Universidade do Minho
Escola de Direito

Joana Margarida Andrade Gonçalves

Pharming: Análise dogmático-penal, em especial enquanto forma de lesão do património

outubro de 2015

Pharming: Análise dogmático-penal, em especial enquanto forma de lesão do património
Joana Margarida Andrade Gonçalves
UMinho | 2015

Universidade do Minho
Escola de Direito

Joana Margarida Andrade Gonçalves

Pharming: Análise dogmático-penal, em especial enquanto forma de lesão do património

Dissertação de Mestrado
Mestrado em Direito e Informática

Trabalho efetuado sob a orientação do
Professor Doutor António Manuel Tavares de Almeida Costa
e do
Professor Doutor Victor Francisco Mendes de Freitas Gomes da Fonte

outubro de 2015

Anexo 3

DECLARAÇÃO

Nome: Joana Margarida Andrade Gonçalves

Endereço electrónico: joang_1366@hotmail.com

Telefone: 916954662

Número do Bilhete de Identidade: 13859804

Título dissertação □/tese □

Pharming: análise dogmático-penal, em especial enquanto forma de lesão do património

Orientadores:

Professor Doutor António Manuel Tavares de Almeida Costa

Professor Doutor Victor Francisco Mendes de Freitas Gomes da Fonte

Ano de conclusão: 2015

Designação do Mestrado ou do Ramo de Conhecimento do Doutoramento: Mestrado em Direito e Informática

1. É AUTORIZADA A REPRODUÇÃO INTEGRAL DESTA TESE/TRABALHO APENAS PARA EFEITOS DE INVESTIGAÇÃO, MEDIANTE DECLARAÇÃO ESCRITA DO INTERESSADO, QUE A TAL SE COMPROMETE;

Universidade do Minho, 31/10/2015

Assinatura: _____

AGRADECIMENTOS

Trabalhar com quem admiramos transforma inevitavelmente a nossa obra, tornando o seu processo de conceção mais estimulante e enriquecedor.

Assim, nunca será demais agradecer a colaboração inestimável do Professor Doutor António Almeida Costa pela sua disponibilidade, rigor e amabilidade, em níveis inexcedíveis.

Também ao Professor Doutor Victor Fonte que contribuiu para o rigor técnico e científico deste trabalho com enorme simplicidade e dedicação, sempre destacando o seu valor e importância.

À minha família, em especial à minha irmã, que sempre ouviu as minhas aspirações e confissões com um entusiasmo desmedido, mesmo embora não as conseguindo perceber em toda a sua plenitude.

A Ivo Mirra, pelo suporte emocional e técnico nos momentos de maior apreensão e por ter ajudado no impulso desta obra.

Por fim, a todos aqueles amigos que se deixaram deslumbrar pela beleza e pertinência deste trabalho e que sempre mostraram todo o gosto em contribuir para aperfeiçoá-la.

A todos eles, infinitos agradecimentos. Sem eles, certamente o resultado final não seria digno de tanto orgulho.

"A via da ciência é difícil,
e é difícil distinguir aí o bem do mal.
E frequentemente os sábios dos tempos
novos são só anões aos ombros de anões."

UMBERTO ECO, O Nome da Rosa

"Afirma-se que o mundo, abreviando
as distâncias, transmitindo o pensamento
pelos ares, se unirá mais e reinará
a fraternidade. Desgraçadamente,
não acredito nessa união dos homens."

FIODOR DOSTOIEVSKI, Os irmãos Karamazov, Volume I

RESUMO

A par dos constantes avanços tecnológico, que destroem barreiras antes entendidas por inultrapassáveis, surgem novas e sofisticadas possibilidades de perpetrar crimes através da *Internet* e por acesso a sistemas informáticos: a chamada Criminalidade Informática.

De facto, são inúmeros os ataques que podem ser cometidos por esta via sem que o homem-médio possa estar a par de todos eles a fim de os conseguir combater efetivamente.

Um desses ataques, cada vez com maior ocorrência, é o *pharming*, avanço em relação ao já mais conhecido *phishing* e que surgiu como forma a ultrapassar certos entraves inerentes a este último, trazendo assim uma maior perigosidade e dificuldade em apurar a correspondente responsabilidade.

Porém, a principal lacuna está ainda em perceber com certeza os limites jurídico-penais de enquadramento, o que pode gerar nos nossos tribunais injustiças e dificuldades de tratamento, dados os contornos demasiado técnico-informáticos que as mais ponderadas conclusões pressupõem.

Por isso, visa este trabalho delimitar com rigor o enquadramento jurídico-penal a que se deve reconduzir tal fenómeno, pela previsibilidade de que a sua ocorrência seja cada vez mais frequente e também porque os nosso tribunais se pronunciaram até então apenas numa perspetiva civilística, imperando a necessidade de uma visão de natureza penal.

Palavras-chave: *Pharming*; *Phishing*; Criminalidade Informática; Enquadramento jurídico-penal; Sistema informático.

ABSTRACT

Being aware of constant technological advances which destroy barriers before faced as unbreakable, nowadays we are faced with new and sophisticated possibilities of perpetrating crimes through the Internet by accessing computer systems: commonly called as Cybercrime.

In fact, the atacks that can be commited through this way are so many that common-men can not be aware and defeat all of them effectively.

Pharming is one of those atacks that have occurred more often – in order to overtake some obstacles well-knowned from phishing – and so it means a bigger threat that brings further challeges to find out legal responsability.

Although, the main gap is to fully understand the criminal boundaries of frameworking due to pharming's profile has such technical and informatical peculiarities that must be understood to take the most balanced conclusions. We have it in mind because these doubts could guide our courts to injustices and treatment difficulties.

As such, the main goal of this work is to define precisely the legal framework: in first place because it is predictable the frequent occurence of this phenomenon in our society, and secondly due to the urgency of a correct criminal vision by our courts that has only pronounced themselves in a civilian perspective until now.

Key words: *Pharming*; *Phishing*; Cybercrime; Criminal legal framework; Computer system

LISTA DE ABREVIATURAS E SIGLAS

AOL – *America Online*
Art. – Artigo
APWG – *Anti-Phishing Working Group*
CC – Código Civil
CEDH – Convenção Europeia dos Direitos do Homem
Cfr. – Confrontar
CP – Código Penal
CRP – Constituição da República Portuguesa
DNS – *Domain Name System*
DoS – *Denial of Service*
DDoS – *Distributed Denial of Service*
DHCP – *Dynamic Host Configuration Protocol*
HTML – *Hyper Text Markup Language*
HTTP: *Hyper Text Transfer Protocol*
HTTPS: *Hyper Text Transfer Protocol Secure*
IANA – *Internet Assigned Numbers Authority*
ICANN – *Internet Corporation for Assigned Names and Numbers*
InterNIC – *Internet Network Information Center*
ISP – *Internet Service Provider*
LC – Lei do Cibercrime
LCI – Lei da Criminalidade Informática
MAC – *Media Access Control*
NSA – *National Security Agency*
p. – página
pp. – páginas
PIN – *Personal Indentification Number*
ss. – seguintes
SSL – *Secure Socket Layer*
STJ – Supremo Tribunal de Justiça
TLS – *Transport Layer Secure*
TRE – Tribunal da Relação de Évora
TRG – Tribunal da Relação de Guimarães
TRL – Tribunal da Relação de Lisboa
TRP – Tribunal da Relação do Porto
URL – *Uniform Resource Locator*

ÍNDICE GERAL

INTRODUÇÃO **15**

PARTE I - ENQUADRAMENTO TÉCNICO-INFORMÁTICO **17**

CAPÍTULO I - *PHISHING*, PREDECESSOR DO *PHARMING* **19**

1.1. DELIMITAÇÃO CONCEPTUAL 19

1.2. ÂMBITOS DE ATUAÇÃO 21

1.2.1. E-MAIL E SPAM *21*

1.2.2. WEBSITE ILEGÍTIMO *22*

1.2.3. VISHING *23*

1.2.4. SPEAR PHISHING *23*

1.3. FERRAMENTAS DE ATAQUE 25

1.3.1. OBTENÇÃO DE DADOS DO CLIENTE *25*

1.3.2. "MAN-IN-THE-MIDDLE" *25*

1.3.3. OCULTAÇÃO DE URL *26*

1.3.4. EXPLORAÇÃO DE VULNERABILIDADES *26*

1.4. DADOS DE RELEVO 28

CAPÍTULO II - *PHARMING* **29**

2.1. DELIMITAÇÃO CONCEPTUAL 30

2.2. PRECISÕES CONCEPTUAIS 31

2.2.1.1. ENDEREÇOS IP E ENDEREÇOS MAC *31*

2.2.2. SERVIDOR DNS *33*

2.2.3. HOST FILE, Servidor DNS Local *36*

2.3. MODUS OPERANDI 37

Corrompimento do servidor DNS (Hijacking ou Poisoning) *37*

Corrompimento do Host File *39*

2.4 MECANISMOS DE DEFESA 41

Certificados digitais *41*

Protocolo SSL *42*

HTTP e HTTPS *43*

DNSSEC *45*

PARTE II - ENQUADRAMENTO JURÍDICO-PENAL **47**

CAPÍTULO I – ENQUADRAMENTO GERAL **49**

CAPÍTULO II – QUANTO À OBTENÇÃO ILEGÍTIMA DE DADOS PESSOAIS **53**

2.1. QUANTO À CRIAÇÃO DE UM *WEBSITE* FORJADO 54

2.2. QUANDO AO ACESSO NÃO AUTORIZADO AO SERVIDOR DNS OU AO *HOST FILE* 61

2.3. QUANTO AO CORROMPIMENTO DOS DADOS DO SERVIDOR DNS OU DO *HOST FILE* 65

CAPÍTILO III - OBTENÇÃO, *STRICTU SENSU*, DE DADOS PESSOAIS: CONCURSO DE CRIMES.... 69

CAPÍTILO IV - QUANTO À UTILIZAÇÃO DOS DADOS OBTIDOS ILEGITIMAMENTE 75

4.1. QUANTO À LESÃO DE BENS JURÍDICOS NÃO PATRIMONIAIS 76

A) Crimes contra a liberdade pessoal 76

B) Crimes contra a honra 77

C) Crimes contra a reserva da vida privada 78

D) Crimes contra a vida em sociedade..... 81

4.2. QUANTO À LESÃO DE BENS JURÍDICOS PATRIMONIAIS 83

CAPÍTULO V – UTILIZAÇÃO ILEGÍTIMA DE DADOS PESSOAIS PARA FINS PATRIMONIAIS: CONCURSO DE CRIMES..... 93

CAPÍTULO VI – PUNIÇÃO CONCRETA RESULTANTE DE PONDERAÇÃO GLOBAL 97

CONCLUSÃO.....101

BIBLIOGRAFIA 103

INTRODUÇÃO

A criminalidade é tão antiga como o próprio homem, assim como o aparecimento da criminalidade informática é tão remoto como o aparecimento dos computadores. Desse modo, pode dizer-se que o avanço tecnológico dos computadores é diretamente proporcional ao surgimento de novas e sofisticadas formas de cibercriminalidade.

