à atual redação do n.º2 alínea b). Com a reforma de 2010 (LO 5/2010 de 22 de Junho[123]) manteve o n.º1 como sendo o tipo penal comum, e o n.º2 como burla informática, mas agora composto por três alíneas, sendo apenas a primeira relevante para o estudo.

O conceito "fraude"[124] levanta muitos problemas, já que se parte do suposto que terá que se produzir um engano, mas não será possível enganar uma máquina ou um computador. Ter-se-ia à partida um problema, sem engano não pode haver fraude nem burla. Daí o legislador espanhol ter introduzido o preceituado, porque havia a necessidade de legislar em matéria que se ajustasse à realidade sócio criminal e em casos em que não se pudesse atribuir elementos típicos da burla, como é o engano. O momento da perpetração do crime é quando a manipulação do sistema é efetiva, e nesse momento não existe engano.

O problema das «definições gerais» é o de que não se sabe quais as condutas que se possam subsumir no tipo legal previsto no artigo 248.2 do CPE. Ora vejamos, os casos de envio de correio eletrónico não solicitado, com mensagens fraudulentas provoca um engano na vítima. Ao considerar-se o engano um elemento básico da burla, e não da burla informática, esta conduta só se poderia subsumir ao n.º1 do artigo 248.º, ou aqueles casos em que o lesado compra algo na Internet, paga o valor acordado e não recebe o produto que pretendia adquirir, também não se incluirá no n.º2, porque dessa relação resultou um engano. Isto não acontece no ordenamento jurídico português.

[122] Cfr. Lei Orgânica 15/2003, de 25 de Novembro, disponível em http://noticias.juridicas.com/base_datos/Penal/lo15-2003.html.

[123] Cfr. Lei Orgânica 5/2010 de 22 de Junho, disponível em http://www.wipo.int/wipolex/en/text.jsp?file_id=267032.

[124] No ordenamento jurídico espanhol, admitem duas formas de se dizer burla informática, "estafa informática" ou "fraude informática".

Os conceitos de manipulação informática ou artifício semelhante levantam ainda problemas. Primeiramente, é necessário saber em que consiste a manipulação informática. Alguma jurisprudência espanhola entende como qualquer método que consista na alteração de elementos físicos necessários para a programação da máquina, ou introdução de dados falsos, com o objetivo de obter a transferência patrimonial[125]. No entanto, em casos de obtenção ilícita de chaves de acesso, por exemplo nos casos de *phishing*, pode levantar problemas uma vez que nem sempre existe uma alteração dos elementos físicos, nem uma introdução de dados falsos, tenhamos como exemplo, o caso em que o agente do crime utiliza ilicitamente as chaves da vítimas, não se diz poder haver uma manipulação. Neste sentido, o Tribunal Supremo[126] vem ampliar o conceito de manipulação informática dizendo por um lado, que consubstanciaria manipulação informática ou artifício semelhante aqueles casos em que se utilizasse programa informático sem a devida autorização ou se o utiliza contrariamente aos seus fins. Se por outro lado, o agente do crime não tem autorização para utilizar as chaves de acesso do legítimo titular, serão considerados atos constitutivos do crime de burla.

Com o artigo 248, n.º2, alínea a) do CPE, o legislador pretendeu englobar aquelas condutas que não podem incluir-se no n.º1 do mesmo preceito, devido à não verificação dos seus elementos típicos.

[125] Cfr. STS 6984/2008, disponível em http://www.poderjudicial.es/search/documento/TS/3480835/Estafa/20090122 (consultado 20 Novembro 2015).

[126] Cfr. Página 4 da STS de 21 Dezembro de 2004, disponível em http://goo.gl/OGhk2f (consultado 20 Novembro 2015).

CAPÍTULO III

1. MODOS DE MANIFESTAÇÃO DAS BURLAS INFORMÁTICAS

1.1. Introdução tecnológica às componentes básicas informáticas

Visto que a predominância dos ataques, que iremos referir subsequentemente, são baseados em elementos da infraestrutura Internet, não poderíamos deixar de enunciar umas considerações acerca de algumas componentes tecnológicas-chaves que nos irão auxiliar na compreensão das técnicas que se seguem. As duas formas mais populares de utilização da infraestrutura da Internet são a *World Wide Web* (vulgarmente designada por *web*) e o correio eletrónico (comumente designado por *e-mail*). A grande diferença entre o momento anterior à existência da Web e o momento posterior à criação da mesma reside no desenvolvimento e disposição de motores de busca que permitem a indexação e pesquisa de informação constante na Internet que irá facilitar a pesquisa de informação ao utilizador.

Hodiernamente, a *web* é uma forma de utilizar os recursos da Internet de uma forma comedida e intuitiva e consegue ter um número de vantagens significativo relativamente a outros meios de comunicação tais como a televisão, rádio, jornais e revistas, porque se trata de um fenómeno sempre atualizado, ilimitado, interativo, personalizado e que contém elementos de multimédia. A sua enorme acessibilidade ocasionou uma explosão de popularidade sem precedentes. O *website* ou *site* faz referência a uma página ou a um agrupamento de páginas relacionadas entre si, acessíveis na Internet através de um determinado endereço. E portanto, um *site* não é menos do que, habitualmente, o resultado da sinergia entre um servidor *web*[127], uma base de dados e os seus utilizadores. Mas antes de avançarmos com alguns entendimentos técnicos, cremos ser pertinente tecermos algumas notas sobre a origem e história da *Web*. *World Wide Web*, ou comumente designada por *web*, é uma rede[128] de alcance mundial que após o aparecimento da Internet surgiu com o objetivo de ligar as pessoas e permitir a partilha

[127] Por servidor web entender-se-á como "um programa de computador responsável por aceitar pedidos HTTP de clientes e servi-los com respostas HTTP, incluindo opcionalmente dados que geralmente são páginas web tais como documentos HTML com objetos embutidos". Disponível em https://pt.wikipedia.org/wiki/Servidor_web (consultado 20 Novembro 2015).

[128] A rede a que aludimos neste ponto não se confunde nem tem correspondência direta com a rede de interligação mundial de computadores que define a Internet.

de ficheiros através do computador, acabando por impulsionar a adoção massiva da Internet. Foi a solução encontrada, em 1990 por Tim Berners-Lee, para criar acesso a um arquivo comum através de computadores ligados entre si. Falando acerca do percurso evolutivo da *web*, sabemos que até aos dias de hoje esta vai sendo alvo de estudos permanentes para que a sua potencialidade seja conseguida ao nível máximo. O acesso à *web* parte sempre da especificação de um URL (acrónimo de *Uniform Resource Locator*) que consiste numa sequência de caracteres que é usado como endereço de uma determinada página da Internet que permite a sua localização e acesso), do protocolo HTTP (permite a comunicação entre o browser e os sites) e da linguagem HTML (consiste num formato de documento destinado a criar documentos para publicação na WWW da Internet).

Antes de aprofundarmos o conhecimento nestes dois protocolos, termos que abordar outros conceitos.

O correio eletrónico não é mais do que um serviço de mensagens enviadas entre utilizadores de sistemas computacionais para obter e enviar mensagens, sendo que os mesmos não carecem de estar em linha ao mesmo tempo, ou até no mesmo computador para comunicar. Durante os primeiros anos da Internet, o correio eletrónico foi um dos grandes impulsionadores da comunicação científica e académica americanas. Cientistas e académicos viam nele um meio de comunicação mais eficaz e reservado que o correio tradicional. O corpo da mensagem pode ter dois tipos de formatações: texto simples (ASCII) ou texto rico (HTML), sendo o segundo retrocompatível com o primeiro. O texto simples não permite nenhum tipo de formatação, enquanto que o texto rico permite não só a inclusão da formatação como também a inserção de imagens. O texto rico funciona da mesma forma que uma página web, sendo composto através da mesma linguagem.

Por sua vez, o HTML[129] é baseado em SGML (*Standard Generalized Markup Language*) e poderá ser descrita como a " linguagem em que são criadas as páginas de informação na Internet"[130]. Essa linguagem de descrição de páginas *web* destina-se à criação de documentos para a publicação na WWW, isto é, quando se acede a uma página *web* acede-se a uma página HTML, que é um texto escrito ou melhor dizendo uma linguagem com uma estrutura. Por outras

[129] Graham, Ian S. *The HTML sourcebook*. John Wiley & Sons, Inc., 1995.

[130] Pereira, Joel Timóteo Ramos. *Direito da Internet e Comércio Eletrónico*. Lisboa: *Quid Juris* Sociedade Editora, 2001, p. 477.

palavras, uma página *web* não é nada menos que uma linguagem de HTML. Com o HTML, um autor da página da *web* controla a experiência do utilizador com o conteúdo. O elemento fundamental desta linguagem é a possibilidade de introduzir códigos que permitem a ligação entre diferentes documentos, locais ou não, a partir de palavras sinalizadas. Alguns elementos da linguagem permitem definir a estrutura do texto, inserir imagens, vídeos, fragmentos de programas (*scripts*) que podem ser diretamente interpretados pelo *browser* através da linguagem de *scripting* mais utilizada no contexto da *web*, o *Javascript*, sendo que a sua incorporação no HTML acarretou benefícios e malefícios. Por conseguinte, documentos HTML são ficheiros de texto simples compostos por instruções HTML que podem ser criados por qualquer editor de texto, tomemos como exemplo o bloco de notas, mas que podem ser utilizados processadores de texto para esse mesmo efeito.

A fim de ilustrar melhor, apresentamos os exemplos abaixo descritos.

Figura ii

Exemplo de linguagem HTML

Qualquer documento HTML tem de compreender certos elementos marcadores que são indispensáveis que consistem em palavras-chave delimitadas por parêntesis angulares, que, para além de criarem *links* entre diferentes documentos ou partes de um mesmo documento, determinam como o texto e os gráficos devem ser exibidos no ecrã. Terá que conter um cabeçalho, onde contém o título e um corpo de texto que contém o texto que é composto por listas, parágrafos, listas, entre outros. Ora, este texto é composto por marcadores e informação adicional que irá ser lida pelos *browsers*, uma vez que estes estão programados de acordo com

as especificações do código HTML. Os marcadores principais são: HTML, HEAD, TITLE e BODY. A primeira instrução indica ao *browser* que o documento contém informação em código HTML e além do mais, os ficheiros com extensão HTML, no caso de não haver restrição de nomes longos, também indicam ao browser que documento contém o código HTML. A segunda instrução indica ao *browser* o cabeçalho da página que está a ser visualizada e é a primeira parte do código HTML e é utilizada em conjunto com o TITLE. A terceira instrução indica de forma geral, o título do documento que está a ser visualizado, que é apresentado no topo da janela do *browser*. Normalmente é resumido e descritivo, e é também aquilo que é mostrado nos Favoritos do *browser*. A última e quarta instrução consiste na segunda parte do código e a mais comprida pois nela está contida toda a informação que é visualizada na página Web. Para além de ser uma linguagem de descrição de conteúdos, e um fenómeno dinâmico apresenta estilos. *Cascading Style Sheets* (CSS) é um mecanismo de folha de estilo em cascata que tem a responsabilidade da apresentação dos conteúdos da sua estrutura (HTML). Descreve como é que os elementos de HTML estão exibidos no ecrã, isto é, através de determinados atributos é possível indicar a cor do fundo, do texto, das hiperligações, respetivamente do documento HTML. Ainda, pode ser colocado no seu plano de fundo uma imagem, música que irá permitir chamar a atenção de quem visualiza a página bem como dar melhor aparência a esse documento.

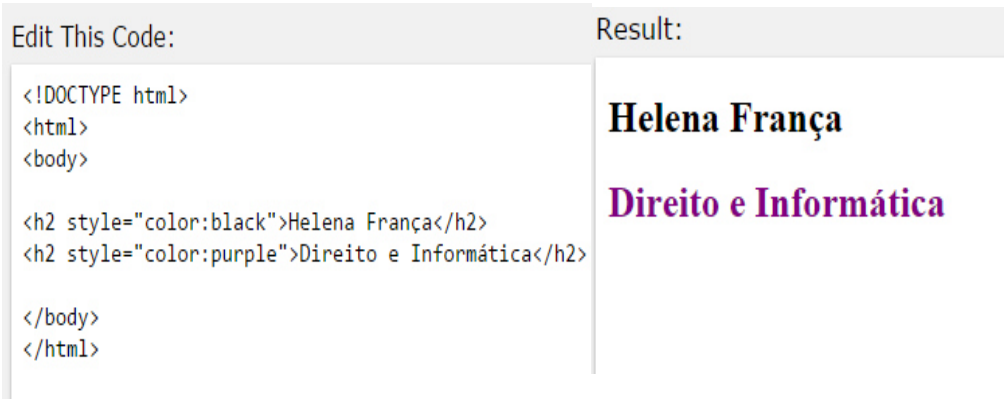

Figura iii

Exemplo de linguagem HTML (CSS)

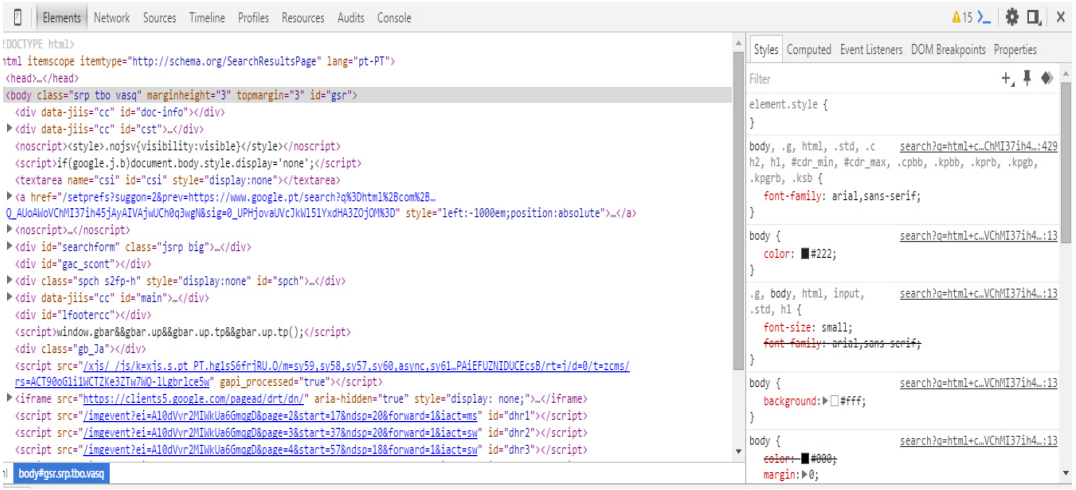

Figura iv

Exemplo linguagem HTML

Quanto à arquitetura de um serviço *web*, ter-se-á em conta a relação dois participantes que se encontram envolvidos na troca de informações, por um lado o cliente que solicita as informações e por outro lado um servidor *web* que atende a esses pedidos. Por seu turno, o servidor *web* é responsável por armazenar (na sua base de dados) e trocar informações com outras máquinas. Deste modo o cliente, por via do seu *browser*, introduz o endereço que pretende consultar, emitindo desta forma um pedido (GET) de HTTP para o servidor *web*. O servidor *web* gera e disponibiliza ao *browser* documentos em HTML, CSS e/ou *Javascript*. Após, a resposta em HTTP será dada novamente ao *browser*. Por via do funcionamento de um serviço *web* é possível visualizar o conteúdo do endereço que o cliente pretende consultar.

A fim de engrandecer a linguagem a HTML foi desenvolvida a linguagem *Javascript*. A linguagem *Javascript* é uma tecnologia que tem como desiderato melhorar a experiência do utilizador e a *web*, e desta forma complementa a linguagem HTML. Foi desenvolvido para permitir que os autores de HTML escrevessem *scripts* (os documentos HTML apresentados aos utilizadores começam a poder exprimir comportamentos, ou seja, passam a ser forçosamente executados pelos browsers dos seus utilizadores) diretamente nos seus documentos. Sempre que se incluir *Javascript* num documento HTML terá que se delimitar essas linhas com um par de marcadores como <SCRIPT>...</SCRIPT>, e desta forma alertam ao programa do *browser* para começar a interpretar todo o texto entre esses marcadores como um *script*. Consiste numa linguagem de programa do lado do cliente mais utilizada que permite criar pequenos programas

encarregados de realizar ações dentro do âmbito de uma página *web*. Isso permite a criação de aplicações atraentes por via de HTML gerada por *script*. Como foi dito anteriormente, o *Javascript* é incorporado nas páginas HTML e interpretado pelo *browser* do cliente que acede à página, sendo uma linguagem orientada a eventos. Os autores das páginas *web* podem incluir *scripts* escritos, em documentos HTML, nesta nova linguagem para melhorar as páginas *web*. A linguagem *Javascript* é uma linguagem que pode auxiliar na transformação de uma página de conteúdo estático para uma página de conteúdo atraente, dinâmico e interativo. Poderá atuar através de efeitos especiais nas páginas *web* (por exemplo, uma simples mudança de cor, ou elementos da página que tenham movimento) ou então permite executar instruções como resposta às ações do utilizador, sendo dessa forma possível, a criação de páginas interativas como por exemplo, uma agenda ou calculadora. Vejamos um exemplo de um código de *Javascript* [131]:

```
<!DOCTYPE html>
<html>
<body>
<h1>What Can JavaScript Do?</h1>
<p id="demo">JavaScript can change HTML content.</p>
<button type="button"
onclick="document.getElementById('demo').innerHTML = 'Hello JavaScript!'">
Click Me!</button>
</body>
</html>
```

A *World Wide Web* é basicamente um agrupado de documentos HTML ligados entre si e em constante expansão. Um *browser* da *web*, não é mais do que uma ferramenta capaz de exibir esses mesmos documentos e seguir os *links* ali contidos. Mas, quando se exploram as páginas *web*, é utilizado o protocolo HTTP para a navegação nestas e quando se clica em algo que tem uma ligação é iniciado através do HTML e HTTP uma leitura e transferência de dados entre computadores que permite aceder à mais diversa informação existente na Internet.

[131] Exemplo retirado e disponível em http://www.w3schools.com/js/tryit.asp?filename=tryjs_intro_inner_html (consultado 20 Novembro 2015).

HTTP consiste num "protocolo que define como dois programas ou servidores devem transferir entre si comandos ou informações relativas à Internet"[132]. Desta forma permite a comunicação entre o *browser* e os *sites* e é utilizador para transferência de informação (de páginas HTML) do computador para a Internet. É baseado em pedidos e respostas entre os clientes e os servidores. O cliente, que poderá ser o *browser* ou o dispositivo que fará o pedido (*user agent*) vai solicitar um determinado recurso enviando um pacote de informações contendo alguns cabeçalhos a um URL, daí que os endereços dos sites contêm no início o «HTTP». Acionamos o protocolo HTTP quando digitamos determinado endereço URL no *browser*, por exemplo, http://www.(...). Por sua vez, existem quatro tipos de pedidos HTTP que indicam a ação a ser realizada, isto é, determina o que o servidor deve fazer com o URL fornecido no momento da requisição de um recurso: GET, PUT, POST, DELETE, com a ressalva de que apenas HEAD e GET são obrigatórios em HTTP puro. GET consiste em solicitar algo ao servidor, como por exemplo, a página inicial do *site*, ou seja a página raiz; PUT aceita criar ou alterar algum objeto do servidor, ou seja envia algo; POST é muito usado, mas na prática de programação deveria de ser GET; DELETE tem o intuito de apagar um recurso ou conteúdo. Por sua vez, os métodos mais comuns para efetuar um ataque são: GET (a informação é injetada através do URL, sendo a mesmo visível na barra de endereço) e POST (a informação é injetada por via de formulários, sendo esta não visível após submissão da informação).

A este propósito, e para uma maior compreensão do que se segue, o HTTPS, diferentemente do que sucede no HTTP garante ao utilizador validar a autenticidade de um *site*. O HTTPS pressupõe que a informação ali contida esteja cifrada. Quando digitamos determinado endereço URL no *browser*, o mesmo tem que apresentar um certificado reconhecido por uma entidade externa fidedigna, logo oficialmente reconhecida. Este certificado digital[133] serve como uma identificação digital e que permite ter-se "a certeza de que o par de chaves (pública e privada) pertence realmente a um determinado emissor"[134]. Se o *site* não for original o certificado não é válido e será visível ao utilizador, advertindo o mesmo que está perante um site

[132] Pereira, Joel Timóteo Ramos. *Direito da Internet e Comércio Eletrónico*. Lisboa: *Quid Juris* Sociedade Editora, 2001, p. 477.

[133] Segundo a asserção de Joel Timóteo Ramos, certificado digital consiste num "documento eletrónico assinado digitalmente, emitido por uma terceira parte de confiança, denominada entidade certificadora" *in* "Direito da Internet e Comércio Eletrónico". Lisboa: *Quid Juris* Sociedade Editora, 2001, p. 42.

[134] Pereira, Joel Timóteo Ramos. *Direito da Internet e Comércio Eletrónico*. Lisboa: *Quid Juris* Sociedade Editora, 2001, p. 42.

que não é genuíno. O certificado de que falamos terá que ser emitido e reconhecido por uma CA (*Certification Authority*). Estas entidades são quem nos permite depositar confiança na autenticidade no parceiro de comunicação e quem garante que o homólogo de comunicação é genuíno e que o certificado é válido. O evento mais ameaçador para a segurança informática é o comprometimento de uma CA.

Passo agora à explicitação do Serviço de Nomes ou DNS que surge das iniciais *Domain Name System*, com a ressalva de que poderá ter a designação de *Server* ou *Service*. Faz corresponder a uma série de números (Internet *Protocol Address* ou IP) que são atribuídos a cada máquina ligada à Internet. E portanto existe a tradução de nomes em endereços IP. Desta forma funda-se num serviço de distribuição parcialmente replicado que interpreta os números pelos quais os servidores ligados à Internet são identificados, apresentando-os ao utilizador como um nome textual. Usualmente têm uma " (...) estreita conexão com o conteúdo do *site* que identificam ou com a entidade que o opera, refletindo aquele ou reproduzindo o nome desta".[135] Os nomes de domínio são atribuídos por entidades devidamente autorizadas para o efeito, como é o caso da ICANN (*Internet Corporation for Assigned Names and Numbers*). O seu principal propósito é o de converter nomes em IPs e vice-versa, guardar essa informação e partilhá-la. A necessidade da sua existência reside no facto de os computadores na Internet normalmente não serem mencionados por nomes, mas por endereços de IP. Vejamos o seguinte exemplo: quando se digita o endereço www.net.pt estamos a aceder a uma máquina que tem um determinado número de IP específico na Internet. O servidor DNS atua neste sentido, pois tenta descobrir a que endereço corresponde determinado nome, não obstante, caso não seja possível essa determinação o que acontece é que encaminha-o para outro servidor e assim adiante até o endereço IP ser encontrado. Todavia existem técnicas de utilização abusiva do servidor de DNS, que visa, a obtenção de vantagem patrimonial, como é o caso do "(...) aproveitamento de um nome sobre o qual incidam direitos de terceiro ou de um nome com ele facilmente confundível, para atrair cibernautas para os sites de quem indevidamente o utiliza. (...) Cria-se, com essa utilização, a enganosa aparência de uma relação entre o legítimo titular de direitos sobre o nome

[135] Andrade, Miguel Almeida. *Nomes de Domínio na Internet: a regulamentação dos nomes de domínio sob.pt.* 1.ª edição. Lisboa: Centro Atlântico, Lda., 2004, p. 12.

usado como nome de domínio e conteúdo do *site*".[136] Um dos ataques principais ao DNS é o designado DNS *cache poisoning*, como veremos de seguida.

Em modo de conclusão, importa ainda sublinhar e não esquecer que tudo o que circula entre o *browser* e o servidor *web* é uma "linguagem", daí a pertinência do ponto acima. A maior parte dos *sites web* que utilizamos funciona por geração dinâmica de conteúdos em HTML, potenciado pela linguagem *Javascript* e por essa via o site, sem intenção, pode ser veículo de um ataque por parte de terceiros. Um utilizador que visite determinada página *web* pode estar imediatamente exposto a ataques. O mesmo não tem conhecimento que algo malicioso pode estar a decorrer "por detrás" da página visível do seu *browser*. Após a injeção de conteúdo malicioso, que poderá atuar por *Javascript*, este é processado pelo *browser*, transparente para o utilizador e pode comprometer seriamente o sistema operativo da vítima. Desta forma através da injeção de um código malicioso no *Javascript*, o programa malicioso vai tentar executar instruções arbitrárias no sistema da vítima.

Devido às vulnerabilidades existentes é possível a concretização de muitos ataques dos quais falaremos adiante.

1.2. Algumas práticas informáticas que conduzem ao cometimento de burlas informáticas

1.2.1. SPAM

Não constitui uma técnica informática propriamente dita em matéria de perpetração do crime de burla informática, aliás é relativamente inócuo mas poder-se-á traduzir enquanto um meio para a realização dos mesmos.

O SPAM curiosamente remonta ao termo caricato de SPAM®[137], uma marca de presunto condimentado (SPiced hAM), um enlatado americano fabricado pela *Hormel Foods Corporation*[138] desde 1930. Satirizado e eternizado por um dos programas clássicos "*Monty Python´s Flying Circus TV Show*", o SPAM a certa altura do episódio torna-se de tal forma repetitivo e incomodativo constituindo, desta forma, a analogia perfeita em relação à sensação

[136] Ibidem, p. 14.

[137] Para o efeito consultar o site disponível em http://www.spam.com/(consultado 20 Janeiro 2016).

[138] Para o efeito consultar o site disponível em http://www.hormel.com/(consultado 20 Janeiro 2016).

de que sofrem os utilizadores vítimas de correio eletrónico indesejado. De todo o modo, a Hormel desaprova a ligação do SPAM, enquanto envio massivo de mensagens não solicitadas à marca SPAM®. No entanto, não deixa de ser curiosa a analogia entre cada uma delas.

O SPAM é a nomenclatura utilizada para definir o envio massivo de *e-mails* geralmente de conteúdo comercial[139]. Corresponde ao envio massivo de mensagens de correio eletrónico não solicitadas em quantidades que causam incómodo, perda de tempo e custos para o seu destinatário, nomeadamente bloquear o sistema de receção por saturação, no destinatário do correio como no servidor de acesso. E como permite contactar milhões de utilizadores potencia a escala do ataque. Geralmente o *spammer* "obtém uma base de dados de endereços eletrónicos, que pode ser recolhida através da busca de páginas de Internet ou grupos de discussão ou mesmo através da utilização de todas as combinações possíveis de endereços de um servidor de correio eletrónico"[140]. Posteriormente "envia as mensagens para essas listas normalmente colocando um endereço falso do remetente em ordem a evitar receber a devolução das mensagens que envia"[141].

Segundo um Relatório da Kaspersky Lab datado de Agosto de 2012, o SPAM atinge em média, 70,2% de todas as mensagens de *e-mail*[142],não havendo indicações que Portugal esteja mais ou menos vulnerável em relação a outros países. Aliás, é um problema à escala mundial que tem vindo a atingir grandes proporções e que tem preocupado os mais variados especialistas.

Ainda assim, poderá viabilizar prejuízos aos utilizadores, designadamente prejuízos financeiros através do envio de *trojans* para roubar os dados bancários das vítimas, através da concretização do *phishing*. O *spammer* pode induzir a vítima em erro para que esta, nos casos de *phishing*, ao clicar no *link* associado ao *e-mail*, execute um determinado programa malicioso, que vai ficar oculto no seu computador e que irá gravar alguns dados, nomeadamente de origem bancária.

---

[139] Conteúdo exclusivamente comercial é designado por UCE – da terminologia inglesa *Unsolicited Commercial E-mail*, cuja tradução é *e-mails* comerciais não solicitados.

[140] Leitão, Luís Menezes. "A distribuição de mensagens de correio eletrónico indesejadas (SPAM)". In *Direito da Sociedade da Informação – Vol. IV,* Associação Portuguesa do Direito Intelectual. Coimbra Editora, 2003, p. 192.

[141] Idem.

[142] Informação disponibilizada em http://goo.gl/7wXaph (consultado 20 Novembro 2015).

Existem certos mecanismos que uma vez adotados universalmente tornarão virtualmente muito pouco admissível a prática de SPAM e consequentemente do *phishing.* Suponhamos que para o envio de *e-mail* seria obrigatório a assinatura digital do remetente. Neste caso o *spammer* seria forçado a revelar a identidade perante uma entidade externa, minimizando, desta forma, o envio de SPAM. A prática de assinatura digital não impediria o envio de SPAM, mas responsabilizaria os seus agentes.

Uma outra realidade que tem relevo nesta matéria como no *phishing* são as redes *botnet*, que são as responsáveis pela maior parte do SPAM enviado. Frequentemente utilizado para o SPAM e *phishing*, o *botnet* consiste num conjunto de computadores controlados por atacantes através de, por exemplo, vírus, cavalos de Tróia no computador completamente incauto. A execução de um ataque de *botnet* processa-se da seguinte forma: o *botnet* quando quiser enviar ataques de *phishing* envia mensagem aos milhares de computadores que controla para o fazerem em vez dele. E, na verdade, mesmo não existindo nenhuma evidência visual, como o rato a mexer, os computadores podem estar a enviar milhares de mensagens por hora. Ora, os utilizadores são agentes que participaram num ataque, mesmo sem qualquer noção de que o estavam a ser.

1.2.2. Phishing

Este novo fenómeno criminal resulta do termo em inglês "*fishing"* e consiste numa das técnicas informáticas que viabiliza o cometimento de burlas informáticas, de "pescar" informação pessoal e confidencial dos utilizadores. O *phishing*, perfeita analogia com a arte de pescar, não é mais do que "morder o isco", e para o efeito, existe a ilusão de que o isco é genuíno. Efetivamente o atacante terá que criar um isco credível e convencer o utilizador a mordê-lo, pois só terá impacto se o isco for credível. A nomenclatura *phishing* foi batizada em 1996, aquando a sua menção teve lugar num *newsgroup* denominado como *alt.online-service.america-online.* É, segundo a asserção de Markus Jakobsson, a sinergia entre a tecnologia e a engenharia social[143].

[143] É o termo que designa a prática de recolha de informações por intermédio da exploração de relações humanas de confiança, ou outros métodos que enganem utilizadores e administradores de sistemas.

Para o STJ o "*phishing* pressupõe uma fraude eletrónica caracterizada por tentativas de adquirir dados pessoais, através do envio de *e-mails* com uma pretensa proveniência da entidade bancária do recetor, por exemplo, a pedir determinados elementos confidenciais (número de conta, número de contrato, numero de cartão de contribuinte ou qualquer outra informação pessoal), por forma a que este ao abri-los e ao fornecer as informações solicitadas e/ou ao clicar em links para outras páginas ou imagens, ou ao descarregar eventuais arquivos ali contidos, poderá estar a proporcionar o furto de informações bancárias e a sua utilização subsequente". [144]

Geralmente a técnica é consumada, numa fase inicial, com o envio massivo de mensagens de correio eletrónico de conteúdo enganoso (SPAM) que incluem um determinado *link* que, ao clicar, acede-se a uma página na *web*. Ao clicar o utilizador será redirecionado para a reprodução de uma página em tudo idêntica à página institucional da instituição bancária ou de uma entidade emissora de cartões de crédito. Esta página construída e gerida por terceiros é falsa! Será solicitado ao utilizador a introdução dos seus códigos confidenciais referentes à sua conta bancária e desta forma é possível para os "burlões informáticos" obterem os dados confidenciais que lhes permitirá aceder à conta bancária da vítima, transferindo o dinheiro para contas suas. Por meio de armadilhas virtuais, utilizam dados confidenciais sem a devida autorização, resultando dessa atividade delituosa um prejuízo e subtração do património das vítimas, logo enquadrável no crime de burla informática. A prática de *phishing* é relativamente fácil de realizar porque o seu custo de execução é muito baixo, todavia apresenta uma rentabilidade bastante elevada No entanto, do ponto de vista técnico construir uma página *web* falsa pode revelar-se um processo moroso e dedáleo.

Relativamente ao enquadramento legal do *phishing* Pedro Verdelho[145] esclarece, desde logo, que o mesmo não é claro, realçando que a maior parte das jurisdições apenas pune antes várias parcelas desta forma de atuar, não qualificando autonomamente esta atividade complexa enquanto crime. Terá que se ter em linha de conta que a elaboração e emissão de mensagens de correio eletrónico de conteúdo enganoso, com indicação falsa do remetente (SPAM) estão

[144] Boularot, Ana Paula, relat. – Acórdão no processo 6479/09.8 TBBRG.G1.S1. Supremo Tribunal de Justiça. [Em linha]. Lisboa (18-12-2013). [Consultado 20 Novembro 2015] Disponível em http://goo.gl/Thaufc.

[145] Verdelho, Pedro. " Phishing e outras formas de defraudação nas redes de comunicação". In *Direito da Sociedade da Informação – Vol. VIII,* Associação Portuguesa do Direito Intelectual. Coimbra Editora, 2009, p. 414.

associadas e subjacentes ao *phishing*. Ao considerarmos que uma mensagem de correio eletrónico se trata de um documento e enquadrável, tal como alude Pedro Verdelho, no artigo 255.º, alínea a) do CP[146] "esta parcela poderá do *phishing* poderá ser enquadrada sem dificuldades na previsão do crime de falsificação, previsto e punido pelo artigo 256.º, n.º1 do CP"[147]. Relativamente ao enquadramento do *phishing,* tendo em conta que é ainda pouco conciso*,* requer que haja um entendimento da sua extensão e do seu alcance. Em matéria de construção de uma página web falsa enganosamente construída e em tudo idêntica à página institucional da instituição bancária discute-se acerca do enquadramento de uma página *web* no preceito do artigo 255.º, alínea a) do CP.

Para nós, estas qualificações jurídico-penais parcelares são supérfluas. É claro que o envio de mensagens de conteúdo enganoso (SPAM) e a construção de uma página *web* em tudo idêntica à original não passam de atos preparatórios para o último desígnio dos agentes do crime, a utilização de dados sem autorização para obtenção de ganhos patrimoniais, assim enquadrável no artigo 221.º do CP. Portanto, é nossa convicção, que essas parcelas apenas deverão ser consideradas atos preparatórios do crime de burla informática e que não deverão ser individualmente punidas.

Esta nova manifestação criminosa, segundo Fátima Flores Mendoza[149], poderá desenvolver-se em três fases, por sujeitos de nacionalidades diferentes, muito habilidosos e com uma alta qualificação tecnológica, que atuam de forma organizada e concertada.[150] Enfrenta-se um novo caso de associação criminosa, previsto no artigo 299.º do CP de carácter

---

[146] **Artigo 255º**

Definições legais

Para efeito do disposto no presente capítulo considera-se:

a) Documento: a declaração corporizada em escrito, ou registada em disco, fita gravada ou qualquer outro meio técnico, inteligível para a generalidade das pessoas ou para um certo círculo de pessoas, que, permitindo reconhecer o emitente, é idónea para provar facto juridicamente relevante, quer tal destino lhe seja dado no momento da sua emissão quer posteriormente; e bem assim o sinal materialmente feito, dado ou posto numa coisa para provar facto juridicamente relevante e que permite reconhecer à generalidade das pessoas ou a um certo círculo de pessoas o seu destino e a prova que dele resulta;

[147] Verdelho Pedro, op.cit., p. 414.

[149] Mendoza, Fátima Flores. "Respuesta Penal al Denominado Robo de Identidade n las Conductas de Phishing Bancario". *Estudios Penales y Criminológicos* vol. XXXIV (Julho 2014): 301-339.

[150] Estas organizações criminais, constituídas por um número significativo de membros com elevada qualificação tecnológica, são dotadas de uma estrutura hierarquizada, e organizativa, o que nos permite falar em delinquência organizada, designadamente de associação criminosa, prevista no artigo 299.º do C.P.

transfronteiriço. A primeira fase respeita à obtenção de dados confidenciais como senhas, números de cartão de crédito e dados de conta. Após obtenção das mesmas os criminosos visam controlar as contas bancárias das vítimas. A segunda fase respeita à utilização não consentida dos dados por parte dos respetivos titulares e a transferências de dinheiro da conta das vítimas para a conta dos criminosos, geralmente situadas no estrangeiro, de preferência onde a legislação a este respeito seja escassa, ou então não exista conduta criminosa. E por fim, na terceira fase essas quantidades de dinheiro transferidas são retiradas rapidamente das contas dos legítimos titulares e enviadas por correio postal ou por empresas de envio de dinheiro a outros membros da organização que se encontram geralmente na Europa de Leste.

A prática de técnicas de *phishing* pode originar: roubo de identidade e o roubo de dados sensíveis. O roubo/usurpação de identidade ou *identity theft* corresponde à primeira etapa do *phishing*. O roubo de identidade consiste na obtenção de dados pessoais e/ou confidenciais da identidade de um determinado individuo. O perigo do roubo/usurpação de identidade desperta alertas para cometimento de outros tipos de fraudes, designadamente a utilização abusiva[151] de cartões bancários. Por conseguinte, os agentes criminosos utilizarão os dados para seu proveito próprio resultando, na esmagadora das vezes, em subtração de quantias patrimoniais das contas dos legítimos titulares. Segundo Fátima Flores Mendoza[152] o roubo de identidade forma parte do *identity related crime* ou roubo de identidade em sentido amplo, dividindo-se, segundo a mesma, em três etapas. A primeira respeita às condutas do roubo de identidade em sentido estrito, isto é, o apoderamento dos dados pessoais e confidenciais de uma determinada pessoa (física ou morta) ou de uma entidade sem personalidade jurídica, sendo que os mesmos podem – e muitas vezes serão – de caráter eletrónico. A este propósito "várias são as finalidades abusivas da usurpação da ciberidentidade" que poderá passar pela "obtenção indevida de vantagem patrimonial" e acresce que "a obtenção indevida de ganhos económicos é abundantemente referenciada como o principal desígnio deste ato ilícito. Assume especial relevância neste campo,

[151] Segundo Maria Raquel Guimarães "por utilização abusiva entende-se essencialmente as operações eletrónicas conducentes a uma inscrição a débito na conta bancária do titular do cartão sem que esta conta disponha de provisão suficiente" in *As transferências eletrónicas de fundos e os cartões de débito: alguns problemas jurídicos relacionados com as operações de levantamento*. Coimbra: Almedina, 1999, p.201.