E isto só é possível porque os sistemas de informação e a Internet estão já de tal forma enraizados nas nossas vidas que nos tornam alvos demasiados fáceis: quer porque este entrosamento não ocorre também quanto ao acompanhamento das crescentes inovações e vulnerabilidades, quer porque a Internet proporciona, pelo menos teoricamente, o Santo Graal de qualquer criminoso – o anonimato.

Mas, ao mesmo tempo, é este anonimato como que um mito, pois para certas entidades ele simplesmente não existe: acontece até conseguirem operar uma vigilância permanente de todos os nossos movimentos internáuticos, que guardam para futuros tratamentos de dados para fins que se lhes sejam úteis. São exemplos destas entidades a NSA, a *Google* e tantas outras que, pelos mecanismos técnicos que têm ao seu dispor, sem que o percebamos, vão esvaziando de sentido os conceitos de anonimato e privacidade *online*.

No fundo, estamos ainda tão extasiados com as novas tecnologias e suas inúmeras possibilidades que nos esquecemos que, como em qualquer realidade, existem fragilidades e, dada a natureza dos bens de que estes mecanismos se servem, muitas e perigosas serão as que se lhe referem.

Reflexo disso mesmo são os dados estatísticos referentes a estas questões. De acordo com a *McAfee*, por exemplo, fornecedora de produtos de segurança, os crimes informáticos relacionados com dados pessoais causaram, só em 2009 e nos Estados Unidos da América, prejuízos de um trilião de dólares.

É nesse panorama que se inserem os múltiplos ataques informáticos, contando-se, entre os mais comuns, o *phishing* e o *pharming*. Estes baseiam-se, embora apenas numa primeira fase, no furto de identidade, uma vez que esta, desde sempre, esteve nas prioridades dos criminosos por ser uma ferramenta valiosa para o subsequente cometimento de crimes. Por isso, dadas as possibilidades que a era digital fornece, tal ilícito parece nunca ter sido tão fácil de consumar.

Em particular, o *pharming* – fenómeno que acabou por eliminar algumas das limitações do *phishing* –, atinge um índice de perigosidade especialmente elevado, impondo, para além de acrescidas exigências de segurança, pertinentes questões de enquadramento jurídico-penal.

Tal acontece porque se tem verificado uma crescente ocorrência de tal fenómeno, exigindo-se, por isso, maior intervenção dos nossos tribunais nesta matéria para dirimir conflitos que tenham por base tais condutas.

Ora, tais decisões nem sempre se mostram fáceis dados os contornos demasiado técnicos deste crime informático. Daí que o nosso propósito com este trabalho seja esclarecê-lo a fim de dissipar todas as dúvidas.

Assim, num primeiro momento, começar-se-á por descrever facticamente o ataque de *phishing*, esclarecendo os seus contornos técnicos – já que é este o antecessor do ataque de *pharming*, verdadeiro objeto do nosso estudo – sem o qual será bastante mais difícil perceber as condutas levadas a cabo pelo *pharmer*.

Seguidamente, analisar-se-á em especial e mais aprofundadamente o ataque de *pharming*, esclarecendo as suas nuances técnicas e todos os conceitos que estas pressupõe, já que só é possível enquadrar juridicamente depois de perceber em que se traduz, na prática e verdadeiramente, a hipótese de estudo.

Após todos estes esclarecimentos de ordem fáctica, passar-se-á à fase de enquadramento jurídico-penal. Para tal, decompor-se-á o ataque de *pharming* nas suas fases constituintes para se perceber a que tipos legais estas se podem reconduzir e concluir pela aplicação de um ou mais deles.

Pretende-se, portanto, que no final se possa concluir acerca da punição que deve respeitar às diversas condutas integrantes deste tipo de crime, pondo por terra as dúvidas até agora existentes.

Parte I

ENQUADRAMENTO TÉCNICO-INFORMÁTICO

CAPÍTULO I - *Phishing*, predecessor do *pharming*

1.1. Delimitação conceptual

§ 1 O advento tecnológico protagonizado pela Internet trouxe inúmeras vantagens de que todos somos testemunhas: uma maior comodidade para a realização das mais variadas operações; a proximidade que parece agora ligar todo o mundo; e até a informação quase infinita que está acessível em qualquer hora e lugar. Porém, em tal panorama não se vislumbram apenas vantagens, e a realidade é que tal avanço tecnológico trouxe também consigo espaço para que muitas ameaças, antes difíceis de concretizar, se consigam facilmente desenvolver.

Por conseguinte, o fenómeno de *phishing* conta-se como uma dessas consequências nefastas que se pretende agora analisar e clarificar. Para tal, a definição de um conceito preciso revela-se de suma importância.

Assim, na esteira de GUNTER OLLMAN[1], podemos definir o *phishing* como um procedimento de cariz tecnológico que se alia a técnicas de Engenharia Social[2] com o intuito de obter informação pessoal e confidencial – e não apenas credenciais de identificação[3] –, daqueles que tiram proveito das múltiplas plataformas *online*. Por isso, este tipo de ataque inicia-se tradicionalmente com um *e-mail* forjado através do qual os criminosos se fazem passar pelas organizações legítimas, detentoras das informações pretendidas (servindo-se das suas designações comerciais, logótipos, *slogan*'s, endereços de *e-mail*, etc.), que, com justificações mais ou menos plausíveis visam os seguintes objetivos:

- Furto de credenciais de acesso a *sites* na *web*[4] (como *Hotmail*, *Gmail*, *eBay*), que, não raro, servem de base a mecanismos em linha de realização de transferências monetárias;
- Furto de credenciais de acesso a serviços bancários (Net-banco);
- Acesso aos detalhes de cartões de crédito;
- Obtenção de moradas e endereços de *e-mail*, já que estas são informações transacionáveis, nomeadamente para empresas com fins publicitários;
- Furto de segredos e outros documentos confidenciais (podendo falar-se a este propósito de *Spear Phishing*[5]).
- Distribuição de *botnets*[6] e agentes DDoS[7].

---

[1] OLLMANN, Gunter – **The Phising Guide: Understanding & Preventing Phishing attacks**. IBM Global Technology Services. USA, 2007, p. 2.

[2] Engenharia Social pode definir-se como um conjunto de práticas que exploram a confiança dos utilizadores, sem necessidade de emprego de qualquer meio técnico, aproveitando-se da dificuldade dos mesmos em acompanhar os progressos informáticos e de compreenderem, por isso, a sua potencialidade para a lesão de bens pessoais e patrimoniais essenciais. Estas técnicas tomam em atenção o facto de o elemento mais fraco de qualquer sistema de segurança de informação ser o próprio ser humano, devido aos seus traços comportamentais e psicológicos que o tornam mais suscetíveis a estes ataques. É, assim, uma ferramenta de exploração das falhas humanas em organizações físicas ou jurídicas.

[3] Como defendem STAMM, Sid ; RAMZAN, Zulfikar ; JAKOBSSON, Markus – **Drive-by Pharming**. Technical Report TR641. Indiana University: Department of Computer Science, 2006, p. 2.

[4] Abreviatura de *World Wide Web* (rede de alcance mundial, em português) ou WWW. Refere-se a um sistema de documentos hipertexto que são interligados e executados na Internet.

[5] Cfr. p. 23, § 7.

[6] Sendo *bot* a abreviatura de robot, este termo respeita à distribuição de *software* malicioso (também designado por *malware*) com o intuito de conseguir controlar totalmente o computador da vítima, transformando-o num

§ 2 O termo *phishing* – utilizado pela primeira vez no ano de 1996, quando um grupo de *hackers* conseguiu obter as informações pessoais dos utilizadores da AOL – visa estabelecer uma analogia com o verbo inglês *fish*[8], já que neste tipo de ataque os criminosos como que tentam pescar informações pessoais: atiram o isco que consiste no envio massivo de *e-mails* fraudulentos para endereços de correio eletrónico (que muitas vezes se adquirem pela compra de bases de dados com tal conteúdo) e esperam que algum dos receptores forneça as informações tão desejadas, fazendo uso, deste modo, da lei dos grandes números.

A razão que está na base da utilização de "ph" é bastante discutida, mas a maioria tende para o paralelismo que se estabelece com o termo *phreaking* que designa um outro ataque mais antigo levado a cabo por *hackers*, mas, desta vez, tendo telemóveis como objeto.

Apesar destas dúvidas, estamos certos de que esta utilização não se refere à conjugação da palavra *fishing* (pescando, em português) com *pharming* – opinião avançada por Paulo Teixeira Gonçalves[9] –, já que este último surgiu posteriormente ao primeiro e dele se distingue em variados aspetos[10].

robot, ou computador *zoombie*, que passa a executar tarefas automatizadas ditadas pelo computador que o controla. Como esta técnica é utilizada simultaneamente para infetar um grande número de máquinas, esses computadores passam a formar uma rede (*net*, em inglês). Desta forma, auxiliam, ainda que involuntariamente a prática da atividade criminosa já que, podendo executar uma ação distribuída coordenada, podem levar a executar um ataque DDoS (cfr. nota de rodapé seguinte) ou até para a propagação de SPAM (cfr. nota de rodapé n.º 11).