[152] Mendoza, Fátima Flores. "RESPUESTA PENAL AL DENOMINADO ROBO DE IDENTIDAD EN LAS CONDUCTAS DE *PHISHING* BANCARIO." *Estudios Penales y Criminológicos* vol. XXXIV (Julho 2014): 301-339.

a burla informática concretizada através do serviço de *homebanking* muitas vezes com recurso ao *phishing* e *pharming*"[153].

A segunda fase corresponde à suplantação da identidade, ou seja, à utilização de dados pessoais alheios com fins ilícitos. Segundo a mesma autora, poderá haver entre estas duas fases uma terceira, aquela em que dedica à venda de dados pessoais a outros sujeitos ou organizações criminosas.[154] O roubo de dados sensíveis, por sua vez, visa o acesso a informação sensível e/ou confidencial e está, normalmente associada ao envio de mensagens de correio eletrónico (muitas vezes SPAM) sob a capa de instituições bancárias que aparentam ser fidedignas. As mensagens são enviadas, indiscriminadamente, para milhares de endereços de correio eletrónico. A operação é, geralmente, realizada por computadores que se encontram sob controlo dos criminosos e que através de servidores *open relay* de correio eletrónico enviam facilmente SPAM.

Várias são as técnicas de *phishing* para obtenção de dados pessoais e informação confidencial dos utilizadores. Com o avanço da tecnologia as técnicas de *phishing* também são mais proeminentes. A este propósito julgamos ser apropriado fazer, de modo breve, alusão ao *Cross-site scripting* (XSS) e ao *Cross-Site Request Forgery* (CSRF). Ambos ataques são baseados na execução de s*cripts*, que não são nada mais que fragmentos de programas interpretados e executados pelo *browser* de Internet do utilizador. Quando o utilizador acede a uma página *web* está a fazê-lo sem saber que está a executar pequenos programas.

O *cross-site scripting*, de modo muito genérico, traduz-se numa exploração de uma vulnerabilidade de um *site*, tentando desta forma atacar a privacidade de um seu utilizador. Este ataque permite que os *hackers* coloquem um *script* malicioso (geralmente *Javascript*) numa determinada página da *web*. Desta forma, vai permitir que o código HTML seja inserido arbitrariamente no *browser* da vítima. Pressupõe a existência de três partes: o *hacker*, a vítima e o *website*. A vítima ao entrar nessa página vai fazer "correr" todos os *scripts*, incluindo aquele

[153] Silva, Flávio Manuel Carneiro de. "A usurpação da ciberidentidade". Dissertação de mestrado, Universidade Católica do Porto, 2014, pp. 33 e 34.

[154] Paralelamente, existe a venda de informação que é eletronicamente copiada da banda magnética que existe nos cartões bancários, comumente designado por *dump*. Dois exemplos de informação que é vendida é o BIN (*Bank Identification Number*) e o PIN (*Personal Idenfication Number*). Composto por seis dígitos, a obtenção do BIN permite o conhecimento da identificação das instituições bancárias. Desta forma, revela-se mais fácil apurar qual a instituição bancária mais vulnerável. Por outro lado, o PIN permite aceder a uma caixa automática e efetuar levantamentos de numerário.

que fora introduzido pelo *hacker*. Este ataque é muito comum em locais onde é partilhada informação entre os utilizadores, como é exemplo, os fóruns. Quando um utilizador publica uma mensagem no fórum, essa mensagem é guardada numa base de dados. Por sua vez, o *script* encontra-se inserido numa mensagem aparentemente vulgar. Subsequentemente quando vem outro utilizador consultar aquela discussão do fórum, a aplicação vai à base de dados e procura as mensagens que devem ser apresentadas. Nestes casos, o *hacker* através de uma mensagem aparentemente vulgar consegue esconder um *script* no seu código de fonte. Um utilizador ao aceder àquela mensagem irá, inadvertidamente, executar o *script* e ser alvo de ataque. Desta forma conseguem aceder aos *cookies* e aos nossos dados sensíveis. Nada impede que uma mensagem padeça de um *script* venenoso.

No ataque de CSRF tenta-se atingir as *cookies*, ou seja, a vítima que começou a sessão (seja de uma rede social, ou mesmo da sua instituição bancária) e não a encerrou, a mesma fica ligada durante um certo tempo (*token* da sessão). Nesse hiato temporal, com a sessão ativa, o utilizador ao abrir uma nova página *web* faz correr o *script* malicioso introduzido pelo criminoso cibernauta, que irá aproveitar-se de todas as *cookies* existentes.

Ambos os ataques pressupõem uma rutura na segurança dos nossos sistemas informáticos. Tipicamente corresponde à invocação da operação GET do protocolo HTTP. Ou seja, a operação GET corresponde a um pedido feito ao servidor e ao visitarmos determinada página *web* estamos a "fazer correr" um pedido GET. Aplica-se ao ataque de CSRF porque é necessário ter um método GET de forma a "apanhar" a página maliciosa.

O ataque típico de *phishing* é o de encaminhar alguém para uma página falsa, em muito idêntica à página original, no entanto o *phishing* também pode originar outros tipos de ataques. O modo de execução de um ataque de *phishing* através do envio de mensagens de correio eletrónico pressupõe que mensagens de correio eletrónico enviadas suportem anexos, geralmente atrativos que o utilizador descarrega com o total desconhecimento do seu conteúdo. Muitas das vezes essas mensagens, depois de abertas, redirecionam para um sítio da Internet onde é feito o *download* do conteúdo malicioso.

A iliteracia informática reflete-se em casos como este, porque o utilizador desconhece que foi ardilosamente induzido a tornar a sua máquina mais vulnerável, comprometendo a

segurança do sistema. Geralmente, o utilizador clica num *link* que aparece na mensagem que recebeu, descarregando automaticamente o programa malicioso; ou abre um arquivo em anexo que contém o programa malicioso; ou insere manualmente informações num *site* falso. Ao descarregar-se o programa malicioso, o mesmo aloja-se algures no sistema operativo, permanecendo até ao momento em que o utilizador tenta aceder à página da sua instituição bancária. O programa malicioso poderá ter ainda outras funcionalidades, como a de *keylogger*, que irá permitir gravar tudo aquilo que o utilizador digita no seu teclado.

Vamos passar a registar, em anexo, alguns dos ataques de *phishing* que se têm verificado com maior frequência, segundo informações da Caixa Geral de Depósitos[155]:

Figura v

"Ataques de "Phishing" com recurso a mensagens falsificadas de e-mail, com referências à Caixa, contendo links fraudulentos passíveis de comprometer a privacidade e a segurança de clientes. -6 de Abril de 2015

Os destinatários destas mensagens são induzidos a aceder incautamente a *links* que remetem para páginas fraudulentas na Internet, as quais, simulando os serviços de *Internet Banking* da Caixa visam a recolha de dados bancários e outra informação confidencial para uso ilícito.

[155] Disponível em https://www.cgd.pt/Seguranca/Seguranca-Phishing/Pages/06-04-2015-Email-de-phishing.aspx (Consultado 3 Março 2015).

Exemplo de e-mail falsificado que utiliza a imagem da Caixa,
contendo uma falsa notificação e um link fraudulento que não deve ser acedido

Figura vi

"Ataques de "Phishing" com recurso a mensagens falsificadas de e-mail, com referências à Caixa, contendo links fraudulentos passíveis de comprometer a privacidade e a segurança de clientes."- 19 de Junho de 2015

Por seu turno, *spear phishing* constitui uma variante muito mais proeminente e perigosa, porque é construída tendo em conta um individuo em particular, e aí o atacante prepara o ataque à medida da vítima. Para o efeito exige-se um investimento muito superior quando comparado com o tradicional ataque de *phishing*, porquanto no segundo pressupõe o envio a milhares de destinatários desconhecidos, no primeiro o sucesso da operação reside na familiaridade. Consiste no envio de uma mensagem de correio eletrónico que, aparentemente, parece de um remetente conhecido ou de uma empresa que conhece, mas que na realidade, não é e que tem como desiderato a subtração de número do cartão de créditos e das contas bancárias, palavras-passe, e outras informações sigilosas.

Tendo em conta que esta atividade delituosa tem uma dimensão transnacional "é difícil combater o *phishing*, a não ser pela prevenção"[156]. Para prevenir ataques de *phishing,* os utilizadores devem de ter conhecimento dos vários tipos de práticas de *phishing* empregues neste tipo de ataques bem como também devem proteger-se com ferramentas *anti-phishing.* O recomendável será o utilizador ter um risco de sensibilidade em não revelar dados sensíveis ou certificar-se que se trata de uma comunicação cifrada, em HTTPS. No que respeita à proteção

[156] Verdelho, Pedro. " Phishing e outras formas de defraudação nas redes de comunicação". In *Direito da Sociedade da Informação – Vol. VIII,* Associação Portuguesa do Direito Intelectual. Coimbra Editora, 2009, p. 413.

contra o *phishing*, dever-se-á ser capaz de identificar e reconhecer uma mensagem de *phishing*, tal como possíveis indícios de falsidade. No entanto, para que os *phishers* sejam bem-sucedidos na sua pretensão, será necessário a verificação de duas condições, isto é, são capazes de enganar as suas vítimas e que as ações resultantes por parte das vítimas são benéficas para os atacantes.[157]

Dever-se-á tomar em atenção que, em circunstância alguma digitar palavras-passe em supostos correios eletrónicos que se digam fidedignos. Geralmente este tipo de correio eletrónico apresenta erros gramaticais, que não são comuns no tipo de correio eletrónico enviado pela entidade fidedigna (indícios de falsidade), Terá que se ter em conta que no campo do remetente aparece o endereço da instituição, e como tal consegue-se perceber se o *e-mail* é ou não verdadeiro. Em suma, o *phishing* usualmente afeta instituições bancárias, ou instituições públicas como o exemplo da Administração Tributária e ter em linha de conta que nem as entidades bancárias, nem outras instituições públicas solicitam o envio de dados pessoais por correio eletrónico. Muitas entidades utilizam protocolos de segurança, que têm como objetivo o reforço de segurança informática, nomeadamente o «HTTPS» no entanto, também são ferramentas falíveis que não conseguem por fim a atividades delituosas, pois continuam a haver ataques de *phishing* com o uso de direções HTTPS na URL.

1.2.3. SMiShing

As hipóteses de um dispositivo móvel ser alvo de ataques aumentam se ligado à Internet.[158] As mensagens de texto são o meio mais comum de comunicação à distância, sendo previsível o envio de um trilião de mensagens de texto recebidas em cada dia, em todo o mundo. Para muitas pessoas seria impensável o telemóvel ser penetrável e é importante que a sociedade se consciencialize de que os ataques de *phishing* também são uma preocupação nos dispositivos móveis.

[157]Disponível em: http://www.markus-jakobsson.com/want-to-avoid-spoofing-click-to-see-how (consultado 20 Novembro 2015).

[158] Disponível em: http://www.ijcsi.org/papers/IJCSI-10-1-3-338-344.pdf, p. 339. (consultado 15 Dezembro 2015).

O ataque de SMiShing, variante do *phishing*, como a própria nomenclatura indica (-shing), tem como objetivo "levar o utilizador a fornecer informação pessoal"[159], através de SMS dos telemóveis, designadamente ser usado enquanto estratégia para "enganar" o recetor da mensagem a transferir dinheiro da sua conta bancária. Segundo um estudo, prevê-se que todos os dias, 1 em 20 utilizadores clique, inadvertidamente, em *links* de *phishing* nos seus dispositivos *android*.[160]

No Direito Penal Espanhol, seguindo o pensamento de Fátima Flores Mendoza[161], esta nova conduta enquadra-se no artigo 399º do Código Penal Espanhol que se reporta à falsificação de cartões bancários e que, naturalmente, entraria em concurso com o crime de burla informática previsto no artigo 248.2 c), punindo a operação patrimonial em prejuízo de terceiro realizada com cartões bancários ou com a informação aí contida.

1.2.4. Vishing

O *vishing*[162], como o próprio nome indica, é a conjugação entre "*voice*" (voz) e "*phishing*"[163] que utiliza engenharia social sobre o sistema de telefonia. Portanto, o vishing visa o ataque através de PSTN[164] usando mensagens de voz para obtenção ilícita de dados sigilosos, como dados bancários e para eventuais roubos de identidade, tal como sucede no *phishing*. Com efeito, uma conversação de telefone em tempo real aumenta significativamente, a eficácia de engenharia social, o que não sucede nos casos dos *e-mails* por constituírem uma ferramenta assíncrona, e por terem de ser abertos e lidos deixam menos margem de ataque aos atacantes

[159] Dias, Vera Marques. "A Problemática da Investigação do Cibercrime". In *DataVenia – Revista Jurídica Digital,* Ano 1, n.º1, ed. Joel Timóteo Ramos Pereira. DataVenia. Julho, 2012, p. 66. http://www.datavenia.pt/ficheiros/edicao01/datavenia01_p063-088.pdf. (consultado 20 Novembro 2015).

[160] Disponível em: http://www.ijcsi.org/papers/IJCSI-10-1-3-338-344.pdf, p. 339. (consultado 15 Dezembro 2015).

[161] Mendoza, Fátima Flores. "RESPUESTA PENAL AL DENOMINADO ROBO DE IDENTIDAD EN LAS CONDUCTAS DE *PHISHING* BANCARIO." *Estudios Penales y Criminológicos* vol. XXXIV (Julho 2014): 301-339,p.303-304.

[162] Curiosamente é uma variante do *phishing* pouco conhecida, no entanto, tem ultimamente tido um impacto exponencial. Para o efeito Cfr. http://home.deib.polimi.it/fmaggi/downloads/publications/2010_maggi_vishing.pdf (consultado 20 Novembro 2015).

[163] Ollmann, Gunter. "The vishing guide." *http://www. infosecwriters. com/text resources/pdf/IBM ISS vishing guide GOllmann. pdf, IBM, Tech. Rep* (2007).

[164] Através de uma rede pública de telefonia comutada (RTPC) é uma rede tradicional, de comutação de circuitos, otimizada para comunicação por voz em tempo real.

para atrair as vítimas. À dissemelhança do *phishing*, é inerentemente mais difícil de analisar o *vishing* por ser de difícil rasto.

Como se processa este ataque? O agente do crime tem acesso a um número indeterminado de números de telefones. Quando a vítima atende o telefone ouve uma gravação automática que a informa que a sua conta bancária foi comprometida, seguindo-se a informação de que terá que ligar para um outro número gratuito a fim de redefinir as suas configurações de segurança. Depois ouve uma outra mensagem automática que solicita o número da conta bancária da vítima e outros dados pessoais através do teclado do telefone.

1.2.5. Pharming

Uma outra variante de fraude *online*, mais aprimorada e perigosa, é o *Pharming* (*farming* conjugado com *phishing*). Esta técnica, para além de pressupor um processo técnico mais avançado, tem como finalidade o furto de dados sensíveis, nomeadamente números de cartão de crédito, dados de conta, senhas, entre outros. Diferentemente com o que sucede no *phishing*, o *pharming* pressupõe um controlo de um ponto de uma infraestrutura de comunicação. O ataque mais frequente, em sede de *pharming* é o comprometimento do *router*, melhor dizendo, todos aqueles utilizadores que utilizam aquela infraestrutura serão explorados simultaneamente porque o atacante consegue controlar parte da rede onde passa essa informação.

Outra forma de ataque tem lugar quando o delinquente usa um processo denominado como "*DNS cache poisoning*"[165] que consiste em suplantar o sistema de resolução dos nomes de domínio (DNS), alterando a configuração do servidor DNS do sistema, com vista a conduzir/redirecionar os utilizadores para uma página *web* falsa, clonada da real ou alterando o *host file* no computador da vítima. Tanto o servidor DNS como o *host file* contêm direções dos IPs ou sequência numérica das direções URL das páginas visitadas. Assim o *pharming* muda as direções de IP contidas no servidor DNS ou no *host file*, conduzindo o utilizador a uma página em tudo idêntica à da pretendida. Não obstante, ressalvamos que a clonagem de páginas *web* falsas também tem lugar em sede de *phishing*, nomeadamente quando se recebe na caixa de

[165] Stewart, Joe. "DNS cache poisoning–the next generation." *2007-08-25). http://www. secureworks. com/research/articles/dns-cache-poisoning* (2003). http://www.ouah.org/DNScp.htm.

correio eletrónico *e-mails* duvidosos, com links de supostamente entidades fidedignas. Em matéria de *pharming*, Pedro Verdelho pronunciou-se referindo-se à difusão de ficheiros ocultos que se auto-instalam nos computadores e uma vez alojados, alteram de forma oculta os arquivos do sistema., designadamente os ficheiros contendo os "favoritos" e o registo de *cookies*, de modo a que o utilizador quando aceder ao seus habitual *site* bancário é redirecionado para um outro site construído e disponibilizado em métodos idênticos ao do *phishing*, tornando muito difícil reconhecer uma fraude.

O processo do ataque de *pharming* funda-se em aceder ao servidor DNS e modificar as direções URL e de IP numérico no próprio *browser* reconduzindo as vítimas para um DNS controlado pelos delinquentes[166]. A vítima escreve o URL correto, mas desconhece que a tradução daquele nome resulta de um endereço IP de um *site* que é uma cópia do site original, criado, gerido e desenhado por um atacante. Neste caso a vítima é ludibriada pelo servidor DNS que foi subvertido pelo atacante, criando desta forma a sua própria "quinta" (pharm(farm)) composta pelas vítimas. A vítima e o servidor desconhecem que estão a ser alvo de um ataque de *pharming*. Trata-se geralmente de cópias de *sites* de instituições bancárias. A vítima para «autenticar» a sua operação indica as suas chaves de acesso, sendo que as mesmas serão depois utilizadas pelos *crackers*, para acederem à verdadeira página da instituição bancária e aí poderem efetuar as operações que entenderem, e portanto, subtrair o património da vítima. Esta entrada na tabela de endereços IPs direcionada a uma página que se crê ser a página original, sendo a página maliciosa, é o elemento caracterizador do *pharming.*

Resumidamente:

1. o delinquente ataca o servidor DNS usado pela vítima, alterando o IP associado ao url «www.bank.com» para um outro IP ilegítimo de um servidor que contém uma réplica desse site;
2. A vítima introduz o endereço «www.bank.com»;
3. O computador questiona o servidor DNS para saber o IP do URL «www.bank.com»;
4. O servidor DNS devolve o IP usado pelo delinquente;
5. A vítima é direcionada para o *site* falso.

[166] Segundo a autora Fátima Flores in *Respuesta Penal al Denominado Robo de Identidade n las Conductas de Phishing Bancario*, tratar- se-á de *pharming* local.

O ataque *cache poisoning*[167] é, potencialmente, o ataque mais proeminente e perigoso em matéria de DNS. O protocolo DNS é intrinsecamente vulnerável ao ataque *cache poisoning* provocando o comprometimento da integridade e segurança do sistema.

Tanto a técnica de *phishing* como a de *pharming* visam a obtenção fraudulenta de quantias monetárias, logo os agentes criminosos estarão a consumir o crime de burla informática. A grande diferença entre o *phishing* e o *pharming*, é a pessoa que é atacada; No *phishing* a vítima é convidada a seguir links aparentemente genuínos, mas que não o são ao passo que no *pharming* recebe-se os *links* genuínos e a vítima é convidada a revelar os dados sensíveis, sendo que o elemento comprometido é o *router* (normalmente existe um DNS no *router*). Portanto, o *phishing* estará no "*client-side*", ao passo que o *pharming* no "*server-side*".

Do ponto de vista do utilizador, deverá ter comportamentos preventivos na medida em que quando introduz dados sensíveis está a fazê-lo através de HTTPS e não de HTTP. Desta forma assegura que o homólogo de comunicação é genuíno através da utilização de protocolos de comunicação seguros.

1.2.6. Skimming

Contrariamente ao que acontece com outras técnicas presentes neste estudo, o *skimming* não se utiliza da infraestrutura Internet para obtenção fraudulenta de dados.

Ao tentarmos enquadrar esta técnica informática, deparamo-nos quase instantaneamente com o estudo da contrafação de cartões bancários. Eis algumas reflexões acerca do mesmo. A perpetração do crime (crime por excelência em matéria de fraudes relativas a cartões bancários) carece de uma aptidão, inovação e sofisticação por parte do contrafator. Para o efeito é necessário o desmantelamento de fábricas ilegais de dispositivos de clonagem, com particular incidência na Roménia[169].

[167] *Cache poisoning*, também denominado por DNS *cache poisoning* é o "envenenamento" de um sistema de nomes de domínio de um servidor, que se processa através da alteração de um endereço de internet com outro, por sua vez, ilícito. Quando um utilizador procura uma página com esse endereço, a solicitação é redirecionada para o endereço falso, não fidedigno.

[169] Informação disponibilizada no Relatório Geral das Atividades da Europol de 2010, p. 46.

Para além da destreza, muitas vezes aliada a grandes habilidades manuais e cognitivas, necessita de material especifico para o efeito, o *skimmer*. A aquisição tem-se revelado demasiado fácil; a Internet oferece diferentes modelos, por vários preços, muitas das vezes apetecíveis. O *skimmer* traduz-se num aparelho de leitura e gravação de bandas magnéticas. A técnica que recorre à aquisição de dados de modo fraudulento é designada por *skimming*, que pode operar, numa simples transação comercial, sem que o legítimo detentor do cartão se aperceba. O *skimming* é apenas mais uma das maneiras que os delinquentes usam para obter e aceder a uma identidade e a dados bancários.

Segundo o Relatório Geral sobre as Atividades da Europol de 2010, *skimming* consiste na "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. 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". A contrafação de cartões bancários é realizada através da cópia dos dados contidos na banda magnética de um determinado cartão bancário, seja ele de que natureza for.

Por seu turno, a banda magnética é constituída por três pistas, nas quais são gravados dados bancários. Na primeira encontra-se armazenada informação alfanumérica respeitante à identificação do titular do cartão e ao número da sua conta; a segunda é numérica contendo designadamente informações relativas ao Banco emissor do respetivo cartão, data da sua emissão, o nome do titular e o número de conta adstrito ao cartão, sendo que esta pista 2 é geralmente o alvo da contrafação; e por fim, a terceira pista que se encontra quase sempre em branco. Um exemplo recorrente, é o do empregado de restaurante que encontrando-se na posse do cartão de multibanco do cliente, que deseja proceder ao pagamento, o passa no leitor/gravador, procedendo imediatamente à gravação do nome do titular do cartão, número da conta bancária associada ao mesmo, como também o número e sua data de validade, antes de o inserir no POS do restaurante.[170]

[170] Para os respetivos efeitos, situações delituosas como esta, entre outras, são monitorizadas pela *Paywatch* cuja atividade é a de detenção de fraudes efetuadas com cartões bancários. A mesma é efetuada mediante a observação de uma série de parâmetros que deverão ocorrer aquando de uma operação de pagamento com cartão bancário. Quando se encontram verificados, são criados alertas, que após serem

A fraude de cartão bancário verificada pelo *skimming* também se manifesta através da instalação de dispositivos em máquinas ATM[171]. Os sujeitos ativos desta prática delituosa são geralmente oriundos da Europa de Leste que, recorrendo a equipamento eletrónico, procedem à sua instalação em caixas automática afigurando-se dissimulado na própria caixa. Têm como função, por um lado, à leitura de bandas magnéticas dos cartões bancários e por outro, filma e grava a introdução dos códigos PIN. É dissimulado no leitor original da caixa automática um leitor de bandas magnéticas ilícito e a câmara que filma e grava a introdução dos códigos PIN passa despercebida pela pessoa que utiliza a ATM devido ao seu tamanho reduzido.

Paralelamente a estas situações, também existem casos em que se procede à introdução de um segundo teclado que é instalado sobre o existente nas ATM registando, assim, todos os códigos PIN pelos titulares que utilizaram a caixa automática. Para um maior lucro, estes sujeitos instalam estes dispositivos em centros tendencialmente turísticos, bastante movimentados e ao escolherem um local como este vão dificultar a tarefa aos Bancos emissores (nomeadamente estrangeiros) dos cartões, pois demorarão mais tempo e sentirão mais dificuldade em reportar a fraude. Após recolherem os dados, e na posse dos mesmos descarregam-nos para um computador e procedem à regravação noutros cartões dotados de banda magnética que serão utilizados posteriormente para adquirir bens e serviços ou levantamentos de numerário.

Outro caso reporta-se à instalação de um pequeno dispositivo no interior de um sistema de POS que se destinam a ler a informação contida no chip, recolhendo assim dados dos cartões que efetuassem transações nesse terminal de forma a regravarem as mesmas em cartões com banda magnética.

É surpreendente a simplicidade dos materiais utilizados!

É evidente que estamos perante o crime de contrafação de cartões bancários. Não obstante, não podíamos deixar de referir que esta arte tem apenas um único propósito, o propósito de subtrair dinheiro! Através da obtenção/subtração dos dados, e utilizando-os em

---

analisados pela empresa, se se fundamentar uma suspeita, serão fornecidos às respetivas autoridades, à Policia Judiciária, mediante formalização de denúncia.

Para mais informações, consultar http://www.sibs.pt/pt/fps/grupo_sibs/Paywatch.html.

[171] A caixa automática ou ATM representa um modo de transmissão assíncrona.

próprio proveito, sem devido conhecimento do legítimo titular e sem autorização deste, procedem a transferências de quantias, gerando desta forma um prejuízo patrimonial à vítima. Vê-se, portanto, preenchida uma conduta típica do tipo legal de crime de burla informática.

A prática deste tipo de crimes, tais como tantos outros que necessitam de meios tecnológicos com uma elevada sofisticação têm denotado um progresso respeitante aos *modus operandi* utilizados.

Os *modus operandis* mais vulgares são os que se seguem[172]:

Figura vii

Colocação estratégica de câmaras nas caixas de ATM,designadamente câmaras de telemóveis que transmitem a informação em tempo real através de dispositivos de wireless que colocam por detrás de equipamentos que colocam sob o visor da caixa ATM.

Poderá existir a colocação de uma microcâmara, com um orifício praticamente impercetível, que é colocada por detrás de uma placa que instalam sobre o teclado permitindo, desta forma, a gravação do código PIN que fora digitado.

[172] Imagens retiradas de http://www.cityofsanmateo.org/DocumentCenter/View/5968 (consultado 20 Janeiro 2016).

Figura viii

Uma outra forma, é a colocação de câmaras no local onde se encontram as informações bancárias em forma de folhetos, que grava tudo o que digita.

Figura ix

Instalação de teclados falsos por cima dos originais, o que permite gravar os códigos PIN.

Figura x

Instalação de dispositivo na entrada onde introduzimos o cartão bancário. Estes dispositivos, geralmente, contêm hardware que tem a capacidade de ler a banda magnética constante no cartão bancário.

A primeira imagem demonstra o painel de uma caixa ATM não adulterada, enquanto na segunda é evidente a instalação de dispositivo. Ao observar a segunda imagem, há a instalação de dispositivo no local onde se introduz o cartão bancário, e pese embora o facto de ter uma aparência de ser parte do terminal, o que é evidente é que a caixa ATM original no local onde se introduz o cartão bancário contém uma luz, e na segunda imagem isso não se verifica.

Atualmente existem dispositivos de tamanho muito reduzido, que se encaixam no orifício do local de introdução do cartão que copia a banda magnética, que são capazes de enganar a maioria das pessoas devido ao seu tamanho reduzido e existe a convicção de que tais dispositivos pertencem a máquina.

Figura xi

Instalação de dispositivo na entrada onde introduzimos o cartão bancário. Estes dispositivos, geralmente, contêm hardware que tem a capacidade de ler a banda magnética constante no cartão bancário.

Na primeira foto, o titular insere o cartão, marca o código PIN e o dispositivo retém o cartão. Este falso encravamento do cartão, faz com que a pessoa abandone o local para se dirigir ao Banco ou para mais tarde ligar a pedir para anular o cartão, e no que medeia entre uma situação e a outra, o agente criminoso retira o dispositivo, tendo acesso ao código do cartão do lesado.

A fim de evitar estes desfalques, dever-se-á sempre inspecionar a caixa automática e ver a aparência de outra caixa automática, para ver se em tudo se encontram semelhantes.

Atualmente, com a disseminação dos cartões bancários com chip, com principal incidência a Europa, esta problemática tem reduzido, aumentando assim a segurança contra falsificações e contrafações e recuperando a fiabilidade dos meios utilizados. Não obstante, nos EUA, os cartões bancários ainda se encontram na dependência na banda magnética para identificação, tornando estes ataques altamente perigosos.

Tomemos como exemplo o SMiShing, explanado anteriormente, utiliza mensagens de texto para obter o número de cartão bancário e respetiva data de validade com a finalidade de «reproduzir» novos cartões bancários (falsos) através da técnica de *skimming.*

1.2.7. Software tipicamente classificado como malware

Apenas ressalvamos que excecionalmente podem ser usadas como mecanismos de fortalecimento da segurança do utilizador. Não são inerentemente más ferramentas. No entanto, o entendimento que se segue é a perversidade na utilização destas ferramentas.

1.2.7.1. Cavalo de Tróia – *Trojan Horse*

Reza a lenda que o cavalo de Tróia fora uma oferenda disfarçada de instrumento de guerra pelos gregos com vista a trespassar a cidade de Tróia. No mundo da informática, o cavalo de Tróia é muito mais do que apenas um mito.

Na informática, o cavalo de Tróia poderá ser entendido como um programa de *software*, geralmente recebido como se de uma «benesse» se tratasse, isto é, disfarçam-se de programas regulares (e.g. jogos, programas antivírus, etc.) com objetivo de executar funções, não só para as que foi inicialmente concebido, mas também funções maliciosas sem o conhecimento do utilizador, podendo causar danos sérios ao nosso computador.

O *trojan horse*, vulgo cavalo de Tróia, traduz-se na técnica informática que consiste num programa que se aloja no sistema informático do utilizador/vítima mediante correio eletrónico e que tem como função modificar a configuração do sistema informático com a finalidade de captar informação sigilosa, tal como as operações bancárias em linha *através do man-in-the-middle*[173].

As funções maliciosas executadas por um cavalo de Tróia podem comportar a: instalação de *keyloggers,* o furto de senhas e outras informações sensíveis tais como o número de cartão bancário, a alteração ou destruição de arquivos, entre outros.

A perigosidade do cavalo de Tróia está no facto de permanecerem ocultos no sistema do utilizador por algum tempo, sendo que os mesmo se ativam, essencialmente, aquando o acesso à página bancária da sua instituição bancária, deste modo, os delinquentes capturam as chaves

[173] É uma forma de ataque que consiste na interceção de dados por um adversário ativo, que faz-se passar por outro agente comprometendo a segurança dos dados.

de acesso associadas às suas contas bancárias. Essa obtenção de chaves de acesso também poderá ser realizadas através de programas maliciosos que intercetam a informação no momento em que se digita as chaves de acesso nos serviços de *homebanking* , capturando as pulsações do teclado, ou seja, através dos *keyloggers*.

O cavalo de Tróia distingue-se dos vírus, pelo simples facto de não propagar réplica de si mesmo de forma automática. Contrariamente ao vírus, o cavalo de Tróia consiste, normalmente, num único arquivo que necessita de ser impreterivelmente executado para produzir os seus efeitos, ou seja, para se instalar no computador da vítima. Enquanto a sua execução, estes programas são suscetíveis de enviar dados sigilosos para outro computador, através da instalação de *keyloggers* ou *screenloggers*[174], alterar informações, apagar e/ou alterar dados, formatar o disco rígido ou instalar *backdoors.*[175] No entanto, importa não confundir cavalo de Tróia com *backdoors*, porquanto os primeiros são instalados ingenuamente pelo utilizador, o *backdoor* é um mecanismo que está implantado no sistema operativo que permite a uma entidade externa aceder e/ou controlar a máquina. O último pode ser conscientemente implementado, por exemplo, por um produtor de *software* sem que o proprietário da máquina tenha conhecimento. O cavalo de Tróia pode ter os mesmos propósitos que o *backdoor*, mas difere por ser "convidado a entrar" pelo utilizador, ao passo que o *backdoor* entram pela "porta dos fundos".

Segundo um estudo levado a cabo pela Kaspersky Lab[176] foram detetados, no segundo trimestre de 2015, um total de 291.800 novos programas de *malware* móvel, um crescimento de 2.8 vezes comparativamente ao período anterior. O programa malicioso mais evidente é a

[174] O *screenlogger* é um programa malicioso que tira prints do ambiente de trabalho do computador, informando onde o cursor do rato foi clicado, obtendo informações confidenciais e/ou outras informações confidenciais.

[175] Consiste num programa secretamente implementado num determinado computador cujo desiderato é obter informações e dados armazenados, interferir com a operação ou obter controlo total do sistema, permitindo desta forma que os cibernautas mal-intencionados tenham controlo sobre a máquina.

[176] Trata-se de uma empresa russa produtora de *software*s de segurança para a Internet que segundo informação disponibilizada em http://wintech.pt/82-noticias/kaspersky/19602-trojans-bancarios-concebidos-para-infetar-dispositivos-moveis-continuam-a-crescer- fez um estudo sobre o desenvolvimento do Trojan em dispositivos móveis (consultado 20 Novembro 2015).

versão mais recente do *Trojan-SMS.AndroidOS.OpFake.cc,* que, por seu turno, visa atacar instituições bancárias (crê-se que tem capacidade para atacar 114 instituições bancárias).[177]

Alguns sintomas possíveis de infeção poderão fazer-se notar (também pode não haver nada) como alguma atividade anormal no computador.

Para colocar termo ou em jeito de prevenção de instalação dos mesmos, é aconselhável a instalação de um antivírus eficiente e atualizador que possibilite a deteção de programas instalados por estes programas maliciosos.

1.2.7.2. Keylogger

Existe uma diversidade ilimitada de *keyloggers.* O *keylogger* consiste num programa do tipo *spyware*[179] de vigilância, que tem como objetivo captar, registar e armazenar tudo o que se digita, ou seja, reconhece os caracteres introduzidos pelo utilizador. Tem como principal objetivo a obtenção de números de cartão bancário e senhas. Após a captura de dados sensíveis e sigilosos, que constituem um verdadeiro ataque à nossa privacidade, os criminosos os utilizam-nos ilicitamente, à revelia do utilizador e para seu próprio proveito.

Atua com os seus próprios mecanismos que permitem o envio automático das informações aos seus recetores e atuam normalmente ao nível do *software*, já sendo possível em forma de *hardware* através de dispositivos situados entre o cabo do teclado e a porta do computador, contendo uma memória interna que grava tudo o que o utilizador digitar naquele computador. A informação recolhida será transposta para um ficheiro de texto, no que se incluirá o *username* e a *password* de acesso bancário, previamente digitadas pelos legitimo utilizador. O *keylogger* pode ser presencial, tomemos como exemplo, o caso das caixas de supermercado, nos terminais de pagamento já existem proteções para evitar que a pessoa seguinte veja a digitação do código, ou até mesmo para evitar que seja captado por uma câmara de vídeo.

[177] Para este efeito, chamamos à colação, o *Trojan Chthonic* que é considerado um dos programas de *malware* bancário mais prejudiciais, que visa a infeção do sistema e recolher informações acerca do sistema, o roubo de senhas de acesso e de arquivos de registo, habilitando, desta forma, o acesso remoto ao sistema para que os cibercriminosos possam controlar a máquina à distância, para que possam furtar dados bancários e aceder às contas das vítimas.

[179] Como o próprio nome indica *spyware* é um «programa espião» que visa recolher informações sobre o utilizador, sem o conhecimento ou o consentimento do mesmo.

Também se corre o risco de encontrar pequenas câmaras dissimuladas juntos das ATM, como já referimos no ponto anterior.

Uma vez que as contas bancárias são os alvos principais dos delinquentes, inicialmente as instituições bancárias adotaram medidas preventivas para que isso não acontecesse, através de teclados virtuais. Novas modalidades de técnicas fraudulentas emergiram comprometendo, mais uma vez, os clientes que aderiram ao serviço de *homebanking*. Uma dessas técnicas são os *screenloggers* que funcionam praticamente como um *print* e que têm capacidade de armazenar a posição do cursor. Ao terem acesso às credenciais bancárias acedem às contas das vítimas. Atualmente as instituições bancárias utilizam o cartão matriz que é uma das formas de impedir qualquer *keylogger* ou *screenlogger.*

Para que um *keylogger* se instale na nossa máquina, é necessário que venha alojado a um programa de *spyware* ou cavalo de Tróia que são geralmente enviados por *e-mail* sem que o utilizador tenha conhecimento de que são programas maliciosos, ou seja, o programa ao ser executado permite que o *keylogger* se instale no computador. Todavia, genericamente a ativação do *keylogger* está condicionada a uma ação prévia por parte do utilizador; o *keylogger* é muitas vezes acionado quando o utilizador visita determinados *sites* específicos de comércio eletrónico.

O risco potencial dos *keyloggers* é incomensurável porque é uma das muitas razões pelas quais, as pessoas veem a sua informação ser alvo de roubo.

1.2.7.3. Spyware

O *spyware* é um tipo de *malware*[180] (*software* malicioso) que recolhe informação de um sistema de computação sem o devido consentimento do respetivo titular. Em tudo similar a outras técnicas que iremos abordar. É capaz de capturar o que se digita (à semelhança do que acontece com os *keyloggers*), endereços pessoais de correios eletrónicos, e acima de tudo dados sensíveis, como informações bancárias. Após a recolha, os dados são enviados para terceiros que, por seu turno, vendem essa informação a outros ou usam-nos para fins publicitários ou SPAM, roubo de identidade ou para perpetração de crimes de índole económica.

[180] Segundo notícia disponibilizada em http://www.itchannel.pt/news/seguranca/quase-5-em-cada-100-pcs-portugueses-estao-infetados-com-*malware*, - quase 5 em cada 100 computadores portáteis portugueses estão infetados com *malware* (consultado 20 Novembro 2015).

As aplicações de *spyware* encontram-se, normalmente, alojadas em programas de *freeware* ou *shareware*[181] que podem ser descarregados da Internet. Ao descarregar-se o programa e uma vez instalado, o *spyware* atua enquanto agente que monitoriza toda a atividade que o utilizador tem na sua máquina e da navegação que faz na Internet. Após esta vigilância, transmite a informação para um terceiro, como já foi referido.