[7] Designa um ataque distribuído de negação de serviço. Tipicamente, um ataque de negação de serviço (ataque DoS) traduz-se numa tentativa de tornar indisponíveis os recursos de um sistema informático para os seus utilizadores: não se trata de uma invasão, mas sim de uma invalidação de sistema pela sua sobrecarga, sendo os alvos mais comuns os servidores *web* (máquinas responsáveis por receber os pedidos dos utilizadores e encaminhar-lhes a respectiva resposta). Já no ataque DDoS, com o mesmo intento, um computador mestre (*Master*) detém sobre seu comando um elevado número de máquinas. Dessa forma, faz com que essas acedam ao servidor-alvo no mesmo momento. Como estes possuem um número limitado de capacidade, o grande número de pedidos faz com que ele não seja capaz de responder a nenhum deles.

[8] Em português, pescar.

[9] TEIXEIRA, Paulo Gonçalves – **O fenómeno do Phishing, enquadramento jurídico-penal**. Lisboa: Universidade Autónoma de Lisboa, 2013. Dissertação de Mestrado, p. 12, nota de rodapé n.º 5.

[10] Cfr. pp. 29 e ss.

1.2. Âmbitos de atuação

§ 3 Assim, o *phishing* tem seguido a evolução dos tempos ao adquirir novos e crescentes laivos de sofisticação. Importará, por isso, analisar, ainda que sumariamente, os âmbitos de atuação preferencialmente escolhidos para levar a cabo este tipo de investidas.

1.2.1. E-MAIL E SPAM[11]

§ 4 Este é o método tradicional no que concerne à conduta criminosa descrita. Neste sentido, apelando a técnicas de Engenharia Social, os agentes tentam incluir falsas garantias de segurança e até outro tipo de esquemas maliciosos nos *e-mails* fraudulentos que enviam:

- Utilizam a linguagem, estrutura e elementos gráficos próprios dos *e-mails* legítimos da fonte autêntica;
- Adicionam anexos aparentemente confiáveis mas que, aquando do respetivo *download*[12], instalam inadvertidamente no computador receptor *software*[13] maligno – ou *malware* – que pode visar não apenas a obtenção de informação pessoal, mas também (mesmo por combinação) outro tipo de abusos em relação à privacidade do utilizador[14]. São disso exemplo:

    1) Vírus: *Software* malicioso desenvolvido por programadores informáticos que, à semelhança do vírus biológico, infeta o sistema em que se insere, reproduz-se a si próprio e tenta propagar-se para outros computadores. Conseguindo infetar o sistema, pode levá-lo a realizar qualquer operação que o seu criador pretender;

    2) *Trojan horses*: Em português, Cavalos de Tróia. Designam-se assim por acederem à máquina da vítima sem o seu consentimento e conhecimento, aparentando ser ferramentas confiáveis. Uma vez que contêm códigos maliciosos, quando executados podem praticar qualquer tipo de ação pretendida pelos *hackers*[17] que o criaram. Tal como os vírus, estes *softwares* que exploram a inocência das suas vítimas, para serem eficazes dependem em grande medida da adequação ao sistema operativo[18] da máquina contaminada e correspondente versão, o que, por vezes, podem ser dados difíceis de obter, daí que estas ferramentas requeiram um elevado grau de engenho dos respetivos criadores;

---

[11] O significado desta designação é bastante discutido, mas a maioria tende a entendê-la como *Sending and Posting Advertisement in Mass*, ou seja, envio e difusão de publicidade em massa, respeitando a mensagens de correio eletrónico não solicitadas.

[12] Termo utilizado no ambiente informático para designar a obtenção de informação existente na Internet. São usados em português também os termos "descarregar", "sacar", "baixar", etc.

[13] Programas informáticos.

[14] Embora estes possam também ser difundidos por outras vias que não o *e-mail*.

[17] Peritos em informática com objetivos puramente maliciosos.

[18] Conjunto de programas cuja função é gerir os recursos de um sistema (memória, arquivo, processador, etc.) e facilitar a criação e execução de outro *software*. Entre os sistemas operativos mais conhecidos contam-se o Windows, Linux, OS X, etc. Cada um deles possuiu várias versões que surgem com as sucessivas atualizações.

3) Spyware (como *key-loggers*[20], os mais vulgarmente conhecidos): Programa informático que, automaticamente e sem permissão, recolhe informação do computador da vítima que transmite posteriormente àquele de onde provém. Distingue-se dos *trojan horses* pois, ao contrário destes, não pretendem manipular e dominar o sistema em que se inserem, mas antes passar despercebidos.

- ❖ Mecanismos que visam ultrapassar as ferramentas de deteção de SPAM;
- ❖ Inclusão dos quatro primeiros dígitos do cartão de crédito para que os alvos do ataque acreditem estar a comunicar com a entidade que possui legitimamente tal informação. Porém, os utilizadores esquecem-se ou não sabem mesmo que estes números não são únicos, mas antes comuns à mesma instituição financeira;
- ❖ Personalização do conteúdo dos *e-mails*, mais uma vez recorrendo a técnicas de Engenharia Social, já que as pessoas tendem a mostrar empatia por certo tipo de conteúdos. Por exemplo, se tais mensagens incluírem o nome da vítima o grau de desconfiança sobre as mesmas tende a diminuir. Contudo, tal informação é relativamente fácil de encontrar se pensarmos que os nossos endereços de correio eletrónico têm por base o nosso nome. Para além disso, o apelo a temas mais sensíveis é normalmente um ponto a favor para concretizar a "pesca" de informações pessoais de quem recebe tais mensagens.

1.2.2. WEBSITE ILEGÍTIMO

§ 5 Uma das inovações no *phishing* diz respeito à inclusão de um URL[21] no próprio conteúdo do *e-mail* que remete para o *site* da pretensa entidade que solicita o fornecimento de informações pessoais. Todavia, não passa essa de uma página falsa, criada pelo *phisher*[22] para tornar ainda mais credível o seu ataque. Neste segmento, combinam-se frequentemente várias técnicas:

- ❖ Falsificação de credenciais de segurança. Para fazer face ao *phishing*, várias organizações desenvolveram métodos para o combater. A criação de uma terceira entidade de validação de segurança dos *websites* foi uma delas, tipicamente através da inclusão de gráficos nessas páginas que remetem para as autoridades de validação e para os seus certificados SSL[23] que garantem a legitimidade desses *sites*, verificando e atestando a sua autenticidade

[20] Programa de computador que visa registar tudo o que é digitado no teclado, nomeadamente, senhas e outros dados sensíveis para prática de futuros crimes.
[21] Ou *link*. Sigla que designa um endereço de um serviço disponível numa rede, seja ela interna ou externa, que obedece a certa estrutura.
[22] Termo que designa aquele que pratica o ataque de *phishing*.
[23] Protocolo desenvolvido com o objetivo de elevar a segurança dos dados transmitidos pela Internet. Pode ser usado em vários serviços, mas o mais habitual é em páginas *Web*. Por tal, estes certificados atestam que o *site* a que se acede é verdadeiro e confiável, já que fazem a validação do endereço de domínio e, em alguns casos, da entidade detentora do domínio. Neste caso, o endereço dos serviços acedidos é apresentado no formato http**s**:// . Cfr. p. 43, § 14.

Devido à simplicidade destes mecanismos se percebe a facilidade em falsificá-los para que sejam apresentados mesmo em *sites* falsos.

Figura 1: Exemplo dos gráficos que asseguram a segurança e confiabilidade de uma página de Internet.
Fonte: OLLMANN, Gunter – **The Phising Guide: Understanding & Preventing Phishing attacks**. IBM Global Technology Servics. USA, 2007, p. 9.

- Tomam partido de técnicas de programação, nomeadamente de HTML[24], que permitem ofuscar partes do URL de destino para que não reflita a falsidade do endereço. Com uma simples linha de código de programação, o *phisher* faz com que determinado *link* passe automaticamente a designar um *site* duvidoso sem que visualmente tal seja possível de identificar.

1.2.3. VISHING

§ 6 A designação combina as palavras *voice* e *phishing*, dizendo respeito ao ataque de *phishing* executado pelo telefone, muitas vezes com a promessa de uma falsa recompensa financeira.

É este um setor cada vez mais explorado já que os serviços telefónicos atuais podem começar ou acabar num computador em qualquer parte do mundo. Para além disso, é sabido que o custo de uma chamada telefónica é hoje praticamente negligenciável comparado com a agradável taxa de sucesso deste mecanismo pelo maior grau de confiança que lhe está inerente devido à personalização do contacto, maior acessibilidade à população em geral e imediata resposta que se obtém quando comparado com a de um *e-mail*, que pode demorar ou mesmo nunca chegar. Ademais, o aumento do número de *call centers*[26] faz com que a população esteja mais recetiva ao facto de estranhos estabelecerem contactos telefónicos pedindo informação confidencial.

1.2.4. SPEAR PHISHING

§ 7 Este tipo de *phishing* caracteriza-se pela existência de um alvo muito específico, de determinada empresa, organização ou grupo, ao contrário do alvo bastante abrangente que normalmente costuma possuir este tipo de conduta informática. É este um ataque muito personalizado e laborioso e que exige que

[24] *Hyper Text Markup Language*. Linguagem de programação que permite criar a estrutura de uma página *online* ao ser lida pelos *browsers* ou navegadores.
[26] Em português, central de atendimento. Conjunto de estruturas físicas que visam centralizar o recebimento e realização de chamadas telefónicas.

se conheça de antemão o perfil pessoal, social ou profissional da vítima e seus conhecimentos médios.

Desenhando um *e-mail* bastante personalizado, simulando, por exemplo, a proveniência de um superior hierárquico ou empregador, este ataque pode conseguir, para além da descoberta de informações confidenciais e pessoais, outros segredos de valor patrimonial e não patrimonial considerável, visando-se, por tal, o acesso à própria organização.

Neste sentido se fala ainda no WHALING, *phishing* dirigido a "*whales*" ou "*big fish*"[27].

[27] Em português, peixe grande, metáfora também entre nós conhecida.

1.3. Ferramentas de ataque

§ 8 Para que um ataque de *phishing* possa ser bem sucedido existe uma multiplicidade de técnicas habilmente utilizadas pelos criminosos.

Seguir-se-á uma enumeração das principais, tendo em atenção que vão aparecendo novos métodos a cada entrave imposto aos já existentes, sendo, portanto, uma lista não exaustiva[28]. Importa ainda sublinhar que estes vetores podem ser combinados para garantir a eficácia do ataque que normalmente anda a par da dificuldade da sua deteção.