O *spyware* tem vindo a se propagar com cada vez mais tenacidade na "rede das redes", mas o que motiva os agentes a utilizá-lo? De grosso modo, são agentes cujos propósitos são a recolha de dados sensíveis por razões financeiras, todavia muitos agentes que utilizam o *spyware* são pessoas "vulgares" que fazem-no para espiar alguém que lhes é próximo. Os sujeitos ativos poderão ser: pessoas que espiam para fins pessoais, associações criminosas, ou então os denominados como *trusted insiders* que são aqueles que têm acesso físico a um determinado computador por razões legítimas, organizações de *marketing*, e por fins os prevaricadores que atuam por sua conta[182].

O *spyware* tem vindo a disseminar-se arrebatadamente. Existem algumas atividades que potenciam essa proliferação e o risco de ser alvo de *spyware*, nomeadamente a instalação de *software* não licenciado pirata.

1.3. Algumas medidas preventivas

Algumas conclusões podem ser extraídas do que foi exposto: os crimes informáticos ou praticados através da informática precisam de ser estudados de modo próprio, por apresentarem um perfil específico e um *modus operandi* muito peculiar, incluindo a perpetração de burlas informáticas. E assim, a aquisição de dispositivos tecnológicos exige o mínimo de condições de prevenção e segurança para que o utilizador esteja devidamente protegido.

São indispensáveis e exigíveis medidas preventivas que façam frente a todas as fraudes com que nos deparamos. A possibilidade de cometer uma fraude de onde se pretende obter um

[181] *Freeware*, como o próprio vocábulo indica, consiste num programa de computador que não está sujeito ao pagamento de licenças de uso; O *freeware* distingue – se do *shareware*, que por seu turno, o utilizador tem de pagar para aceder à funcionalidade completa ou com um tempo limitado de utilização gratuita.

[182] Disponível em http://www.cs.toronto.edu/~lloyd/howtoDCS/office/email/spam/spywarehome_0905.pdf (consultado 20 Janeiro 2016).

benefício económico, resultando do mesmo um prejuízo patrimonial, afetam a maior parte das operações económicas, ganhando magnitude e expansão através da Internet. Os equipamentos utilizados, desprovidos de medidas de proteção, apresentam uma grande vulnerabilidade, sendo exigido ao utilizador a adoção de uma «cultura de segurança» no meio Internet, tal como deverá ter no seu quotidiano. As medidas de que falaremos dentro de momentos deverão ser complementadas por boas práticas por parte do utilizador, por uma postura de precaução e desconfiança que se tem na vida, digamos, real no momento de guardar os seus códigos, palavras-passe e outros dados para que os mesmos não sejam subtraídos e utilizados para fins ilícitos ou até para impossibilidade de aceder às contas bancárias.

A título de medidas preventivas no geral, dever-se-á: evitar aceder às contas bancárias em locais públicos que exijam a identificação mediante digitação de chaves, contudo, no caso de se o fazer deverá encerrar o *browser*, garantir que os *cookies* estão desativados e limpar a cache; atualizar o *software* bem como o programa de antivírus e *antispsyware*; modificar periodicamente as chaves de acesso; nunca aceder a pedidos que solicitem a introdução de chaves de acesso, por muito fidedigna que pareça a página; comprovar que o sítio a partir do qual se comercializa transmite informação cifrada, mas mais do que cifrada deverá de ser apresentado certificado reconhecido por uma terceira entidade fidedigna; não anotar as chaves de acesso em locais acedíveis ou transmiti-los a terceiros; guardar cópia das operações que se fez em sede de *homebanking* ou em sede de comércio eletrónicos; rever periodicamente as contas de forma a controlar a existência de movimentos estranhos; analisar as datas de acesso ao *homebanking* de forma a ver se corresponde ao último acesso do respetivo utilizador; entre outras. Com estas contramedidas e com boas práticas, o utilizador torna-se menos vulnerável a ataques que possibilitem a perpetração de burlas informáticas.

1.4. As organizações criminosas e os "mulas"

Os ficheiros recolhidos pelos agentes do crime aquando a instalação do programa malicioso no computador da vítima serão enviados para um servidor alojado em qualquer ponto do mundo, que se localizam em verdadeiros paraísos cibernéticos onde a malha legal é muito ténue ou praticamente inexistente no que diz respeito à sua penalização. Aquando a deteção dessas páginas e denúncia às autoridades, os membros da organização "deslocalizam" esses domínios para outros servidores, cujo sistema legal os favoreça, com o máximo de celeridade e mobilidade. O servidor, para o qual são enviados e depositados os dados ora recolhidos, é criado e mantido para finalidades ilícitas, onde os agentes criminosos acedem a esse servidor descarregando daí informação aí consignada respeitante a dados confidenciais de clientes das mais diversas instituições bancárias. Após procederem à subtração de importâncias da conta dos ofendidos ilegitimamente, através de parceiros que colaboram para com estas organizações criminosas, deslocam as verbas subtraídas para contas de cujos parceiros são titulares.

Este tipo de atividade ilícita é levada a cabo por organizações criminosas, concertadamente estruturadas, com *know-how* e altamente especializadas na área da informática. Têm como ocupação o desenvolvimento de aplicações e novas técnicas para a prossecução de fins ilícitos, nomeadamente à obtenção de credenciais de acesso bancário dos mais diversos utilizadores à escala mundial, utilizando portanto, o "cibercrime como forma de financiamento"[183]. Funcionam como verdadeiras empresas e são estruturalmente muito semelhantes a uma empresa fidedigna, tendo para o efeito: a gerência composta por líderes da organização e gestores da organização, departamento financeiro tal como contabilistas, caixas[184] e os "mulas", departamento técnico formado por programadores que desenvolvem *malware* e aplicações a utilizar pela organização como também *hackers, phishers*, *spammers* e fornecedores que dispõem de acolhimento seguro para servidores com teor ilícito e

[183] Dias, Vera Marques. "A Problemática da Investigação do Cibercrime". In *DataVenia – Revista Jurídica Digital,* Ano 1, n.º1, ed. Joel Timóteo Ramos Pereira. DataVenia. Julho, 2012, p. 69. http://www.datavenia.pt/ficheiros/edicao01/datavenia01_p063-088.pdf (consultado 20 Novembro 2015).

[184] Os caixas, são pessoas cuja função é controlar a atividade das contas, ou seja, as *drop accounts* e que, para o efeito, fornecem nomes bem como dados bancários a outros prevaricadoras mediante o pagamento de uma importância.

departamento comercial que integra os distribuidores cuja ocupação é transacionar os dados ilicitamente adquiridos.

Esta "máfia" vive de um mercado fechado, de uma tamanha complexidade que passa completamente despercebida à esmagadora maioria. Geralmente localizadas no Brasil e leste europeu, principalmente na Rússia[185], esta máfia é composta por uma rede transversal com ramificações transnacionais que para além de funcionarem concertadamente, dispondo desta forma de recursos financeiros e técnicos que lhes permite levarem a cabo os seus intentos, utilizam outros meios para prossecução dos seus fins. Recrutam os designados *Money Mules*[186], que atuam enquanto intermediários destas organizações. Os "mulas" são pessoas que são «usadas» para o transporte e lavagem de dinheiro ou até de mercadoria da mais variada espécie, são eles quem faz o trabalho. No caso em apreço, as pessoas são aliciadas a guardar nas suas contas as importâncias anteriormente subtraídas às vítimas, por força do *phishing*, para posteriormente a entregarem pessoalmente aos prevaricadores ou através de serviços como a Western Union, mediante uma comissão, que poderá variar entre os 5% a 10% do total dos valores transacionados[187].

O esquema de recrutamento é feito, normalmente, a partir do envio de milhares de *emails* com propostas aliciantes, de forma aleatória. Muitos dos que aceitam têm conhecimento do que se trata, outros nem tanto, agem em total ignorância, outros são movidos apenas por necessidades financeiras. Muitos dos esquemas de recrutamento *online* passam por ofertas/oportunidades de "trabalhar em casa" e têm como alvo pessoas que se encontram interessadas na conveniência e flexibilidade deste tipo de trabalho. Existem empresas legitimas que oferecem este tipo de trabalhos, portanto, os agentes do crime tentam frequentemente fazer a oferta o mais credível possível, de forma a que os utilizadores não sejam capazes de reconhecer uma oferta maliciosa, fazendo-o através de: elaboração cuidadosa de texto para que

[185] De entre as mais conhecidas existe a *Russian Business Network* (RBN). A Rússia sempre foi conhecida pelos seus programadores de vírus, designadamente vírus denominados por *Bagel, MyDoom, Netsky.* A RBN é uma infraestrutura e um prestador de serviços ao mais alto nível do cibercrime. Desenvolve atividades como, pornografia infantil, *phishing*, DDoS, tráfico onlie de droga, *botnets*, apostas, entre muitas outras. Uma das suas atuações mais proeminentes foi a feitura do s*oftware malware MPack* que serviu de ataque ao Banco da Índia em 2007. Disponível em http://www.bizeul.org/files/RBN_study.pdf (consultado 20 Janeiro 2016).

[186] Cfr. https://www.us-cert.gov/sites/default/files/publications/money_mules.pdf (consultado 15 Dezembro).

[187] Teixeira, Paulo Alexandre Gonçalves. " O Fenómeno do Phishing – Enquadramento Jurídico-Penal". Dissertação de Mestrado, Universidade Autónoma de Lisboa, 2013, p. 16.

o *e-mail* não se pareça com SPAM e para que o mesmo não seja retido por filtros de SPAM; colocação de *links* à disposição presumivelmente pertencentes a empresas reconhecidas ou promovem empresas que nem sequer existe; colocação dessas ofertas de trabalho em *sites* legítimos, incluindo *sites* direcionados para a procura de emprego.

O processo típico após o recrutamento e assentimento do futuro colaborador passa por em primeiro lugar a "empresa" recolher informações pessoais do mais recente associado e ainda poderá celebrar um aparente contrato de trabalho entre a empresa e o "mula"; num segundo momento a empresa cria uma conta bancária para que o mula a possa utilizar para depositar e transferir importâncias; o "mula" recebe determinada importância ou algum tipo de mercadoria; a empresa dá instruções ao "mula" de como transferir as importâncias, por transferência bancária, para outra conta bancária ou para entregar mercadoria a um terceiro e geralmente dão instruções para que o "mula" proceda a levantamento desses montante para os transferirem via *Western Union*[188], ou por outro meio semelhante para destinatário localizados no estrangeiro. Através deste processo, o agente criminoso recebe o dinheiro roubado ou a mercadoria, sem nunca ter estado envolvido diretamente em todo o processo. Ou seja, quem acaba por ser descoberto pelas autoridades respetivas é quase sempre o "mula", porque é o seu nome que aparece como fachada nas informações bancárias. Usualmente o agente criminoso só usa o "mula" uma vez, e visto terminado o seu papel na transação, o agente criminoso dissolve a relação e recruta um novo "mula". Desta forma, conseguem complicar as investigações policiais e passar despercebidos.

Estas organizações criminosas são constituídas por membros com elevada qualificação tecnológica, e possuem uma estrutura hierarquizada e organizativa bem delineada e com tarefas distribuídas aos elementos que integram estas organizações criminosas. Tendo em conta que as atividades levadas a cabo pela criminalidade organizada, se encontram cada vez mais complexas, diversificadas e internacionais, entendemos que devemos falar em delinquência organizada, designadamente de associação criminosa, prevista no artigo 299.º do CP[189]. O crime

[188] A *Western Union* consiste num serviços de transferência muito célere de dinheiro que se processa à escala mundial. Destina-se exclusivamente a particulares permitindo enviar ou receber dinheiro para/de outros países. A transferência poderá ser efetuada *online*, por via do Visa ou MasterCard, ou através de um Agente, em numerário, e por fim o destinatário poderá levantar a importância em postos de venda. Disponível em http://goo.gl/6Fnnqk (consultado 20 Janeiro 2016).

[189] *Artigo 299.º do C*

de associação criminosa pressupõe a comparticipação dos agentes do crime numa determinada atividade ilícita, que atua de forma concertada e cujos elementos integrantes têm uma função previamente delineada com objetivo de obter os resultados definidos pela organização.

No caso supra analisado, serão responsabilizados à luz do artigo 299.º do CP, todos os agentes responsáveis pela criação de empresas falsas e de *websites* que servem de suporte às mesmas que vão criando e mantendo pelo tempo que se justifique para recrutamento de "mulas", que não são só mais do que comparticipantes, cuja função passa por servirem de colaboradores que fornecem as suas contas bancárias para receção das verbas ilicitamente subtraídas. Os colaboradores, mais vulgarmente designados por "mulas", são elementos que mostram uma disponibilidade bem como uma subordinação à vontade coletiva que merece censura penal. Existe disponibilidade permanente devido ao lucro fácil, uma vez que o seu objetivo é única e exclusivamente o de receber, reenviar o dinheiro e beneficiar da respetiva comissão que lhe é atribuída.

1.5. O serviço de *Homebanking*[190]

Em primeiro lugar, não poderíamos avançar sem deixar algumas considerações relativamente ao contexto em que se insere o serviço de *homebanking*.

O avanço tecnológico tem vindo a insurgir-se cada vez com mais afinco nos últimos anos, remexendo todo o comércio jurídico, designadamente ao nível das relações bancárias e ao

---

Associação criminosa

1 — Quem promover ou fundar grupo, organização ou associação cuja finalidade ou atividade seja dirigida à prática de um ou mais crimes é punido com pena de prisão de um a cinco anos.

2 — Na mesma pena incorre quem fizer parte de tais grupos, organizações ou associações ou quem os apoiar, nomeadamente fornecendo armas, munições, instrumentos de crime, guarda ou locais para as reuniões, ou qualquer auxílio para que se recrutem novos elementos.

3 — Quem chefiar ou dirigir os grupos, organizações ou associações referidos nos números anteriores é punido com pena de prisão de dois a oito anos.

4 — As penas referidas podem ser especialmente atenuadas ou não ter lugar a punição se o agente impedir ou se esforçar seriamente por impedir a continuação dos grupos, organizações ou associações, ou comunicar à autoridade a sua existência de modo a esta poder evitar a prática de crimes.

5 — Para os efeitos do presente artigo, considera -se que existe grupo, organização ou associação quando esteja em causa um conjunto de, pelo menos, três pessoas, atuando concertadamente durante um certo período de tempo

[190]Para este efeito, partimos do estudo do acórdão 6479/09.8TBBRG.G1.S1 de 18 de Dezembro de 2013, disponível em: http://goo.gl/TV0RJS (consultado 20 Novembro 2015).

nível "do modo de funcionamento das instituições bancárias"[191]. O uso da informática veio possibilitar a rapidez, simplificação e desmaterialização da banca, designadamente nos seguintes aspetos: "contratação e prática de diversos atos bancários, execução de deveres de informação e de comunicação, designadamente quanto às chamadas obrigações de caixa e manutenção da contabilidade e o exercício da supervisão"[192]. A Internet reformou as práticas bancárias, sendo que o sistema de cartões bancários é hoje reflexo disso mesmo.

Através da emissão de cartões bancários é possível realizar uma imensidão de operações nomeadamente através dos serviços de *homebanking,* sendo possível, para o efeito, aceder a uma variedade de operações bancária em linha, tudo através de um simples dispositivo, o computador.[193] Indissociavelmente ligado ao depósito bancário, visto que não há abertura de conta sem fundos, o contrato de conta bancária designa-se como o acordo havido entre uma instituição bancária e um cliente, "através do qual se constitui, disciplina e baliza a respetiva relação jurídica bancária"[194]. Esta figura contratual, que constitui a relação jurídica, tem vindo a ser assumida pela jurisprudência e pela doutrina na espécie negocial de depósito.[195] Destarte, a abertura de conta pressupõe a possibilidade de aceder a um serviço proporcionado pela instituição bancária de efetuarmos operações através da Internet. Para tanto é outorgado um contrato de adesão entre a instituição bancária e o cliente.

Estamos perante o serviço de *Homebanking* ou banco ao domicílio. O mesmo consiste num serviço prestado pelas instituições financeiras que permite gerir e efetuar operações bancárias" tradicionalmente levadas a cabo nos balcões das suas sucursais"[196], agora através da Internet nos seus próprios domicílios ou escritórios originando, desta forma, " a consequente descentralização dos serviços prestados"[197]. A instituição bancária confere aos seus clientes, mediante aceitação de determinados condicionalismos, a possibilidade de utilizar de forma

---

[191] Guimarães, Maria Raquel. *As transferências eletrónicas de fundos e os cartões de débito: alguns problemas jurídicos relacionados com as operações de levantamento*. Coimbra: Almedina, 1999, p. 42.

[192] Cordeiro, António Menezes. *Manual de direito bancário*, 3.ª edição. Almedina, 2008, p. 149.

[193] Atualmente o serviço de *homebanking* também se encontra disponível nos *smartphones* e consequentemente em *tablets*.

[194] Antunes, José A. Engrácia. *Direito dos Contratos Comerciais.* Coimbra: Edições Almedina, 2009, p. 483.

[195] Cfr. Artigo 1185.º e 1187.º do C.C. Por outro lado o depósito bancário é regido pelos estatutos da instituição de crédito em tudo quanto se não achar prevenido no regime do depósito mercantil e mais disposições legais aplicáveis, designadamente o art. 407.º do Código Comercial.

[196] Guimarães, Maria Raquel. *As transferências eletrónicas de fundos e os cartões de débito: alguns problemas jurídicos relacionados com as operações de levantamento*. Coimbra: Almedina, 1999, p.42.

[197] Idem.

online, 365 dias, 24 horas por dia, um leque de diversas operações bancárias relativamente às contas de quem são titulares, através da junção de canais telemáticos que conjugam os meios informáticos com os meios de comunicação à distância, mediante uma página fidedigna da instituição bancária. As vantagens associadas à utilização do serviço de *homebanking*[198] – nomeadamente pagamentos de serviços e compras, consultas de saldos, carregamento de telemóveis, transferências de valores –prendem-se com a possibilidade de utilizar os serviços da instituição bancária a qualquer hora, em qualquer dia, em qualquer lugar, desde que haja acesso à Internet.

Para tanto, é disponibilizado àqueles clientes que pretendem beneficiar deste serviço, não só senhas de acesso pessoais, mas também cartões matriz compostos por milhares de composições numéricas, que não são mais do que canais de autenticação secundário (primeiro autentica-se depois autoriza-se)[199] e que tentam garantir a segurança destes serviços. Este cartão matriz, que deverá ser utilizado para autenticar, no final, a operação, deverá ser apenas do conhecimento do cliente, não devendo em circunstância alguma fornecer nenhum dos dados nele incluídos visto que tanto o protocolo da página bancária como o tráfego de toda informação aí processada são cifrados, tornando quase irrealizável um terceiro obter ou alterar informação após o envio.

Não obstante a fiabilidade do sistema devido ao facto da informação se encontrar encriptada, tudo é falível, até um *site* bancário. A criptografia não afasta a possibilidade de uma página de um banco ser alvo de ataques informáticos que têm vindo, lamentavelmente, a ser comuns por todo o mundo através de "novas" modalidades de atuações ilícitas como o *phishing* e o *pharming* que têm como alvo principal as instituições de crédito. Convém lembrar que a maior parte dos *sites* bancários, bem como sites da Administração Pública utilizam o protocolo HTTPS permitindo, dessa forma, ao utilizador validar a autenticidade do *site*.

A perpetração do crime de burla informática subsume-se nestas técnicas eletrónicas, sendo que o "assalto" a contas por via do serviço de *homebanking* tem vindo a revelar-se preocupante. Qualquer uma das técnicas supra citadas têm como objetivo a aquisição

[198] Serviços de *homebanking* oferecidos pela instituição bancária Montepio: Disponível em https://goo.gl/oTpLX5 (consultado 20 Novembro 2015).

[199] Para se garantir uma maior fiabilidade do sistema do cartão matriz utilizam o telemóvel para enviar o código de autenticação.

fraudulenta de fundos sendo cada vez mais exigível o combate à iliteracia informática, e preocupações acrescidas, principalmente verificar o remetente de *e-mail*, não abrir nem executar ficheiros que não tenham sido solicitados, ter um antivírus atualizado e um *firewall* habilitado.

No caso de ter havido uma intromissão fraudulenta no computador da vítima e consequentemente ter sido retirada determinada quantia da conta da cliente sem a sua autorização, a quem devemos imputar a responsabilidade? Decorre da relação entre cliente e banco deveres recíprocos, de diligência e cuidado, de lealdade, alerta, aviso, advertência e prevenção, de informação e acima de tudo a transparência da contratação de serviços de pagamento. Casos como estes levantam muitas questões. No caso em que a vítima entra diretamente na página que lhe apareceu no ecrã do seu computador como sendo a página do Banco e nela fez as suas certificações e operações usuais – tendo sido direcionada para uma página maliciosa que julgava ser a do Banco – é elemento de *pharming.* A vítima foi «vítima» de um esquema fraudulento! A mesma entrou na página que julgava ser a oficial da instituição bancária, e ao invés, acedeu a uma página clonada, acabando por agir em total insipiência. A vítima ao comunicar imediatamente a ocorrência à instituição bancária recaía sobre a mesma o ónus de provar que a operação foi autorizada pela vítima, ou então que havia agido de forma negligente. Para este efeito – cfr. artigo 796.º, n.º1 do CC[200] –"os riscos da falha do sistema informático utilizado, bem como dos ataques cibernautas ao mesmo, têm de correr por conta da instituição bancária (...)".

Para corroborar e complementar, decorre do artigo 68.º, n.º1, al. a) e 71.º, n.º1 do DL 317/2009, de 30 de Outubro (transpôs a Diretiva 2007/64/CE do Parlamento Europeu e do Conselho de 13 de Novembro), que os " riscos pela utilização normal do sistema correm por conta do Banco (...) " e que "a responsabilidade pelo reembolso das quantias objeto de transferências não autorizadas (...) impende sobre o prestador de serviços". Com isto quererá

[200] ***Artigo 796º do CC- Risco***

1 - Nos contratos que importem a transferência do domínio sobre certa coisa ou que constituam ou transfiram um direito real sobre ela, o perecimento ou deterioração da coisa por causa não imputável ao alienante corre por conta do adquirente.

2 - Se, porém, a coisa tiver continuado em poder do alienante em consequência de termo constituído a seu favor, o risco só se transfere com o vencimento do termo ou a entrega da coisa, sem prejuízo do disposto no artigo 807º.

3 - Quando o contrato estiver dependente de condição resolutiva, o risco do perecimento durante a pendência da condição corre por conta do adquirente, se a coisa lhe tiver sido entregue; quando for suspensiva a condição, o risco corre por conta do alienante durante a pendência da condição.

dizer-se que a falsificação da página *web* da instituição bancária levada a cabo por delinquentes cibernautas não foi imputada nem ao cliente nem à instituição de crédito, portanto transferência eletrónica não autorizada ou ordenada obriga o banco a reembolsar imediatamente o cliente desse montante, repondo a conta na situação em que estaria se essa transferência não autorizada não tivesse tido lugar. Seguimos integralmente a douta decisão jurisprudencial[201] em imputar a responsabilidade ao banco em caso de risco de fraude do sistema de pagamentos ou transferências.

Posto isto, tomamos como certeiro de que o ato levado a cabo pelo delinquente é consubstanciado na prática de um crime de burla informática, porquanto existe um enriquecimento ilegítimo, à revelia da ofendida e sem autorização da mesma, mediante uma subtração do património, com utilização de dados sem autorização e estruturação incorreta de programa informático.

1.6. A fraude com cartão bancário

A fraude com cartões de pagamento é um problema mundial em crescimento, causador de enormes prejuízos financeiros na União Europeia. [202]

Por nos parecer uma temática com especial pertinência, principalmente num universo dominado pelas TIC e pela Internet, concordamos em fazer alusão à fraude de cartão de pagamento, por não só consubstanciar um perigo que tem em vista lucros financeiros, mas também por ser uma ação delituosa propulsionadora na perpetração do crime de burla informática.

O cartão bancário vulgarizou-se em pouco tempo e é elemento caracterizador da atual prática bancária; simples, rápida, desmaterializada. A sua expansão, em Portugal, remonta à década de 50. Consiste num instrumento de pagamento eletrónico de bens e serviços, assumido sob a forma de um cartão de plástico emitido por instituições de crédito ou sociedades financeiras devidamente autorizadas para o efeito. Na prática, os cartões bancários são

[201] Acórdão 6479/09.8TBBRG.G1.S1 de 18 de Dezembro de 2013, disponível em: http://goo.gl/TV0RJS (consultado 20 Novembro 2015).

[202] Expressão retirada do Relatório Geral sobre as Atividades da Europol, de 2010, p. 44.

documentos elaborados com recursos aos meios informáticos, que dispõem de uma banda magnética onde está contida toda a informação relativa ao legítimo titular do cartão, também essa disponibilizada com recurso a meios informáticos e, estes instrumentos ainda vão ser utilizados em equipamentos que se traduzem como verdadeiros computadores, ou que para o seu funcionamento recorrem à informática, como é o caso da ATM e POS[203].

Segundo o Banco de Portugal, "estes instrumentos de pagamento eletrónicos têm vindo a ganhar preponderância" em detrimento de outros métodos, que têm caído em desuso. Essa tendência deve-se à evolução inerente às infraestruturas tecnológicas e pela massificação de dispositivos de aceitação de cartões que permite realizar pagamentos por via eletrónica, designadamente através da oferta de serviços de pagamento através da Internet, ou seja, o *homebanking* que possibilita a gestão das contas bancárias, o acesso a produtos bancários e a realização de pagamentos, a partir de um computador ou de um telemóvel.

No que concerne à tipologia que o cartão bancário pode adotar, "é claro que dentro da categoria dos cartões bancários são abrangidos cartões com funções muito diferentes"[204] e mediante a sua função principal, iremos apenas fazer referência ao cartão de crédito e ao cartão de débito.[205] Por um lado, o cartão de crédito encontra-se associado a uma conta-cartão[206] ou a uma linha de crédito outorgada pela entidade que emitiu o cartão, cujo titular do cartão beneficia de um determinado crédito concedido pela entidade emitente. Por outro lado, o cartão de débito está associado a uma conta de depósito, permitindo o titular realizar operações de levantamento de dinheiro, pagamentos, transferências bancárias, e uma vez utilizado, a conta é debitada pelo

---

[203] "O levantamento de numerário em caixas automáticas, bem como o pagamento eletrónico de bens e serviços são apenas duas das variadíssimas operações que se reconduzem à categoria mais ampla das transferências eletrónicas de fundos, também designadas pela sigla EFT, correspondente à expressão anglo-saxónica *Electronic Fund Transfer*. (..) As operações EFT poderiam ser entendidas, num sentido amplo como «ordens de transferência de fundos dadas por uma pessoa a favor de outra através de meios eletrónicos» " (definição de Hal Scott), disponível em "As transferências eletrónicas de fundos e os cartões de débito*:* alguns problemas jurídicos relacionados com as operações de levantamento", p. 18 e 19.

[204] Guimarães, Maria Raquel. *As transferências eletrónicas de fundos e os cartões de débito: alguns problemas jurídicos relacionados com as operações de levantamento*. Coimbra: Almedina, 1999, p. 62.

[205] Para o efeito cfr. Aviso n.º11/2001 do Banco de Portugal, disponível em https://www.cgd.pt/ajuda/Espaco-Cliente/Informacao-util/Documents/Aviso-BdP-11_2001.pdf (consultado 15 Dezembro 2015).

[206] Segundo informação disponibilizada pelo Banco de Portugal, consiste na conta associada a cada cartão de crédito, existente na entidade emitente e na qual se registam os movimentos associados à utilização do cartão, Disponível em http://www.bportugal.pt/pt-PT/PublicacoeseIntervencoes/Banco/CadernosdoBanco/Biblioteca%20de%20Tumbnails/Cart%C3%B5es%20Banc%C3%A1rios.pdf (consultado 20 Novembro 2015).

valor equivalente. Denote-se que, a tendência é para que cada vez mais os cartões bancários apresentem mais do que uma função, possibilitando assim ao titular do cartão efetuar várias operações com o mesmo instrumento de pagamento.

As transações comerciais são efetuadas com base na estrutura tripartida que os cartões bancários apresentam, concretizando: emissor, titular e comerciante. O comerciante, a fim que se efetue de forma plena as transações comerciais, tem apenas que dispor de um dispositivo leitor de cartão através do qual a operação de pagamento é realizada designadamente de POS[207].

Várias são as operações e vantagens de que o titular da conta pode beneficiar ao adquirir um cartão bancário. A entidade emissora do cartão permite aos seus clientes facilitismo, uma vez que o meio de pagamento é muito mais cómodo, o que contribuiu significativamente para o aumento das vendas, isto porque o titular não tem necessidade de transportar consigo dinheiro físico, nem quando se desloca ao estrangeiro. Há a possibilidade de realizar vendas à distância, de forma quase sempre segura e diligente, porquanto é aconselhável uma maior prudência por parte do titular do cartão. Ainda, os comerciantes cobram o valor das vendas com toda a rapidez e segurança, ou seja, tem a certeza de efetuar a cobrança efetiva e por maioria de razão prefere este meio de pagamento, evitando assim roubos e furtos.

As operações bancárias, como alude Maria Raquel Guimarães[208], são classificadas como operações de transferências eletrónicas de fundos e uma gama de opções de operações bancárias passou a ser oferecido aquando a instalação do Multibanco. Afinal, os cartões bancários não passam de documentos produzidos por via de meios informáticos, dispondo de uma banda magnética constante de informação colocada por recurso de meios informáticos e que vão ser utilizados em equipamentos que são *per si* computadores, que para o seu funcionamento recorrem à tecnologia informática, como é o caso da ATM ou do POS.

[207] Corrobora Maria Raquel Guimarães dizendo que " (...) o procedimento POS distingue-se dos movimentos levados a cabo através da ATM na medida em que pressupõe uma relação triangular, da qual são partes um banco, um utilizador dos sistema e um comerciante" *in* "As transferências eletrónicas de fundos e os cartões de débito*:* alguns problemas jurídicos relacionados com as operações de levantamento", p. 50.

[208] Guimarães, Maria Raquel. "A repartição dos prejuízos decorrentes de operações fraudulentas de banca electrónica (home banking): anotação ao Acórdão do Tribunal da Relação de Guimarães de 23.10.2012, Proc. 305/09". In *Cadernos de Direito Privado*, nº41, pp.45-69, 2013.

O recurso às operações bancárias pressupõe assim a aplicação de meios informáticos a fim de concretizar as mesmas, abrindo portas a crimes de índole "económica-informática", isto porque, são colocadas à disposição do titular do cartão várias possibilidades de transacionar fundos monetários, seja através de um computador, utilização física do cartão, numa ATM ou através de POS. A propósito dos crimes informáticos, remetemos para o Capítulo I, mas acrescente-se que a informática está cada vez mais próxima da banca.

A fraude aqui retratada é entendida como uma expressão que abrange todas as atuações do agente e cuja consumação lesa um bem jurídico, com recurso ao computador que assume um papel central. A fraude é portanto entendida como uma ação fraudulenta, com dolo da parte de um terceiro, cujo desiderato é retirar algum proveito do instrumento de pagamento. Atestamos assim uma subtração do património pelo ato de defraudar e espoliar, cujos agentes criminosos utilizam para o efeito estratagemas que encobertam a execução de um crime, tornando-a mais grave, por ser mais insidiosa.

Antes de abordar o tema em pleno, é preciso ter em consideração duas distinções de operações. Por um lado, o *Card Present* (CP), cujo agente recorre à presença física do cartão bancário para consumir a fraude, por outro, no *Card-not-Present* (CNP) não recorre à presença física do cartão bancário, mas à utilização dos dados, comummente para compras através da Internet e do telefone. A fraude CNP julgamos nós ser a mais investigada, pelo facto de ser a mais fácil de realizar. Neste caso basta que sejam utilizados dados que constam no cartão físico, o que quer dizer que qualquer pessoa com acesso ao mesmo o possa utilizar, sendo ou não o legítimo titular.

Na fraude com cartão bancário assiste-se a uma multiplicidade no que respeita à qualificação do tipo de crimes, não existindo uma harmonização relativamente à recondução da conduta criminosa a um tipo de crime.[209] Não obstante, os exemplos que iremos de seguida relatar conduzem-nos, muitas vezes não diretamente, a várias formas de manifestação do tipo legal de crime de burla informática. Posto isto, e a fim de ilustrar os diversos exemplos respeitantes à fraude com cartão bancário que indicia a prática do crime de burla informática

[209] É do nosso entendimento que a atribuição da qualificação jurídica deste tipo de criminalidade encontra-se em grande parte das vezes dependente do conhecimento e sensibilidade jurídica por parte dos magistrados, no que respeita à aplicação da Lei da Cibercriminalidade.

iremos proceder a uma devida explanação acerca da utilização ilegítima de cartão bancário autêntico. Este fenómeno verifica-se na maior parte da jurisprudência nacional e configura-se quando um terceiro utiliza e apropria-se de um cartão bancário, sem consentimento do legítimo titular e o utiliza de forma abusiva. Existe uma apropriação ilegítima de cartão bancário com vista a retirar algum proveito económico, o que nos reconduz imediatamente para o crime de burla informática. Estas situações são, incontestavelmente, praticadas de forma regular – caso mais recorrente de burla Informática na jurisprudência nacional – e, para além do roubo ou furto do cartão, o cenário mais corriqueiro é de aquele terceiro, que aproveitando-se da especial relação de proximidade do titular do cartão, o utiliza em seu proveito próprio. Geralmente trata-se de filhos ou contexto familiar, amigos, empregadas domésticas ou senhoras que têm a seu cargo idosos, que aproveitando-se da sua especial vulnerabilidade, utilizam o cartão sem que estes o saibam. No âmbito investigatório, geralmente estes processos caem por terra.

Para a efetiva consumação do crime é necessária a obtenção do código PIN que consiste na visualização do mesmo quando o legitimo titular o utiliza para realizar levantamentos de numerário ou operação de pagamento. No entanto, existem situações em que o terceiro obtém o código PIN através da sua visualização quando este se encontra manuscrito no cartão ou junto deste ou de forma que seja identificável.

1.7. Fraude no comércio eletrónico

Nos últimos tempos, a Internet passou de um estado de mera curiosidade académica para um meio marcante e essencial de comunicação para empresas e particulares. Para as empresas tem-se revelado uma necessidade e uma ferramenta estratégica, para os particulares um método alternativo de aquisição de bens e serviços.

Nos dias que correm a experiência tem revelado que o comércio eletrónico (*e-commerce*) é o meio eleito na aquisição de bens e serviços que se encontra permanentemente em crescimento. Neste contexto a troca de bens e serviços encontra-se desmaterializada, originando uma "desinstitucionalização dos tradicionais meios de pagamento"[210]. Desta forma

[210] Rocha, Maria Vitória. "Novos Meios de Pagamento no Comércio Eletrónico (e-commerce)".In *Direito da Sociedade da Informação – Vol. V*, Associação Portuguesa do Direito Intelectual. Coimbra Editora, 2004, p. 204.

consideramos que o comércio eletrónico constitui um dos "pilares basilares da sociedade da informação, mas também num indutor de profunda transformação ao nível das práticas comerciais tradicionais"[211].

Talvez devido à comodidade associada aquando a compra do produto ou serviço, à possibilidade de efetuar a operação a qualquer hora do dia através do computador ou outros dispositivos móveis desde que ligados à Internet e proporciona ao cliente uma maior pesquisa comparativa, possibilitando desta forma novas oportunidades de negócio. Por comércio eletrónico podemos entender como "todas as formas de transações comerciais que envolvam, quer organizações, quer indivíduos e que são baseadas no processamento e transmissão de dados por via eletrónica, incluindo texto, som e imagens"[212]. O comércio eletrónico permite satisfazer potenciais negócios entre empresas e consumidores (B2C) ou entre empresas (B2B) através da Internet enquanto "plataforma de troca de informações, encomenda e realização de transações financeiras"[213].

O que também se tem tornado manifestamente evidente, é o aumento de fraudes associadas ao e-commerce sendo que "um dos aspetos que tem entravado o crescimento mais acelerado deste tipo de comércio é a falta de confiança por parte dos clientes na segurança do sistema quantos aos meios de pagamento"[214]. Em fraudes desta natureza terá que se ter em linha de conta a relação tripartida entre o cliente, o comerciante e o sistema bancário, mas a transação só será consumada eficazmente e legitimamente "após a introdução dos mecanismos necessários ao estabelecimento da confiança entre comerciante e cliente", nomeadamente ao nível da segurança e pagamento. Ainda, "os consumidores que participam no comércio eletrónico devem beneficiar de uma proteção transparente e eficiente de um nível pelo menos equivalente ao da proteção assegurada em outras formas de comércio".[215]

---

[211] Jesus Almeida, Maria teresa de." A tributação do Comércio Eletrónico on-line". Dissertação de Mestrado, Instituto Superior de Contabilidade e Administração da Universidade de Aveiro, 2010, p.66.

[212] Cfr. Documento Orientador de Iniciativa Nacional para o Comércio Eletrónico *in* Resolução do Conselho de Ministros n.º94/99, de 25 de Agosto, disponível em https://dre.pt/application/dir/pdf1sdip/1999/08/198B00/57535762.pdf (consultado 27 Dezembro).

[213] Pereira, Joel Timóteo Ramos. *Direito da Internet e Comércio Eletrónico*. Lisboa: *Quid Juris* Sociedade Editora, 2001, p. 475.

[214] Ibidem, p. 203.

[215] *In* Recomendação do Conselho relativa às linhas diretrizes que regem a proteção dos consumidores no contexto do comércio eletrónico da OCDE, disponível em http://www.oecd.org/sti/consumer/34023696.pdf (consultado 5 Dezembro 2015).

O utilizador poderá sofrer uma utilização abusiva dos dados do cartão por um terceiro e deparar-se-á com a dificuldade de reagir perante situações de incumprimento ou de cumprimento defeituoso. Convém relembrar que, para efetuar uma operação através de comércio eletrónico deverá indicar o número do cartão, indicar a data de validade do cartão e indicar o código de verificação de segurança. Ao expor as suas informações bancárias na rede, já *per si*, constitui vulnerabilidade suficiente para cibercriminosos roubarem os dados. O principal motivo que obsta à compra de bens e serviços na Internet, que afeta não só os consumidores individuais como também as empresas, é o medo de ser enganado na hora de comprar através da Internet.