1.3.1. OBTENÇÃO DE DADOS DO CLIENTE

§ 9 Traduz-se este num dos preferidos e mais antigos métodos utilizados por *hackers*. Aqui se inserem várias ferramentas como os *screen-grabbers* e os já referidos *key-loggers*, utilizadas para obter informação pessoal e confidencial na medida em que, instalados sem autorização dos visados, permitem aos atacantes receber toda a informação processada pelos ecrãs (no caso dos *screengrabbers*, que apareceram mais recentemente para fazer face a técnicas de segurança dos bancos, nomeadamente os teclados virtuais) ou pelos teclados (no caso dos *key-loggers*) para posterior uso para as finalidades que se lhes aprouver.

1.3.2. "MAN-IN-THE-MIDDLE[29]"

§ 10 Este é um dos métodos de atuação com maior taxa de sucesso. Através dele os atacantes posicionam-se, no percurso de comunicação, entre o cliente e o *site* real, conseguindo ter acesso a toda a informação que é transmitida sem que os intervenientes o possam perceber.

Isto acontece porque, por meio de diversas técnicas[30], o cliente é levado a conectar-se ao servidor do atacante – que funciona como *proxy*[31] –, que apresenta o *site* como se do verdadeiro se tratasse e, ao mesmo tempo, estabelece uma ligação em tempo real com o *site* fidedigno. A **Figura 2** contém um esquema que explica claramente este fenómeno.

[28] Acerca de todos os vetores de ataque existentes cfr. OLLMANN, Gunter – **The Phising Guide: Understanding & Preventing Phishing attacks**. IBM Global Technology Servics. USA, 2007, pp. 23 a 40.
[29] Em português, homem-no-meio.
[30] Cfr. OLLMANN, Gunter – **The Phising Guide: Understanding & Preventing Phishing attacks**. IBM Global Technology Servics. USA, 2007, p. 24.
[31] Servidor que age como intermediário na recepção de pedidos pelos utilizadores (de ficheiros, páginas *Web*, etc.), solicitando recursos a outros servidores como meio de simplificar e controlar a complexidade que caracteriza esta rede de pedidos.

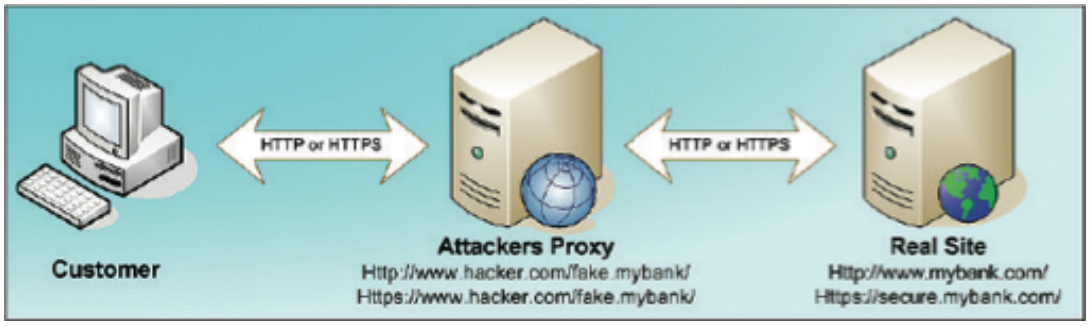


Figura 2: Ataque "man-in-the-middle".
Fonte: OLLMANN, Gunter – **The Phising Guide: Understanding & Preventing Phishing attacks**. IBM Global Technology Servics. USA, 2007, p. 9.

1.3.3. OCULTAÇÃO DE URL

§ 11 Uma das técnicas mais comuns utilizadas para perpetrar um ataque de *phishing* é a inclusão de um URL forjado – no texto de um *e-mail* ou outro método análogo de transmissão de mensagens – a que as vítimas deverão aceder para atestar a credibilidade do pedido que lhes é dirigido. Para convencer os utilizadores a fazê-lo, os *phishers* utilizam várias ferramentas[32] que permitem esconder a parte que poderá indiciar tratar-se de um endereço corrompido, mostrando apenas o que aparentemente constitui a hiperligação para a página legítima.

1.3.4. EXPLORAÇÃO DE VULNERABILIDADES

§ 12 Ao mesmo tempo que aparecem sucessivas atualizações *softwares* existentes e novos outros para combater as suas fragilidades, aumentam as possibilidades de ataque, pois há quem se dedique unicamente a explorar vulnerabilidades dos mesmos que permitam o sucesso dos seus intentos criminosos. Isto acontece ainda porque, simultaneamente, os utilizadores estão cada vez menos a par dos contornos técnicos dos programas que utilizam pela sua crescente sofisticação.

E para quem pense que estas vulnerabilidades são difíceis de descobrir, desengane-se: existem até *websites*[33] que se destinam exclusivamente a fornecer um motor de busca para essas questões. Basta, assim, saber que *software* se quer atacar, fazer uma pesquisa sobre ele e, em poucos segundos, obtém-se o calcanhar de Aquiles de cada um deles. Depois, resta apenas explorar essas fragilidades, realizando o ataque pretendido.

Mais uma vez, neste caso, tratam-se de páginas perfeitamente legítimas e que geralmente pretendem alertar os possuidores dos referidos *software's* para o perigo a que se encontram expostos, devendo tais avisos servir para que se proceda a atualizações ou correções que lhes permitirão minorá-lo. Porém, como em quase tudo, são estas ferramentas aproveitadas para levar a cabo acções com fins mais duvidosos.

---

[32] Cfr. OLLMANN, Gunter – **The Phising Guide: Understanding & Preventing Phishing attacks**. IBM Global Technology Servics. USA, 2007, pp. 25 e ss.
[33] Cfr. por exemplo, https://web.nvd.nist.gov/view/vuln/search e https://web.nvd.nist.gov/view/vuln/search-advanced .

Importa destacar que esta não é uma ferramenta de uso exclusivo para a realização de um ataque de *phishing*, podendo ser utilizada em inúmeros outros contextos e para atingir as mais diversas finalidades.

1.4. Dados de relevo

§ 13 Serão, porventura, estes tão díspares contornos que explicarão a frequente ocorrência e sucesso do *phishing*, tal como demonstram as **Figuras 3 e 4** quando comparadas, constantes dos relatórios trimestrais da APWG – entidade que se dedica ao combate a este tipo de criminalidade – disponíveis na sua página oficial[34].

Statistical Highlights for Q1 2008

	January	February	March
Number of unique phishing reports received	29,284	30,716	25,630
Number of unique phishing sites received	20,305	36,002	24,908
Number of brands hijacked by phishing campaigns	131	139	141
Country hosting the most phishing websites	US	US	US
Contain some form of target name in URL	28.3%	23.2%	26.1%
No hostname; just IP address	5.5%	13.2%	4%
Percentage of sites not using port 80	.81%	.45%	.49%
Longest time online for website	31 days	29 days	31 days

Figura 3: Número de ataques de *phishing* reportados no primeiro trimestre de 2008.

Statistical Highlights for 1st Quarter 2014

	January	February	March
Number of unique phishing websites detected	42,828	38,175	44,212
Number of unique phishing e-mail reports (campaigns) received by APWG from consumers	53,984	56,883	60,925
Number of brands targeted by phishing campaigns	384	355	362
Country hosting the most phishing websites	USA	USA	USA
Contain some form of target name in URL	56.76%	54.31%	64.47%
Percentage of sites not using port 80	0.85%	0.42%	0.56%

Figura 4: Número de ataques de *phishing* reportados no primeiro trimestre de 2014.

Comparando as duas figuras, concluímos que entre 2008 e 2014 o número de ataques de *phishing* reportados a esta organização passou de 85.630 para 125.215 casos, concluindo, desse modo, pelo seu significativo aumento. Daí que as preocupações a este fenómeno atinentes sejam mais do que justificáveis.

[34] Cfr. www.apwg.org .

CAPÍTULO II - *Pharming*

§ 1 Distinguindo-se do *phishing*, mas tendo-o por base, apenas em 2003 este tipo de ataques se começaram a tornar populares.

De facto, com o aparecimento de incontáveis ferramentas e técnicas que visavam combater a ameaça inerente ao *phishing*, surgiu um novo tipo de ataque, mais sofisticado e difícil de detetar e para o qual os mecanismos desenvolvidos até então não ofereciam qualquer proteção.

Para descrever esta evolução nenhuma outra frase poderá encaixar melhor do que a de Bob Violino[35], que serve de título ao seu artigo: *After Phishing? Pharming!*[36].

Para além de pertinente, não temos dúvidas que esta citação surge também como um aviso, pois apesar de o *phishing* estar ainda na ordem do dia, cremos mesmo que, num futuro pouco longínquo, emergirá a todo o vapor o *pharming,* tomando o seu lugar, mas com a diferença de que, o combate deste último será muito mais penoso.

Para entender porquê, importa primeiro perceber os contornos deste novo ataque e quais os seus traços distintivos.

[35] VIOLINO, Bob – **After Phishing? Pharming! Security experts are concerned about pharming, a technically sphisticated DNS-based attack**. New York: CSO, 2005.
[36] Em português, Depois do *Phishing*? *Pharming*!.

2.1. Delimitação conceptual

§ 2 Numa primeira abordagem, podemos definir *pharming* como um **conjunto de técnicas informáticas que manipulam a forma como os utilizadores localizam e se conectam aos domínios *online* de determinada organização, através da modificação do processo de resolução de nomes**.

Com tal conduta, o URL apresentado no *browser*[37], aquando da pesquisa pelo utilizador, é o legítimo, mesmo tratando-se de um *website* falso criado previamente pelo *pharmer*[38] para o efeito (prática comum ao *phishing*). Desta forma se supera o principal obstáculo ao total sucesso do *phishing* referente à utilização de técnicas mais ou menos credíveis para esconder a parte comprometedora do URL, a que permitia detetar a sua falsidade. No *pharming* há um redireccionamento direto para um *site* falso, de onde advém a sua maior perigosidade já que, para o utilizador comum, não se torna perceptível a diferença. Há, assim, o corrompimento do Serviço DNS[39], seja ele local (no próprio computador das vítimas) ou remoto.