As condutas fraudulentas mais óbvias em sede de comércio eletrónico traduz-se na entrega do bem e/ou serviço-por parte do vendedor – ou na ausência de pagamento – por parte do comprador. Do ponto de vista do adquirente, a maioria dos meios fraudulentos, baseiam-se na ausência de pagamento e na suplantação de personalidade do comprador real, gerando, desta maneira, encargos para o mesmo ou para terceiro alheio à operação.

Segundo o Centro Europeu do Consumidor[216], o caso mais recorrente em sede de fraude de comércio eletrónico é a venda fictícia de um veículo. Geralmente, este tipo de fraudes (bem como tantas outras) têm uma taxa de sucesso elevada devido à sua aparência genuína e aos estímulos psicológicos que os vigaristas exercem sobre a potencial vítima. Neste caso, o veículo é anunciado de forma atraente, a um preço competitivo e abaixo do mercado. O potencial comprador ao deparar-se com tal anúncio aliciante contacta o suposto vendedor e, na grande esmagadora dos casos, é-lhe comunicado que o veículo encontra-se no estrangeiro, nomeadamente no Reino Unido. Em circunstâncias deste tipo poderá haver casos em que o vigarista pede ao potencial comprador um pré-pagamento de uma determinada quantia para "reservar" o veículo, desaparecendo após transferência dos fundos; ou após pedir o pré-pagamento e verificação da receção da transferência, o vigarista leva o caso mais ao extremo, informando a vítima que o veículo encontra-se a caminho de Portugal e que é necessário o pagamento de mais uma nova quantia, desta vez, a título de seguro; a fase seguinte respeita a supostos problemas alfandegários, de que o veículo ficou retido e que para ter acesso a ele é

[216] Disponível em http://cec.consumidor.pt/topicos1/comercio-eletronico/compras-na-internet/fraudes.aspx (consultado 5 Dezembro 2015).

necessário o pagamento de mais uma quantia. Paralelamente vão enviando *e-mails* falsos aos potenciais compradores para dar mais credibilidade ao esquema fraudulento.

Em jeito de conclusão, o cartão de crédito é o meio de excelência na aquisição de bens e serviços na Internet. O cartão de crédito permite ao utilizador uma ampla margem de manobra. Uma delas é fazer compras *online* através deste meio de pagamento, sendo só preciso usar o número do cartão, a validade, o código de segurança e inserir o montante correto da operação. Outra é a possibilidade de "sempre que haja utilização fraudulenta de um cartão de crédito ou de débito por outrem, o consumidor pode solicitar a anulação do pagamento efetuado e a consequente restituição dos montantes debitados para pagamento".[217] Deste modo, é necessário a existência de um controlo dos serviços.

Normalmente a fraude no comércio eletrónico traduz-se em fraudes na entrega da coisa por parte do vendedor ou no pagamento do preço por parte do comprador. Em bom rigor, existem muitos casos como o descrito em cima, como veremos mais adiante, nos tribunais portugueses cuja procedência cai normalmente por terra.

1.8. Casos recorrentes na jurisprudência nacional e dificuldades no plano de investigação e cooperação internacional

Em sede de análise documental, não podemos deixar de sublinhar que dos mais variados processos a que tivemos acesso os modos de execução são quase sempre os mesmos. É nossa convicção de que os processos que dão entrada nos tribunais não representam nem tão pouco a realidade sócio criminal.

Obtivemos acesso a dados do Tribunal São João Novo e do Tribunal Judicial de Oliveira de Azeméis. No primeiro, dos processos ora analisados, verificamos que os *modus operandis* são em tudo semelhantes ou iguais. Casos em que o agente ao apoderar-se ilicitamente do cartão bancário de outrem, o utiliza em diversos levantamentos da conta do respetivo titular e/ou no pagamento de compras, aproveitando o facto de se encontrar um papel no qual estava escrito o correspondente código de acesso e/ou obrigando a vítima a revelar-se os respetivos

[217] Cfr.Artigo 18.°, n.°2 do Decreto-Lei n.° 24/2014 de 14 de fevereiro, que transpõe a Diretiva 2011/83/UE do Parlamento Europeu e do Conselho, de 25 de outubro de 2011, relativa aos direitos dos consumidores.

códigos de acesso. As ações analisadas integram uma das condutas típicas do crime de burla informática, o de aproveitamento de dados sem autorização.

Em termos globais, quanto aos dados recolhidos durante o hiato temporal compreendido entre 01-01-2014 e 15-06-2015 as conclusões são as seguintes: na comarca de Aveiro, concluímos que em sede de Inquérito, a experiência revelou: 389 processos arquivados, dos quais 150 por desistência de queixa, outros – artigo 277.º, n.º1 – 72 e pelo artigo 277.º, n.º2 – 166, pendentes 279 e apenas 6 acusados – singular; no Tribunal de Oliveira de Azeméis, em sede de Inquérito, a experiência revelou os seguintes números: 29 processos arquivados, dos quais 18 por desistência de queixa, outros – artigo 277.º, n.º1 – 1 e pelo artigo 277.º, n.º2 – 10, outros motivos por incorporações verificou – se 2, 20 pendentes e apenas 1 acusado.

Como se pode apurar, a quantidade de processos arquivados é massiva em relação aos processos a que deduzem acusação.

No Tribunal de Oliveira de Azeméis apenas analisamos apenas aqueles cuja duração de processo é maior, por nos afigurar mais marcante para a pesquisa. Analisamos um processo de furto de cartão bancário para proveito próprio; um onde acederam ilegitimamente à conta bancária retirando determinado montante e um processo complexo de um técnico oficial de conta que desviou verbas depositando em conta sua.

Em sede de análise documental, deparamo-nos com um processo de um caso de um indivíduo português que, através de um anúncio de venda de automóveis, procedeu à suposta compra e venda de um automóvel, sendo que o mesmo pagou o respetivo preço indicado e após a transferência não obteve mais nenhuma notícia por parte do alegado vendedor. Apresentou queixa e o processo acabou por se tornar improcedente. Face aos factos expostos no auto de notícia é nosso entendimento que culminou com um erro de qualificação jurídica. Perspetivamos que o caso supra exposto não preenche os requisitos do crime de burla informática, como consta no processo, é ao invés, um crime de burla praticada através da Internet, por não preencher as condutas típicas previstas e punidas no artigo 221.º CP. Posto isto, humildemente concluímos a insensibilidade dos magistrados face a crimes de índole informática.

No plano de investigação, em casos de burla informática ou burlas cometidas através da Internet, a Polícia Judiciária pouco ou nada consegue apurar porquanto estes tipos de burlas

provêm dos mais diversos países[218]. Salienta Pedro Verdelho que "(...) os crimes praticados no ambiente digital têm suscitado problemas resultantes da imaterialidade (...) a localização física dos agentes não é óbvia (...) (in)determinação de jurisdição"[219]. Decorre da *praxis* que a cooperação das autoridades estrangeiras (como é o caso de Reino Unido, Rússia, Roménia, Nigéria, Turquia, Benim, Senegal, Camarões, Tailândia, EUA) adquirida em casos de burlas cometidas através da Internet ou burlas informáticas é nula ou ineficaz.

A solicitação de elementos carece da elaboração de um pedido onde seja especificado a razão do pedido, o fornecimento de informação sobre a natureza da investigação, a especificação de como e em que medida o acesso aos dados solicitados fará progredir a investigação, a indicação da data, hora e local exatos da investigação, a identificação completa dos indivíduos envolvidos nos factos e o papel que desempenharam nesses mesmos factos, o motivo porque é necessário obter essa informação e o que se pensa conseguir com a mesma, a indicação dos motivos porque os objetivos da investigação não podem ser atingidos por outros meios, tendo ainda que ser tido em consideração a possibilidade de invasão da privacidade de terceiros e delinear um plano para minimização desses risco. Para além de se tratar, na maioria de queixas contra desconhecidos, as cartas rogatórias enviadas a fim de solicitar elementos que auxiliem a investigação ou até que são decisivas para a mesma, para além de demorarem muito tempo a responder (variando de 1 a 2 anos) ou se negarem a solicitar elementos não se obteria com toda a certeza a identificação dos autores do crime, sendo inteiramente improdutivo porque as identificações fornecidas pelos destinatários são falsas, tudo isto tendo em conta os

---

[218] " Geralmente, os agentes do crime integram uma rede especializada que cria e/ou simula *e-mails* como forma de dar maior credibilidade e simultaneamente levar a que sejam enviadas as quantias supostamente destinadas ao pagamento das despesas do suposto amigo (autor do email), mostrando-se, na maior parte dos casos, praticamente impossível a identificação da proveniência das comunicações fraudulentas em virtude do remetente de um *e-mail* ser facilmente forjável e de atualmente ser possível mascarar os endereços de IP e subsequentemente os provedores de serviços de internet (ISP) utilizando redes de túneis virtuais (*tunnelling*). *Tunneling* ou VPN permite ligar dois quaisquer pontos na Internet através de uma rede virtual. Esta rede não existe propriamente e assenta sobre a rede física que se tem implementada na Internet. A sua principal vantagem é que ela ignora todos os pontos intermédio por onde passa, o que impede que a informação dos pacotes que passam na rede física seja extraída e usada, uma vez que é praticamente impossível determinar a origem e o destino, visto que o túnel é definido diretamente entre esses dois pontos. É usada, principalmente, para dificultar encontrarem qual o IP de origem – nomeadamente em situações em que se pretenda não mostrar o endereço – para criar camadas adicionais de segurança (visto que os túneis podem ter uma camada de segurança com autenticação, por exemplo) ou para fazer *bypass* a certas limitações que uma rede imponha, como por exemplo, firewall ou portos bloqueados", excerto retirado de relatório da PJ do Porto.

[219] Verdelho, Pedro. " Phishing e outras formas de defraudação nas redes de comunicação". In *Direito da Sociedade da Informação – Vol. VIII,* Associação Portuguesa do Direito Intelectual. Coimbra Editora, 2009, p. 418.

resultados que se têm obtido em sede de inquérito em casos semelhantes. [220] Segundo Pedro Verdelho "a ação dos investigadores esbarra com fronteiras políticas nacionais que os impedem de intimar operadores de telecomunicações e fornecedores de serviço Internet estrangeiros a colaborarem com a investigação e que os proíbe de lhes solicitarem diretamente dados e informações de que disponham"[221]

Efetivamente o *iter criminis* de uma burla informática resulta de um processo complexo e elaborado que requer cooperações de vários ordenamentos jurídicos bem como de grandes perícias. É sabido que muitos processos de burlas informáticas, devido à extrema dificuldade de descoberta de fraude por parte da PJ – por exigirem perícias tecnologicamente rigorosas – e por implicar outros ordenamentos jurídicos, não têm procedência criminal ou implica, na esmagadora das vezes, desistência do processo.

Pelo que fora exposto, é percetível e manifesta a insuficiência e escassez de meios e mecanismos que a Policia Judiciária tem ao seu dispor.

No plano de política criminal, temos a Lei-quadro da Política Criminal n.º17/2006, de 23 de Maio alterada pela Lei n.º38/2009 de 20 de Julho, que tem como objetivo "prevenir, reprimir e reduzir a criminalidade, promovendo a defesa de bens jurídicos, a proteção das vítimas e a reintegração dos agentes do crime na sociedade". A Lei de política criminal estabelece e elenca crimes de carácter prioritário, ou seja, crimes de prevenção prioritária e crimes de investigação prioritária como decorre dos artigos 3.º e 4.º respetivamente. No que respeita a crimes de investigação prioritária o legislador deveria de ter sido mais cauteloso, porque o leque de crimes é demasiado extenso, tornando tudo prioritário, o que poderá dificultar ou inviabilizar a eleição de área de focalização de atuação. Como decorre do artigo 4.º, n.º1, alínea b), o crime de burla informática é considerado um crime de investigação prioritária "tendo em conta a gravidade dos crimes e a necessidade de evitar a sua prática futura". Ainda que seja de investigação prioritária, o facto é o de que não conseguem dar resposta, também devido à insuficiente cooperação internacional pondo assim em causa a eficácia do exercício da ação penal.

---

[220] Nem mesmo os ISP respondem a pedidos de dados efetuados pela Polícia Judiciária, nem as autoridades locais da maior parte dos países referenciados neste tipo de fraudes respondem a pedidos policiais diretos, só o fazendo em casos graves.

[221] Verdelho, Pedro. " Phishing e outras formas de defraudação nas redes de comunicação". In *Direito da Sociedade da Informação – Vol. VIII,* Associação Portuguesa do Direito Intelectual. Coimbra Editora, 2009, p. 418 e 419.

No plano de investigação tudo se torna mais abstruso. Sob o ponto de vista investigatório, devido à sua natureza semipública[222], depende de queixa, levando a que na esmagadora maioria dos casos, haja desistência do procedimento criminal por envolverem relações de grande proximidade entre os intervenientes.[223]

Em matéria de cooperação internacional e judiciária, todos os países têm o dever de cooperar e prestar amparo no que respeita a matéria judiciária e policial, sempre que se justifique. A desadequação do direito é indiscutível e como atesta Joel Timóteo Ramos Pereira, Portugal bem como a generalidade dos países "não se têm adaptado à internacionalização das redes informáticas" bem como "as normas substantivas (...) não se coadunam com o caráter transfronteiriço e virtual dos atos praticados na Internet".[224] Os progressos tecnológicos têm impedido que as autoridades façam um acompanhamento eficaz e em tempo "real", o que também prejudica a obtenção de provas destes comportamentos ilícitos. Para tentar, de certo modo, suprir estas falhas surgiu em 2013 o Centro Europeu da Cibercriminalidade cujo desiderato é o do reforço e melhoramento da capacidade da União Europeia na luta contra a cibercriminalidade, de modo a garantir uma mudança significativa e viabilizar uma Internet livre, aberta e mais segura.

Para finalizar, acima de tudo é necessário fomentar a cooperação das várias entidades seja a nível nacional como internacional, com responsabilidades na área criminal, especialmente em matéria de crimes económico-financeiros, que permita uma eficaz investigação dos crimes, conservação de material probatório, captura dos criminosos e seu efetivo sancionamento. A nível interno existe uma evidente desadequação do Direito e dos processos penais e acrescenta Joel Timóteo Ramos que "o formalismo do processo penal não se tem adaptado à internacionalização das redes informáticas das transferências de dados de fundos ilícitos"[225].

À facilidade técnica junta-se a provável impunidade dos agentes do crime, porque os tribunais têm dificuldade em impor as suas decisões noutros ordenamentos jurídicos. A recolha de provas digitais é de difícil obtenção, pois é comum a alteração e eliminação do rasto dos

[222] A apresentação da queixa recai à pessoa prejudicada e não ao proprietário ou utente dos dados ou programas informáticos.

[223] No que respeita à utilização indevida de cartão autêntico confrontado com a utilização por um filho, por exemplo, não se manifesta por parte do progenitor vontade em prosseguir criminalmente.

[224] Pereira, Joel Timóteo Ramos. *Direito da Internet e Comércio Eletrónico*. Lisboa: *Quid Juris* Sociedade Editora, 2001, p. 240.

[225] Idem.

crimes informáticos e para além disso as provas digitais podem ser de tal forma volumosas o que afeta a investigação pois os investigadores terão de despender muito tempo, muitos recursos de computação, no espaço de armazenamento e na análise das mesmas e na recolha de elementos determinantes para resolução do caso. Do mesmo modo que admitimos a dificuldade em obter condenações porque se trata de panóplia de crime cuja natureza exige uma polícia que atue quase em tempo real.[226]

É uma problemática a ser dizimada ao nível internacional, devido fundamentalmente ao apoio, cooperação e apoio das autoridades de todos os países envolvidos, mas realçamos para o facto de os nossos OPC necessitarem de uma «reeducação» em matéria de cibercrime e de investigação, recolha e preservação da prova digital, porque na realidade é fundamental que os investigadores tenham à sua disposição todos os mecanismos, recursos e ferramentas que necessitarem para fazerem face à permanente evolução da tecnologia. O direito será sempre obsoleto em relação à tecnologia.

Reiterando o que já fora dito, não só para magistrados mas como também outros atores processuais alguns conhecimentos profundos para a melhor aplicação do direito, preparando melhor os tribunais para novos modos de execução do crime que vão surgindo rapidamente com a tecnologia, para combater a cibercriminalidade e servir de melhor modo a justiça Portuguesa.

[226] Verdelho, Pedro. " Cibercrime". In *Direito da Sociedade da Informação – Vol. IV,* Associação Portuguesa do Direito Intelectual. Coimbra Editora, 2003.

CONCLUSÃO

O progresso pertinaz nas tecnologias de informação e na Internet tiveram e continuam a ter um impacto assinalável na sociedade. Nos dias de hoje, é raro o sector da sociedade que não está compreendido por estas, tendo vindo a conceder metamorfismos nas atividades desenvolvidas pelo Homem. Estes progressos nas tecnologias da informação não desencadearam consigo apenas aspetos positivos, permitiram também que surgissem aspetos negativos associados a estas evoluções. Houve o aparecimento de novas tipologias de crime, agora associadas às novas tecnologias, como é o caso do tipo legal de crime de burla informática previsto e punido pelo artigo 221.º CP. A este propósito atesta Anabela Miranda Rodrigues que "o crime é um dos sintomas da emergência desta sociedade global e que, ao mesmo tempo, permite compreender a sua evolução: não só do ponto de vista das ameaças que a espreitam, mas também porque o crime se adapta às novas formas de socialização."[227]

Concluímos que a burla informática é um fenómeno criminoso que tem tido maior magnitude e relevância, nos últimos anos, no âmbito da criminalidade informática, sendo este a base principal do crime informático. Os números de burlas informáticas têm superado o prejuízo patrimonial das burlas cometidas pelas vias tradicionais e são um reflexo da alucinante evolução tecnológica e do fator socioeconómico, isto porque, tudo o que motiva à perpetração de crimes desta índole é a vontade do lucro. E como é o dinheiro que move o mundo, e mediante a gravidade destes crimes que se tem evidenciado a cada ano que passa, fez-se sentir a necessidade de proceder a esta investigação.

Temos, porém, uma apreciação crítica. A moldura penal prevista para o tipo legal de burla tradicional (artigo 217.º CP) e burla informática (artigo 221.º CP) é a mesma, prevê-se pena de prisão até 3 anos ou com pena de multa. É nossa opinião que, no crime de burla informática, o tipo de valor subjacente carece de uma proteção muito mais alargada, pois para além da proteção do património estão subjacentes valores na ordem da proteção dos sistemas informáticos. É certo que em ambos os tipos legais existe uma subtração de património, no entanto, não esqueçamos que para o efeito o modo de execução do crime é diferente, mais perverso e insidioso no segundo caso. O legislador ao fixar molduras penais iguais está a censurar comportamentos, que na sua génese são diferentes, e em nada se preocupou na

[227] Rodrigues, Anabela Miranda. *O Direito Penal Europeu Emergente*. Coimbra Editora, 2008, p. 170.

proteção das novas tecnologias e sistemas informáticos. Outro aspeto que se destaca é o número superior de perpetração do crime de burla informática, em relação ao crime de burla tradicional. É necessária uma tutela penal acrescida nos casos de burla informática, devido aos números que se têm vindo a registar bem como o reconhecimento de uma medida preventiva, a fim de, no futuro, com a agravação da moldura penal, não recrudescer a criminalidade em matéria de burla informática. Existem autores que admitem que a burla informática é estruturalmente uma burla, do qual discordamos pelos motivos supra expostos. Posto isto, o legislador deveria de ter a preocupação de classificar o crime de "burla informática" autonomamente, dando para o efeito, uma designação diferente, isto porque quando pensamos em burla informática somos remetidos para a burla tradicional.

Numa humilde análise em matéria de Direito comparado, perspetivamos que existe uma harmonização de *ratio legis* relativamente ao crime de burla informática. Pese embora a previsão de definições gerais no caso de Espanha e Itália e de uma enumeração exaustiva no caso de Portugal e Alemanha, chegamos à conclusão que os limites da proximidade do crime de burla informática e burla tradicional não diferem muito. Existe convicção, e isso é unânime, de que ao invés de pressupor um engano da pessoa, como sucede na burla tradicional, não se pode enganar um computador. Os elementos típicos, independentemente da sua extensão, são análogos entre si.

Numa perspetiva mais pautada pela informática, as burlas informáticas manifestam-se através de uma conjunto de aptidões e práticas informáticas, cada vez mais aprimoradas e persistentes. Isto é, "têm sido desenvolvidas (...) formas de enganar incautos por via da Internet (...) provocando grandes perdas económicas às vítimas"[228] . O universo da informática tem sofrido constantes mudanças a uma velocidade frenética, e portanto, é necessário impor-se a tutela de determinados bens como a segurança jurídica nas relações entre indivíduos. As burlas sempre existiram. Porém, assumem, neste contexto, mecanismos diferentes aos utilizados pela via tradicional. No nosso entendimento, traduz-se numa preocupação emergente na ótica do utilizador de uma comunidade informatizada, devido ao comprometimento da sua privacidade e confidencialidade dos dados. Não menosprezando os restantes, é nossa convicção que o

[228] Verdelho, Pedro. " Phishing e outras formas de defraudação nas redes de comunicação". In *Direito da Sociedade da Informação – Vol. VIII,* Associação Portuguesa do Direito Intelectual. Coimbra Editora, 2009, p. 416.

phishing e *pharming* são os ataques mais frequentes. Existe muita tendência em confundir estas duas técnicas, mas não esqueçamos que são diferentes. Também existe a falsa impressão que o *phishing* só é utilizado para perpetração de crimes de burla informática, através do envio de correio eletrónico. Temos que desmistificar isso, pois o *phishing* pode ser utilizado para instalar vírus ou mesmo para comprometer o *router* local de casa. Tipicamente, contacta através do envio de *e-mails* a um número indiscriminado e significativo de utilizadores tentando, de forma mais ou menos convincente, persuadir os utilizadores a morder o isco.

Através do emprego de técnicas de *pharming* os agentes criminosos conseguem dissimular páginas institucionais de entidade bancárias, colocando em causa todo o serviço de *homebanking*. Ainda, através da dissimulação de equipamentos é possível defraudar o cartão bancário e obter vantagens patrimoniais.

Pedro Verdelho sublinha a inconsciência de Portugal na dimensão do cibercrime.[229] Subscrevemos esta opinião, tanto o cidadão comum como o magistrado não tem a verdadeira noção dos prejuízos que o computador pode conceber. A iliteracia informática é uma das causas geradoras de vulnerabilidades informáticas.

Pretendeu-se com este trabalho de investigação consciencializar não só os juristas, mas o utilizador comum a prevenir-se, a detetar e mitigar eventuais ciberataques que visam acima de tudo, arranjar formas de enganar um utilizador no que respeita a submissão de informação.

No que respeita à análise documental, pese embora o facto de os *modus operandi* deverem ser meticulosamente e individualmente estudados, nos casos observados o *modus operandi* praticado é essencialmente sempre o mesmo, o da utilização de dados sem a devida autorização. Dever-se-á ter em linha de conta a plasticidade dos comportamentos criminais consoante a realidade criminológica. Melhor dizendo, tem-se verificado de um modo geral, uma evolução de *modus operandi*, ou seja, há alguns anos o crime de burla informática centrava-se em levantamentos em caixas automáticas ou pagamento em POS com utilização indevida dos códigos dos cartões. Nos dias de hoje, centra-se essencialmente em transferências monetárias através da Internet, nomeadamente, no acesso indevido a serviços de *homebanking*.

[229] Verdelho, Pedro. " Cibercrime". In *Direito da Sociedade da Informação – Vol. IV,* Associação Portuguesa do Direito Intelectual. Coimbra Editora, 2003, p. 351.

Neste panorama, é manifesto que os sistemas penais, quando individualmente considerados não conseguem dar resposta eficaz à emergente criminalidade. É inconcebível considerar as incólumes fronteiras jurídicas entre os Estados, quando os crimes (designadamente o crime de burla informática) se praticam sem qualquer fronteira. São necessários mais e melhores meios de combate aos crimes de burla informática.

A escassez de conhecimento dos juristas e dos próprios magistrados das mais diversas técnicas existentes torna-se um vazio por preencher. Em bom rigor, o Direito em circunstância alguma irá estar situação de paridade com a evolução tecnológica. Nem mesmo os especialistas da segurança informática conseguem ter ócio na matéria. Há seguramente uma pressão sobre a investigação criminal e a legislação estará sempre a tentar adaptar-se a um ritmo sem precedentes a esta nova realidade.

É nossa asseveração e desejo que este estudo tenha rematado algumas lacunas e ajudado, de alguma forma, no combate do crime de burla informática.

Porém, não esqueçamos que as burlas informáticas irão continuar a subsistir, bem como novos métodos e ferramentas irão aparecer e que entabulará uma guerra sem precedentes.

REFERÊNCIAS BIBLIOGRÁFICAS

Aas, Katja Franko. *Globalization and crime*. 2.ª edição. SAGE Publications Limited, 2013.

Albuquerque, Paulo P. de. *Comentário do Código Penal.* 3.ª edição Lisboa: Universidade Católica Editora, 2015.

Almeida Costa. *Comentário Conimbricense*, II. Coimbra: Coimbra Editora, 2010.

Andrade, Miguel Almeida. *Nomes de Domínio na Internet: a regulamentação dos nomes de domínio sob.pt*. 1.ª edição. Lisboa: Centro Atlântico, Lda., 2004.

Amato, Astolfo di. *Codice di Diritto Penale delle Imprese e della Società: annotato com la giurisprudenza*. 1.ª edição. Giuffrè Editore, 2001.

Antunes, José A. Engrácia. *Direito dos Contratos Comerciais.* Coimbra: Edições Almedina, 2009.

Ascensão, José de Oliveira. *Estudos sobre o Direito da Internet e da Sociedade de Informação*. Almedina, 2001.

Ascensão, José de Oliveira. "Sociedade da Informação". In *Direito da Sociedade da Informação – Vol. I*, Associação Portuguesa do Direito Intelectual. Coimbra Editora, 1999.

Bajo, Jaime Barbero. "Phishing y otros delitos informáticos: el uso ilícito de Internet." *Lex nova: La revista* 53 (2008): 6-10. http://www.lexnova.es/pub_ln/revistas/revista_ln/Revista53/Revista53.htm.

Berghel, Hal. "Phishing mongers and posers." *Communications of the ACM* 49.4 (2006): 21. http://ww.berghel.net/col-edit/digital_village/apr-06/dv_4-06.pdf.

Bernal, Javier Sánchez. "El bien jurídico protegido en el delito de estafa informática." *Cuadernos del Tomás* 1 (2009): 105-121.

Bride, Mac. *Iniciação à criação de páginas na Web em HTML*. Publicações Europa América, Lda. 1997.

Brody, Richard G., Elizabeth Mulig, and Valerie Kimball. "Phishing, pharming and identity theft." *Academy of Accounting and Financial Studies Journal* 11.3 (2007): 43-56. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.97.6078&rep=rep1&type=pdf.

Cabana, Patricia Faraldo. "Los conceptos de manipulación informática y artificio semejante en el delito de estafa informática." *Eguzkilore: Cuaderno del Instituto Vasco de Criminología* 21 (2007): 33-57. http://www.ehu.eus/documents/1736829/2176629/02+Faraldo.indd.pdf.

Campanelli, Giuseppe. *La giurisprudenza della Corte di Cassazione in tem di "truffa informatica"*. Diritto e società dell' informazione. Milão: Nyberg Edizioni, 2004. https://books.google.pt/books?id=2WT_UclXrBsC&pg=PA27&dq=art.+10+della+l.547/93&hl=pt-PT&source=gbs_toc_r&cad=4#v=onepage&q=frode&f=false.

Campos, Luís de. *Dicionário de computadores*. 2.ª edição revista e atualizada. Lisboa: Editorial Presença, 1995.

Capanema, Walter Aranha. *O spam e as pragas digitais : uma visão jurídico-tecnológica*. São Paulo : LTr, 2009.

Castells, Manuel. *A Era da Informação: Economia, Sociedade e Cultura, Vol. I A Sociedade em Rede*. Lisboa: Fundação Calouste Gulbenkian, 2005.

Cendon, Paolo. *Trattato dei nuovi danni- Informazioni Erronee Soggetti Deboli Illeciti Informatici Danni Ambientali*. Vol. 5. CEDAM, 2011.

Claybourne, Anna. *Dicionário de computadores para principiantes*. Lisboa: Verbo, cop.1995.

Cordeiro, António Menezes. *Manual de direito bancário*, 3.ª edição. Coimbra: Almedina, 2008.

Costa, F. Bruto da. *SPAM e mail-bomb : subsídios para uma perspectiva criminal*. Lisboa : Quid Juris, 2005.

Cunha, Soraia Daniela Rodrigues. " Características faciais e a interpretação de perfis criminais". Dissertação de Mestrado, Universidade de Aveiro, 2011.

David, Joaquim I.S.. *Edição de páginas HTML.* 1.ª edição. Lisboa: Fundação para a Divulgação das tecnologias de Informação, cop.1998.

Dhamija, Rachna, J. Doug Tygar, and Marti Hearst. "Why phishing works."*Proceedings of the SIGCHI conference on Human Factors in computing systems*. ACM, 2006. http://escholarship.org/uc/item/9dd9v9vd.

Dias, Jorge de Figueiredo. *Direito Penal: parte geral, tomo I*. 2.ª edição. Coimbra Editora, 2007.

Dias, Jorge de Figueiredo e Manuel da Costa Andrade. *Criminologia: O Homem Delinquente e a Sociedade Criminógena*. Coimbra Editora, 1997.

Dias, Vera Marques. "A Problemática da Investigação do Cibercrime". In *DataVenia – Revista Jurídica Digital,* Ano 1, n.º1, ed. Joel Timóteo Ramos Pereira. DataVenia. Julho, 2012. http://www.datavenia.pt/ficheiros/edicao01/datavenia01_p063-088.pdf .

Figueiredo, Bruno. *Web Design: Estrutura, conceção e produção de sites Web.* 2.ª edição atualizada e aumentada. Lisboa: FCA, cop. 2007.

Freitas, Pedro Miguel. "Breves nótulas sobre o crime de acesso ilegítimo previsto na Lei do Cibercrime. "In *Estudos em comemoração dos 20 anos da Escola de Direito da Universidade do Minho*, ed.Mário Ferreira Monte, et al., pp. 565-585, Coimbra Editora, 2014.

Garcia Marques, A. J. e A.G. Lourenço Martins. *Direito da Informática.* 2.ª edição. Coimbra: Almedina, 2006.

Guimarães, Maria Raquel. "A repartição dos prejuízos decorrentes de operações fraudulentas de banca electrónica (home banking): anotação ao Acórdão do Tribunal da Relação de Guimarães de 23.10.2012, Proc. 305/09". In *Cadernos de Direito Privado*, nº41, pp.45-69, 2013.

Guimarães, Maria Raquel. *As transferências eletrónicas de fundos e os cartões de débito: alguns problemas jurídicos relacionados com as operações de levantamento*. Coimbra: Almedina, 1999.

Graham, Ian S. *The HTML sourcebook*. John Wiley & Sons, Inc., 1995.

Hoyos, Gustavo Balmaceda. "El delito de estafa informática en el derecho europeo continental." *Revista de Derecho y Ciencias Penales* n.º17 (2011):111-149.

Leukfeldt, E.R., e W.Ph.Stol. *Cyber safety: An Introduction*. Eleven Internacional Publishing, 2012.

Jesus Almeida, Maria teresa de." A tributação do Comércio Eletrónico on-line". Dissertação de Mestrado, Instituto Superior de Contabilidade e Administração da Universidade de Aveiro, 2010.

Leitão, Luís Menezes. "A distribuição de mensagens de correio eletrónico indesejadas (SPAM)". In *Direito da Sociedade da Informação – Vol. IV,* Associação Portuguesa do Direito Intelectual. Coimbra Editora, 2003.

Leukfeldt, Rutger, Sander Veenstra, e Wouter Stol. "High Volume Cyber Crime and the Organization of the Police: The results of two empirical studies in the Netherlands." *International Journal of Cyber Criminology* 7.1 (2013): 1-17. http://cybercrimejournal.com/Leukfeldtetal2013janijcc.pdf.

Mendes, Paulo de Sousa. "A responsabilidade de pessoas coletivas no âmbito da Criminalidade Informática em Portugal." In *Direito da Sociedade da Informação – Vol. IV*, Associação Portuguesa do Direito Intelectual. Coimbra Editora, 2003.

Mendoza, Fátima Flores. "Respuesta Penal al Denominado Robo de Identidade n las Conductas de Phishing Bancario". *Estudios Penales y Criminológicos* vol. XXXIV (Julho 2014): 301-339.

Mockapetris, Paul, and Kevin J. Dunlap. *Development of the domain name system*. Vol. 18. No. 4. ACM, 1988. http://www.dtic.mil/dtic/tr/fulltext/u2/a203901.pdf.

Moniz, Helena. "Internet e Globalização – Problemas Jurídico-Penais: notas breves". In *As telecomunicações e o direito na Sociedade de Informação*, coord. António Pinto Monteiro. Coimbra: Instituto Jurídico da Comunicação. 1999.

Morgado, Maria José e José Vegar. *O inimigo sem rosto, fraude e corrupção em Portugal*. Edições D.Quixote, 2003.

Murphy, Diane R., and Richard H. Murphy. "Phishing, Pharming, and Vishing: Fraud in the Internet Age." *REVIEW* (2007): 37. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.136.3368&rep=rep1&type=pdf#page=41.

Oliveira, Wilson. *Segurança da Informação: técnicas e soluções*. Vila Nova de Famalicão: Centro Atlântico, 2001.

Ollmann, Gunter. "The vishing guide." *http://www. infosecwriters. com/text resources/pdf/IBM ISS vishing guide GOllmann. pdf, IBM, Tech. Rep* (2007). http://www.gupiaoya.com/tools/Miscellaneous/IBM_ISS_vishing_guide.pdf.

Oxman, Nicolás. "Estafas informáticas a través de Internet: acerca de la imputación penal del" phishing" y el" pharming"." *Revista de derecho (Valparaíso)* 41 (2013): 211-262. http://www.scielo.cl/scielo.php?pid=S0718-68512013000200007&script=sci_arttext.

Pablo, José Antonio Cruz de. *Derecho Penal y Nuevaas Tecnologías-Aspectos sustantivos*. Difusión Jurídica y Temas de Actualidad, S.A, 2006.

Pereira, Joel Timóteo Ramos. *Direito da Internet e Comércio Eletrónico*. Lisboa: *Quid Juris* Sociedade Editora, 2001.

Prada, Ignacio Flores. *Criminalidad Informática (Aspectos sustantivos y procesales).*Valencia:Tirant lo blanch, 2012.

Rocha, Maria Vitória. "Novos Meios de Pagamento no Comércio Eletrónico (e-commerce)".In *Direito da Sociedade da Informação – Vol. V*, Associação Portuguesa do Direito Intelectual. Coimbra Editora, 2004.

Rodrigues, Anabela Miranda. *O Direito Penal Europeu Emergente*. Coimbra Editora, 2008.

Santos, Cláudia Maria Cruz. *O crime de colarinho branco: da origem do conceito e sua relevância criminológica à questão da desigualdade na administração da Justiça Penal*. Coimbra Editora, 2001.

Santos, M.Simas e M.Leal Henriques. Noções Elementares de Direito Penal. 2.ª edição. Editora Rei dos Livros, 2003.

Santos, Rita Coelho. *O tratamento jurídico-penal da transferência de fundos monetários através da manipulação ilícita dos sistemas informáticos*. Coimbra : Coimbra Editora, 2005.

Sheng, Steve, et al. "Anti-phishing phil: the design and evaluation of a game that teaches people not to fall for phish." *Proceedings of the 3rd symposium on Usable privacy and security*. ACM, 2007.

Silva, Flávio Manuel Carneiro de. "A usurpação da ciberidentidade". Dissertação de mestrado, Universidade Católica do Porto, 2014.

Stewart, Joe. "DNS cache poisoning – the next generation." *2007-08-25). http://www. secureworks. com/research/articles/dns-cache-poisoning* (2003). http://www.ouah.org/DNScp.htm.

Teixeira, Paulo Alexandre Gonçalves. " O Fenómeno do Phishing – Enquadramento Jurídico-Penal". Dissertação de Mestrado, Universidade Autónoma de Lisboa, 2013.

Teruelo, Javier Gustavo Fernández. "Respuesta penal frente a fraudes cometidos en Internet: Estafa, Estafa informática y los nudos de la Red."*Revista de derecho penal y criminología* 19 (2007): 217-243.

Veiga, Pedro, e Marta Dias. "A Internet e as novas dimensões legais." (2012). http://janusonline.pt/popups2011_2012/2011_2012_1_5.pdf.

Venâncio, Pedro Dias. "Investigação e Meios de Prova na Criminalidade Informática". In *Compilações doutrinais Verbo Jurídico*. Verbo Jurídico, 2006. http://www.verbojuridico.net/doutrina/tecnologia/meiosprovacriminalidadeinformatica.pdf.

Venâncio, Pedro Dias. "Relatório Explicativo da Convenção sobre o Cibercrime" (versão portuguesa. In *Lei do Cibercrime*. Coimbra Editora, 2011.

Verdelho, Pedro. " Cibercrime". In *Direito da Sociedade da Informação – Vol. IV,* Associação Portuguesa do Direito Intelectual. Coimbra Editora, 2003.

Verdelho, Pedro. " Phishing e outras formas de defraudação nas redes de comunicação". In *Direito da Sociedade da Informação – Vol. VIII,* Associação Portuguesa do Direito Intelectual. Coimbra Editora, 2009.

Verdelho, Pedro. "A nova Lei do Cibercrime." *Scientia Ivridica n.º 320. Revista de Direito* (2009).

Wall, David S.. *Cybercrime-The Transformation of Crime in the Information Age*. Polity, 2007.

Yar, Majid. *Cybercrime and society*. 2.ª edição. Sage, 2013.