Por isso, facilmente se conclui que o *pharming* é muito mais complexo e trabalhoso que o *phishing*. Neste último, ganham destaque as técnicas de Engenharia Social, que apenas pressupõem o conhecimento das fraquezas humanas no envio massivo de *e-mails* não solicitados, requerendo-se diminuto investimento financeiro e temporal, tirando-se antes partido da lei dos grandes números: enviando mensagens para milhões de destinatários, a "pesca" de pelo menos um deles, mais desprevenido, será quase que óbvia.

Já no *pharming*, a queda em tal ataque é quase inevitável já que, fazendo uso de técnicas bastante avançadas – mesmo possível em locais de acesso público e facilitado – e mais dispendiosas em termos económicos, o *pharmer* consegue criar um cenário quase impossível de ser detetado.

Por conseguinte, tal como no *phishing*, os objetivos principais são o furto de informações bancárias e de identificação e a obtenção de vantagens patrimoniais como em momento posterior mais oportuno se discorrerá.

Todavia, para perceber mais claramente e em toda a amplitude a definição traçada, é necessário proceder a algumas precisões conceptuais, dados os contornos técnico-informáticos descritos.

---

[37] Programa informático que torna possível o acesso a páginas *web*, criadas através de diversas linguagens de programação.
[38] Aquele de leva a cabo o ataque de *pharming*.
[39] Isto é, de resolução de nomes – serviço que transforma um *link,* ou URL, num endereço IP que identifica inequivocamente um *site*. Cfr. pp. 33 e ss, § 5 e ss.

2.2. Precisões conceptuais

2.2.1.1. ENDEREÇOS IP[40] E ENDEREÇOS MAC

§ 3 Em todos os sistemas de comunicação, para que a transmissão de informação possa ser feita com sucesso é necessário que as partes envolvidas possam ser identificadas. Na comunicação feita pela Internet são os endereços IP que permitem tal identificação única dos sistemas informáticos (computador, *website*, servidor, telemóvel, etc.).

Nesse sentido, por cada rede em que está inserido, um sistema terá um endereço IP que identifica essa ligação: não identifica um dispositivo na rede, mas um ponto de ligação do dispositivo à rede.

Os endereços IP da versão tradicional (IPv4) são constituídos por uma sequência de 32 bits[41] integrada por quatro grupos de, no máximo, três algarismos (de 0 a 250) separados por pontos – por exemplo, o endereço IP 192.168.1.8.

Porém, porque a estabilidade da Internet depende da exclusividade dos endereços de rede utilizados, mais recentemente surgiu a versão IPv6, uma sequência agora de 128 bits constituída por oito grupos de quatro dígitos (algarismos ou letras), para fazer face ao crescente aumento de dispositivos ligados em rede, oferecendo um número gigantesco de endereços – só comparável ao número de partículas do Universo – para que possa mesmo vir a substituir a versão inicial. Esta necessidade existe efetivamente já que, com o surgimento da Internet das Coisas, qualquer equipamento possui ligação à Internet[42] (seja isso uma vantagem ou desvantagem). Para tal, como já se referiu, é necessária a atribuição de um endereço IP a cada um deles para que seja possível esse tipo de comunicação. O endereço 2001:0db8:85a3:08d3:1319:8a2e:0370:7344 é, assim, um exemplo desta nova versão. Em qualquer destas versões, os endereços têm correspondência em código binário[43], sistema base de qualquer equipamento informático.

Para além disso, todos os endereços IP têm duas partes: a que identifica a rede à qual o sistema está ligado; e a que identifica o dispositivo na rede. Funciona quanto aos mesmos um endereçamento hierárquico, como serve a **Figura 5** de exemplo.

[40] *Internet Protocol*, ou Protocolo Internet, em português. Um dos muitos protocolos existentes já que a Internet se baseia nestes acordos para garantir as funcionalidades que lhe são inerentes.
[41] Simplificação de **B**inary Digi**t**. Menor unidade de medida de informação que pode ser transmitida ou armazenada. Usada em Computação.
[42] Vemos atualmente o caso de torradeiras, frigoríficos e outros utensílios que estão agora *online*.
[43] Sistema de numeração posicional em que todas as quantidades se representam com base em dois números: zeros (0) e uns (1).

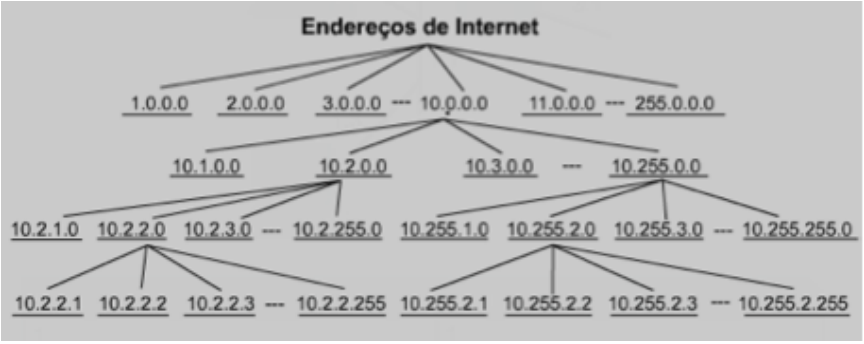


Figura 5: Estrutura hierárquica da disposição dos endereços IP.
Fonte: http://ltodi.est.ips.pt/redescomp/Downloads/Diapositivos/CCNA1-09%20-%20Conjunto%20de%20Protocolos%20TCPIP%20e%20enderecamento%20IP.pdf

Importa ainda salientar que geralmente a um mesmo sistema é atribuído um endereço IP diferente de cada vez que se conecta à rede, o que impossibilita em grande medida a sua descoberta relativamente aos computadores utilizados para a prática de atividades criminosas.

A atribuição destes endereços foi inicialmente concedida à InterNIC, mas passou, desde 2009, para a entidade americana IANA[44].

§ 4 A par destes, cuja existência só faz sentido numa comunicação em rede (na Internet), existe ainda um endereço físico exclusivo de cada dispositivo de rede ("placa de rede"), atribuído pelo fabricante da placa de interface de rede. São estes os endereços MAC que apenas possuem significado local (ao nível da própria máquina) e existem havendo ou não comunicação em rede.

No caso de esta existir, há então uma pergunta que se impõe: como se dá a conversão destes endereços MAC nos correspondentes endereços IP? Esta atribuição pode ser manual, fixa ou dinâmica, sendo esta última mais comum.

Na atribuição manual existe uma tabela de associação entre o endereço MAC e o endereço IP e seus dados, feita pelo administrador de rede. Nesta, apenas os clientes cujos endereços MAC constam nessa lista podem receber as configurações desse servidor, o que será certamente uma limitação.

Já na atribuição fixa, o cliente obtém um endereço IP de um espaço de endereços possíveis – normalmente sem vínculos –, especificado pelo administrador.

A atribuição dinâmica faz-se através do DHCP: cada cliente tem a sua interface de rede configurada para requisitar um endereço assim que for ligada a máquina na rede. Perante esse pedido, o cliente receberá um conjunto de configurações onde constará, pelo menos, um endereço IP e outros dados a ele atinentes. É alocado, assim, um endereço IP que é, neste tipo de atribuição, temporário, isto é, tem um tempo de vida: desligando-se a máquina, o tempo de vida do endereço IP que lhe foi atribuído esgota-se e pode ser atribuído a outro equipamento. Por isso, da próxima vez que o mesmo equipamento se ligar na rede receberá provavelmente um endereço IP diferente.

[44] Cfr. https://www.iana.org .

2.2.2. SERVIDOR DNS

§ 5 Apesar de todas as pessoas que navegam na Internet fazerem uso desta ferramenta várias vezes por dia, o servidor DNS é talvez o serviço menos conhecido, mas de que a rede de alcance mundial[45] não poderia prescindir pela comodidade e conveniência que possibilita.

É este um mecanismo composto por várias camadas de serviços que se interligam e de fluxos complexos de informação que se pretende "confiável". Apesar de aqui nos referirmos ao Servidor DNS como uma ferramenta fundamental no funcionamento da *web*, a verdade é que ele é também imprescindível noutros serviços existentes fora dela, como os serviços de *e-mail* (*Outlook*, por exemplo) entre outros. Assim, é importante perceber que não existe uma correspondência entre o servidor DNS e a *web*: esta última não existe sem os servidores DNS, mas o contrário já não sucede.

Como já foi referido, é o Protocolo Internet (IP) que torna possível a comunicação entre dois sistemas através da atribuição de endereços numéricos. Contudo, as pessoas (singulares ou coletivas) tendem a preferir, em vez desse, um nome que mais facilmente designe os *websites* pela maior facilidade de memorização. Daí que o Servidor DNS seja o responsável por converter os nomes de domínio (dos *websites)* nos correspondentes endereços IP.

Utilizando uma ferramenta que permite fazer simular essa atividade de conversão (*DNS Lookup*[46]*)*, podemos concluir que, por exemplo, ao nome de domínio *http://www.datavenia.pt/* corresponde o endereço IP 130.185.84.191. É precisamente isto de que se encarrega o servidor DNS: de transformar o que conhecemos por o URL de um *website* no correspondente IP, que posteriormente servirá para o localizar a fim de fornecer ao utilizador os conteúdos pretendidos.

Conclui-se, nesse sentido, que sem esta ferramenta seria praticamente impossível obter aquilo que procuramos na Internet pela sua maior facilidade e comodidade. Importará, por isso, perceber, ainda que sucintamente, o seu funcionamento e estrutura.

§ 6 No que toca à sua **estrutura e funcionamento**, o servidor DNS possui uma estrutura hierárquica de servidores que fornecem informação para servidores mais específicos e com informação mais concreta. Tem, desse modo, uma estrutura piramidal: no topo, estão os servidores-raíz (*Root Servers*)[47], seguindo-se os servidores de Domínios de Topo (*Top Level Domain* ou TDL)[48] e, por fim, os servidores de Domínios Autoritários (*Authoritive Domain Servers*)[49].

---

[45] Ou seja, a Internet.

[46] Cfr. http://www.dnsstuff.com/ .

[47] Distribuídos estrategicamente por toda a Internet com nomes distintos que permitem a sua identificação. Têm como função exclusiva apontar para o apropriado servidor *Top Level Domain*

[48] Têm como função dirigir o servidor DNS para um servidor de Domínios Autoritários. Esta camada é dividida em duas classes: os TDLs Genéricos (gTDLs) – por exemplo, .com, .org, .net, . gov. – e TDLs de Códigos de Países (ccTDLs), por exemplo, .pt, .uk, .us. Por sua vez, estes últimos podem possuir outros subdomínios de instituições pertencentes aos diferentes países. Pode dizer-se, portanto, que atualmente os gTDLs e os ccTDLs são mais cruciais para o bom funcionamento da Internet do que os próprios servidores de raíz.

[49] Estes gerem uma zona específica e ainda fornecem os endereços IP e seus detalhes. Podem também delegar esta tarefa noutro servidor DNS.

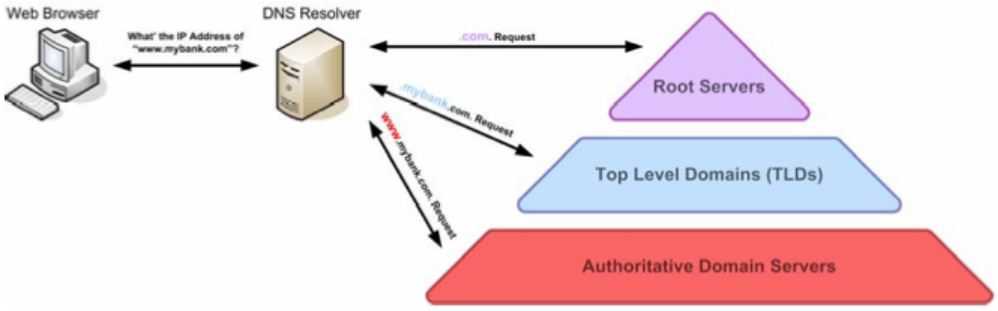


Figura 6: Hierarquia e funcionamento do.
Fonte: OLLMANN, Gunter – **The Pharming Guide: Understanding & Preventing DNS-related attacks by Phishers**. 2005, Next Generation Securuty Software Ltd., p. 5.

É este esquema simples que permite que os utilizares acedam a serviços *online* de qualquer parte do mundo e que as organizações administrem os seus próprios ficheiros de nomes (*host names*)[50].

Em concreto, se alguém digitar o URL *www.meubanco.com*, o servidor DNS irá primeiramente ligar-se ao *Root Server* para obter os detalhes da parte *.com*. Depois, esse servidor fornecerá os detalhes do apropriado servidor de *Top Level Domain* ao qual são solicitados detalhes da estrutura *.meubanco.com*. Como o TLD identifica algo associado ao *website* procurado (como a organização que o detém, o seu local de origem, etc.), cada um deles constitui um registo independente gerido por uma organização sobre a direçãoão do ICANN. Assim, existem várias categorias de TLD pré-estabelecidas e que constam de uma lista específica[51] mantida pela IANA.

Finalmente, dirige-se um pedido os servidores de Domínios Autoritários para fornecer o endereço IP da componente www. para que o utilizador possa aceder efetivamente ao *website* (ver **Figura 6** e **7**), importando destacar que se a tentativa de acesso ocorrer em pontos geográficos distintos, o caminho percorrido pelo servidor DNS será certamente diferente, pois este procura os servidores que estão mais próximos da localização do pedido para conseguir um procedimento mais célere já que é este o motivo que subjaz à criação do servidor DNS.

Gradualmente, as coisas acabam por se complicar, nomeadamente se uma organização estiver registada em múltiplos domínios (por exemplo, meubanco.com, meubanco.pt e meubanco.uk). Isso significa que os pedidos dos utilizadores, para os diferentes serviços em função do domínio, vão requerer diferentes percursos de resolução de nomes para descobrir o endereço IP pretendido. Também os servidores-raíz e os TDLs selecionados mudam em função da localização do domínio pesquisado.

§ 7 O processo descrito, apesar de complexo, demora apenas alguns milissegundos e, por tal, o aparecimento do *site* respetivo por partes é um sinal deste processamento. Para fazer face a possíveis demoras o computador do utilizador pode optar por guardar em *cache*[52] o endereço IP obtido para evitar

[50] Ficheiros de onde consta a correspondência entre um endereço IP e o respetivo nome de domínio (vulgo, nome do site ou *link*).
[51] Cfr. http://www.iana.org/domains/root/db .
[52] Designa o processo de armazenamento temporário de informação (em função de tempo ou de número de pedidos) que, após o limite estabelecido sem que seja utilizada, acaba por ser apagada.

pedidos sucessivos sobre o mesmo tema ao servidor DNS: através deste processo, o servidor DNS verificará primeiro se possui já a informação pretendida na sua base de dados. Se esta informação ainda não tiver expirado, o servidor fornecerá os dados já alojados sem necessidade de aceder a outros servidores, o que poupará bastante tempo de processamento. Caso contrário, o servidor procura a informação desejada segundo o procedimento já referido, guardando-a para futuras necessidades: designam-se estes por servidores DNS com função de *Caching* (*DNS Cache Servers*).
Porém, se se tratar de um primeiro acesso, e para poupar no tempo de resposta, pode recorrer-se a um ISP[53] Local e, na falta deste, a um ISP nacional. Só no caso de estes falharem se recorrerá ao servidor de raíz e cadeia subsequente por esta opção implicar uma maior demora.

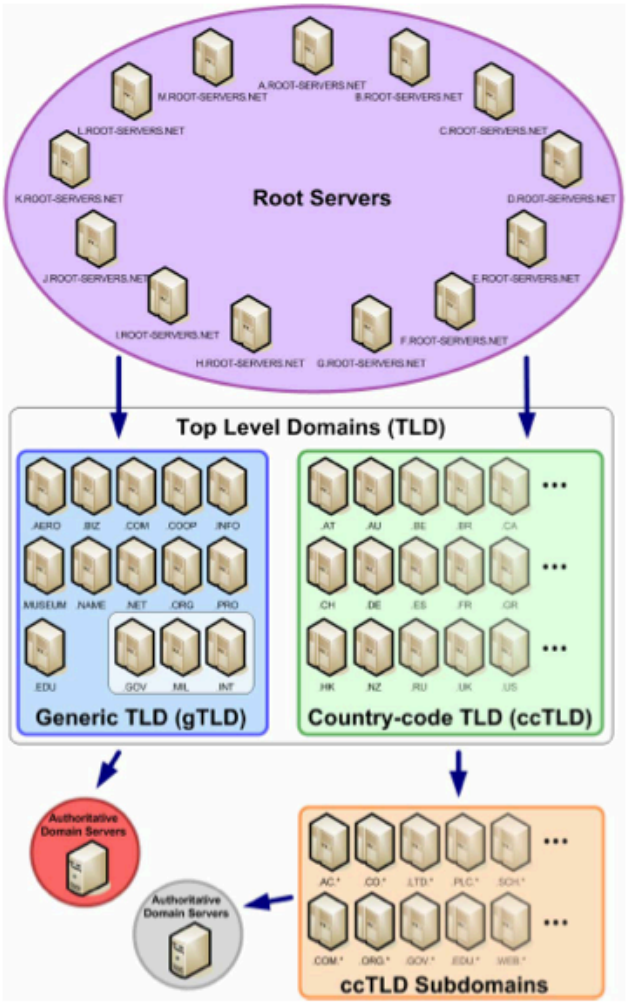


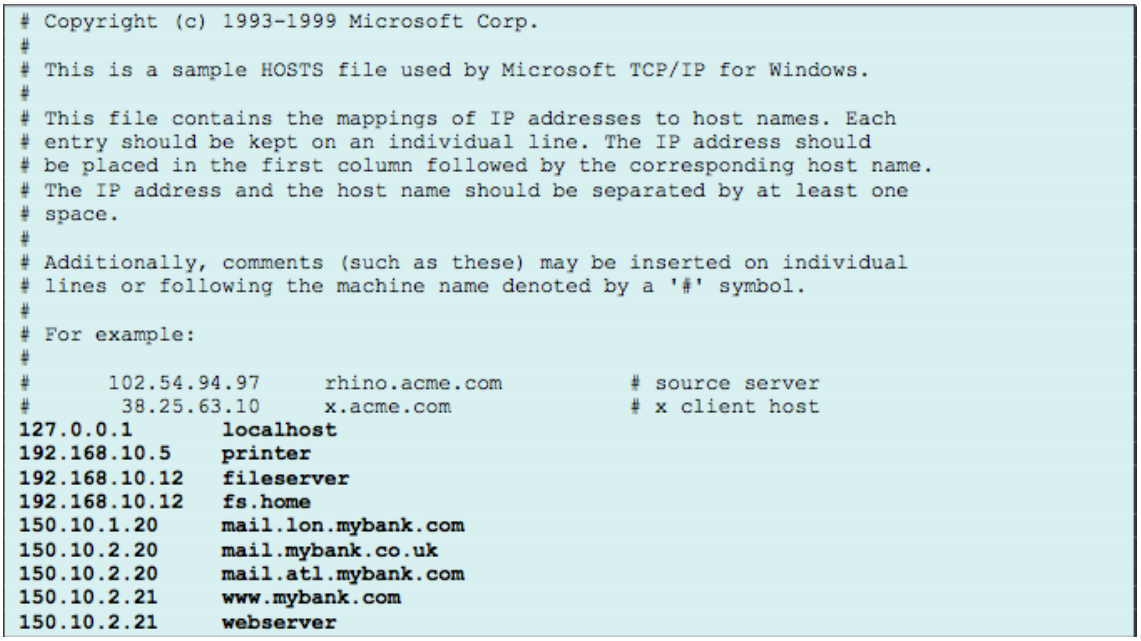
Figura 7: Funcionamento detalhado da resolução do servidor DNS.
Fonte: OLLMANN, Gunter – **The Pharming Guide: Understanding & Preventing DNS-related attacks by Phishers**. 2005, Next Generation Securuty Software Ltd., p. 8.

[53] Fornecedor de acesso à Internet.

2.2.3. HOST FILE, Servidor DNS Local

§ 8 Devido às anteriormente referidas preocupações de rapidez, todos os computadores continuam a manter um ficheiro designado por *host file*, ou ficheiro anfitrião, que é de extrema importância para perceber uma das facetas do *pharming* de que mais à frente se falará. Esta técnica, que corresponde à forma tradicional de fazer corresponder certo *link* ao seu endereço IP, acabou por ser substituída pelo Servidor DNS pela sua maior comodidade já que o *host file* implica uma configuração prévia e exaustiva dos *links* e IP's de todos os *websites* a que se pretende aceder, só tal sendo possível tal acesso na medida em que estes constem da mesma lista. Todavia, esta ferramenta acabou por ser novamente repiscada com maior relevância para fazer face às demoras a que tal Servidor pode conduzir em certos casos.

Este ficheiro contém uma espécie de mapeamento da informação acerca da correspondência entre um URL e o seu endereço IP e localiza-se no ficheiro /etc/hosts.



```
# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host
127.0.0.1       localhost
192.168.10.5    printer
192.168.10.12   fileserver
192.168.10.12   fs.home
150.10.1.20     mail.lon.mybank.com
150.10.2.20     mail.mybank.co.uk
150.10.2.20     mail.atl.mybank.com
150.10.2.21     www.mybank.com
150.10.2.21     webserver
```

Figura 8: Exemplo de um *host file*.
Figura 7: Funcionamento detalhado da resolução do servidor DNS.
Fonte: OLLMANN, Gunter – **The Pharming Guide: Understanding & Preventing DNS-related attacks by Phishers**. 2005, Next Generation Securuty Software Ltd., p. 14.

Dependendo do computador em questão, pode configurar-se a utilização preferencial deste ficheiro para o processo de resolução de nomes em vez do servidor DNS remoto. Isto acontece porque usar o *host file* comporta uma série de vantagens: a velocidade – já que lê apenas a informação local, o que é bastante mais rápido do que o recurso a meios externos; a facilidade de atualização, pois em pequenas redes torna-se mais fácil a configuração e modificação do que num servidor DNS tradicional; a redução do volume de tráfego de Internet, pela necessidade de um menor número de pedidos.

2.3. Modus operandi

§ 9 Pelo que até aqui se expôs, facilmente se percebe que quando alguém se tenta conectar a um serviço *online* (e, consequentemente, a um nome de domínio) vários são os processos que se executam a cada momento por detrás de um *browser.* Por esse mesmo motivo, múltiplas são as possibilidades através das quais o *pharmer* pode perpetrar o seu ataque. Apesar disso, nem todas são úteis: já que o intuito deste é a obtenção de informações confidenciais, alguns vetores de atuação são mais propícios à sua prossecução.

Seguir-se-á uma análise detalhada dos principais vetores. Contudo, em primeiro lugar importa atender ao facto de que, a existência de mecanismos automatizados de resolução de nomes reforça a necessidade de uma gestão e configuração manual cuidadosa dos mesmos de forma a optimizar os serviços e evitar falhas ou erros que potenciam oportunidades de quebras de segurança e de integridade da informação que estas ferramentas contêm: são, não raro, estes fatores humanos os principais responsáveis pelos ataques existentes.

Corrompimento do servidor DNS (*Hijacking ou Poisoning*)[54]

§ 10 Neste tipo de ataque há a inserção de informação de resolução de nomes incorreta no próprio servidor a que se obtém um acesso ilegítimo: *hijacking*[55]. Dessa forma, o atacante pode desviar o utilizador do *website* ou servidor legítimo para outro sobre o qual detém o seu controlo. De acordo com um estudo realizado em 2003, relativamente à "*Domain Health Survey*[56]", um terço do total dos servidores existentes na Internet estão vulneráveis a este tipo de ataque.

Num circuito normal de resolução de nomes, o computador do utilizador dirige primeiramente um pedido ao servidor DNS para que este forneça o endereço IP correspondente ao URL do *site* a que pretende aceder (por exemplo, www.meubanco.pt). Este, executando os processos a que já se aludiu[57], fornece o endereço pretendido para que depois o computador possa conectar-se ao mesmo, acedendo ao servidor que o aloja.

Contudo, com o tipo de ataque mencionado, este processo altera-se substancialmente, já que antes de qualquer passo o agente criminoso acede ao servidor DNS e altera a informação relativa ao endereço IP do *site* em apreço. Apesar de a cadeia continuar sem alterações, o utilizador receberá agora o endereço IP fornecido pelo *pharmer* que corresponderá a um domínio por ele detido e em tudo semelhante ao original e por ele criado. Sem que tenha motivo para duvidar – pois está-se aparentemente perante o *site* real – a vítima insere as suas credenciais de acesso para realizar as normais operações bancárias e, com isto, envia-as para o atacante que as aloja numa base de dados para que, mais tarde, possa aceder ao *site* real e aproveitar-se desta possibilidade ilícita de acesso fornecido, ainda que inconscientemente, pelo próprio titular. Para o utilizador, que está no *site* falso, o que acontece é que lhe pode ser apresentada uma mensagem de indisponibilidade temporária ou de erro na página, pedindo-

[54] É relevante destacar que apesar de o corrompimento – do servidor DNS ou do *Host File* – ser a forma mais frequentemente utilizada para concretizar um ataque de *pharming*, não é a única, podendo ser utilizada a técnica *man-in-the-middle* já mencionada.
[55] Em português, pilhagem, extorsão.
[56] Exame da Saúde dos Domínios
[57] Cfr. pp. 33 e ss.

se a sua atualização. Com esta ação, acaba por haver um redireccionamento, desta vez para a página verdadeira onde se conseguirá o efetivo acesso.

Uma outra técnica possível para executar o *pharming* é o chamado envenenamento da de DNS ou *DNS Cache Poisoning*[58]. Neste, o criminoso tira partido das vulnerabilidades da função de *caching* do servidor DNS já abordada[59], adicionando múltiplas entradas de resolução de nomes não pedidas e que o servidor DNS não tem autorização para fornecer. Assim:

> **1.º** O atacante dirige um pedido ao servidor DNS para saber o endereço IP de um domínio que lhe pertence;
>
> **2.º** Como o servidor DNS não possui essa informação em *cache*, tem de resolver esse domínio através de um pedido a um servidor DNS autoritativo que, no caso, pertence ao atacante (pois o domínio pesquisado está na sua posse também);
>
> **3.º** O servidor DNS autoritativo – que pertence ao atacante e que aloja o *site* sobre o qual foram pedidas informações – informa posteriormente o servidor DNS com função de *caching* do correspondente endereço IP que lhe foi pedido. Em adição, inclui outras informações falsas de resolução de nomes não pedidas que ficarão também alojadas em *cache*. Por exemplo, envia ainda que ao URL *www.meubanco.pt* pertence o endereço IP x.
>
> **4.º** Mais tarde, qualquer utilizador que use aquele servidor DNS com função de *caching* e questione qual o endereço IP para o site ***www.meubanco.pt*** receberá o endereço previamente enviado pelo servidor DNS detido pelo atacante, e que ficou retido temporariamente na sua memória, em vez de ir pesquisá-lo num servidor DNS autoritativo: a vantagem associada à economização de tempo inerente à função de *caching* é, com este ataque, aproveitada como ponto de ataque.

A **Figura 9** esquematiza precisamente o processo descrito, cuja primeira ocorrência ficou registada no ano de 1997.

Importa ainda referir que o DHCP pode também ser corrompido, uma vez que possui, da mesma forma, esta função de resolução de nomes: controlando as suas configurações, um atacante pode definir qual o servidor DNS deve ser utilizado pelo computador em causa para proceder à resolução de nomes que se mostre necessária. Aquando da mesma definição, o criminoso pode inserir então o endereço IP de um servidor DNS que controla e que fornecerá informação incorreta em seu favor, direcionando o utilizador para um domínio à sua escolha, que pode traduzir-se na cópia de um *site* legítimo que o convencerá a inserir normalmente as suas informações pessoais sensíveis, que, com isso, passam a estar alojadas sob a esfera de disponibilidade do agente para posterior uso no *site* verdadeiro, sendo inúmeras as consequências possíveis a partir de tal uso.

---

[58] Ao contrário do que defendem outros autores, não é este um método específico de phishing, mas antes um tipo de pharming já que contende com o processo de resolução de nomes, âncora deste último tal como os mesmos autores destacam, prova da sua contradição. Para tal, cfr. MATHEW, A.R. ; AL HAJJ, A. ; AL RUQEISHI, K. – **Cyber crimes: Threats and protection**. [Em linha]. In **Networking and Information Technology (ICNIT), International Conference on Networking and Information Technology**. Manila: 2010, pp. 16.

[59] Cfr. p. 38, § 7.

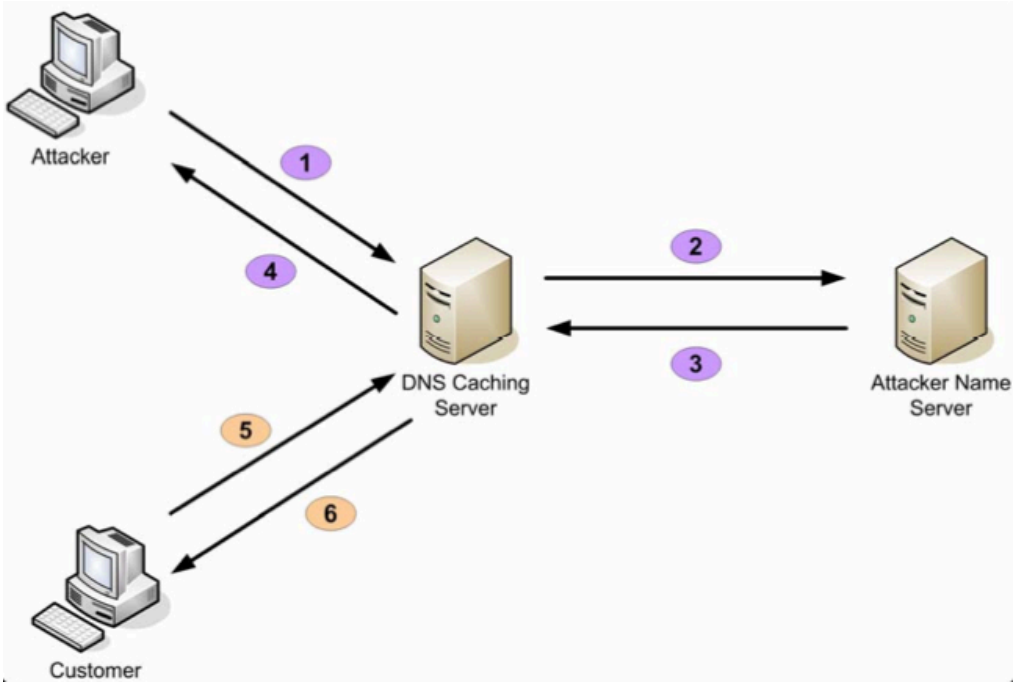


Figura 9: Processo do ataque de Pharming enquanto DNS Cache Poisoning
Fonte: OLLMANN, Gunter – **The Pharming Guide: Understanding & Preventing DNS-related attacks by Phishers**. 2005, Next Generation Securuty Software Ltd., p. 27.

Corrompimento do Host File

§ 11 Nos últimos anos registou-se um aumento substancial de ataques que têm por base o controlo dos computadores das vítimas. Os mecanismos empregues para tal variam em função do objetivo a atingir. Através da disseminação de vírus, Cavalos de Tróia ou outros *software's* maliciosos[60], os atacantes ganham controlo das máquinas que infetam, pois quanto ao ataque a que agora nos referimos, o que se pretende é adquirir a capacidade de modificar as referências de nomes ou os ficheiros de que eles dependem. Também isso pode acontecer através de exploração de vulnerabilidades a nível local, o que não será de sobremodo difícil já que existem *sites* perfeitamente bem intencionados que enumeram as mais recentes vulnerabilidades descobertas em diversos sistemas[61].

Assim, conseguindo inserir-se no computador das vítimas, o atacante procede à alteração do *host file* em seu proveito.

Dessa forma, imaginando que o ficheiro de nomes do computador da vítima designa que ao site *www.meubanco.pt* corresponde o IP 200.1.1.10, pode o *pharmer*, alterando este ficheiro, fazer com que quando o *browser* tenta aceder a esse *site* – e uma vez que o *pharmer* sabe que este ficheiro é usado preferencialmente em relação ao servidor DNS externo – aceda, ao invés, ao endereço IP que corresponde ao *site* falso previamente criado de forma semelhante à página original. Para a vítima, aquando deste acesso, nada há que duvidar já que o URL é o mesmo e o aspeto do *website* também. Por isso, a vítima tentará normalmente inserir as suas credenciais de acesso para proceder

[60] Cfr. p. 21, § 4.
[61] Cfr. p. 26, § 12 e nota de rodapé n.º 33.

às operações bancárias que lhe aprouver. Sem saber, contudo, com essa ação, as suas credenciais são enviadas automaticamente para uma base de dados detida pelo criminoso que poderá depois aceder ao *site* verdadeiro e inserindo as informações obtidas, realizar as transferências monetárias que quiser[62].

Tudo isto é possível porque é bastante simples, para quem controla este ficheiro, modificar as configurações de rede de um computador para apontar todos os pedidos de resolução de nomes a um servidor DNS controlado pelo *pharmer*. A **Figura 10** apresenta esse menu de configuração disponível em cada um dos nossos computadores.

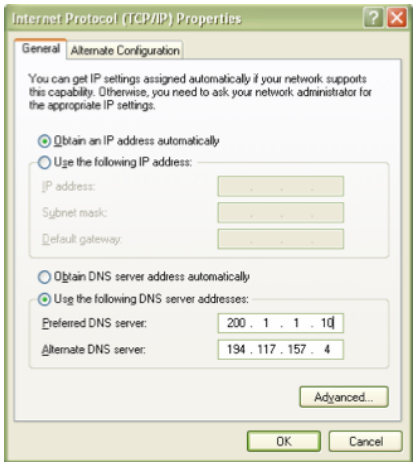


Figura 10: Modificação das preferências do servidor DNS no *host file*.
Fonte: OLLMANN, Gunter – **The Pharming Guide: Understanding & Preventing DNS-related attacks by Phishers**. 2005, Next Generation Securuty Software Ltd., p. 21.

Como se viu, também neste tipo de ataque de *pharming* não há qualquer necessidade de clicar em *links* de *e-mails* para este se torne praticável, daí a sua especial perigosidade e impossibilidade de deteção, pretendendo-se a obtenção de informação pessoal e financeira.

Por tudo o que aqui se referiu quanto a este ataque, devido à complexidade técnica implicada para a sua eficácia – necessidades de adequação do ataque ao sistema operativo, sua versão, etc. –, este ataque é bastante mais difícil de executar do que o tradicional corrompimento do servidor DNS. Porém, claramente se percebe que quando realizado poderá ter consequências muito mais gravosas, devido aos bens jurídicos que aqui estão em causa.

[62] Também quanto a este aspeto pode ser utilizada a técnica "*man-in-the-middle*" já explorada quanto ao *phishing*. Cfr. página 25, § 10.

2.4 Mecanismos de defesa

§ 12 Apesar da documentação acerca deste tipo de ataque ser escassa, os especialistas em segurança das mais variadas empresas alertam para a necessidade de preparar os utilizadores com a sua própria defesa e educação pois muitos deles se encontram ainda sobre o erro de que basta evitarem o clique em *links* desconhecidos para se manterem seguros. Para além dessa percepção ser errada, os principais gestores de segurança mostram-se ainda bastante preocupados por o *pharming* ser capaz de causar danos demasiado graves para serem ignorados. Isto acontece porque com a exponencial popularidade dos pagamentos eletrónicos há cada vez uma maior quantidade de informação valiosa e apetecível a circular na Internet.

O próprio APWG tem procurado discutir aquilo que utilizadores e vendedores precisam de fazer para combater esta ameaça. Não raro, o que dificulta o seu combate é o facto de que o estudo acerca deste ataque é quase inexistente apesar da sua perigosidade e atualidade – como refere Dave Jevans, presidente da APWG –, pois o aumento da sofisticação técnica faz com que a possibilidade de o *pharming* causar sérios danos seja crescentemente considerável (apesar de, ao mesmo tempo, os contornos técnicos que lhe subjazem, pela sua dificuldade, não serem do domínio de um grande número de pessoas). Todavia, dada a sua perigosidade, mesmo que estes ataques possam acontecer menos, os danos associados serão muito mais consideráveis.

Pese embora tudo o que acabou de ser dito confirme que estamos uma ameaça permanente, o que se verifica é que a grande maioria dos utilizadores não conhece minimamente estas possibilidades de ataque e as suas técnicas de exploração, fornecendo facilmente até os seus dados a *sites* fraudulentos com relativa facilidade, pois não conseguem distinguir os legítimos dos restantes. Isso acontece por não conhecerem as regras de segurança *online* mais básicas que devem ser respeitadas para se evitarem danos de maior porte.

Como o *pharming* envolve uma grande variedade de técnicas, são úteis vários meios de defesa (embora alguns dos serviços *online* que utilizamos – como por exemplo o *G-mail*) já comecem a estar munidos de algumas delas): desde os conhecidos programas anti-vírus, *firewalls*[64] com filtros de *spyware's*, programas de prevenção de intrusão e outros *software's* que possibilitam o funcionamento controlado das ferramentas de resolução de nomes.

Para além disso, assumem particular relevância neste âmbito as ferramentas que se explicitarão seguidamente.

Certificados digitais

§ 13 A autenticação é crucial para proteger as comunicações já que aqueles que comunicam devem conseguir provar a sua identidade. Esta operação é bastante complexa já que as partes não se encontram fisicamente nas comunicações *online*, o que torna bastante fácil para outros subverter uma identidade. Para evitar tal incidente, os certificados digitais são, sem dúvida, essenciais por fornecerem formas de verificar uma identidade, fazendo uso de

[64] Em português, parede de fogo. Dispositivo que aplica uma rede de computadores uma política de segurança a um determinado ponto dessa rede para filtrar o tráfego e definir o que pode ou não circular na rede.

técnicas criptográficas[65] que limitam em grande medida a possibilidade de ataque às identidades eletrónicas.

Um certificado digital é um arquivo de computador que contém um conjunto de informações relativas à entidade que pretende ser identificada (pessoa singular, coletiva, computador, etc.) e a sua chave pública e privada, de titularidade única, que são emitidos por uma Autoridade Certificadora com especiais competências para tal. Desse modo, uma mensagem assinada com a chave privada da entidade referida pode ser verificada pelo destinatário da mensagem utilizando a sua chave pública que pode ser encontrada numa cópia do mesmo certificado, a todos acessível. Se a autenticação for bem sucedida, significa que a assinatura foi produzida utilizando a chave privada do requerente do certificado (já que para a assinatura se considerar válida deve ser produzida, em conjunto, com as duas chaves). Assim, para que um destinatário possa confiar na identidade do remetente da mensagem é necessário que este preze por manter a sua chave privada em segredo.

Contudo, os certificados podem ser usados de múltiplas formas e para prosseguir diversos objetivos: autenticação de um *site*, através do protocolo TLS ou SSL; autenticação de um servidos através do protocolo SSL, etc.

Protocolo SSL

§ 14 O protocolo SSL (e o TLS, versão atualizada do mesmo) tornou-se um método universal para autenticação de *websites* e codificação das comunicações entre os utilizadores e os servidores *web*.

Este tornou-se tão determinante porque permite que os utilizadores confirmem a identidade de um servidor *web* ao qual se conectam. Daí que, quando este é utilizado, o *browser* retribui uma mensagem de ilegitimidade do servidor com que se estabelece conexão aquando de um ataque *man-in-the-middle*[66], por falhar a mesma autenticação: este certificado verifica automaticamente o Certificado do Servidor e a correspondente chave pública, analisando se foram emitidos por uma Autoridade Certificadora competente para o efeito.

[65] A Criptografia, fusão das palavras gregas *kryptós* (oculto) e *gráphien* (escrever) designa a ciência que estuda as formas de codificar a informação de forma a que só o emissor e o recetor consigam decifrá-la. Para isso, várias técnicas podem ser utilizadas, uma vez que com a evolução dos tempos foram sendo modificadas e aperfeiçoadas ou surgiram até novas outras que garantem uma maior segurança. Como na computação este valor adquire especial relevo pelos motivos que bem se percebem, usa-se a técnica das chaves criptográficas: trata-se de um conjunto de *bit*'s que tornam possível codificar e descodificar informações. Se as chaves usadas pelo emissor e recetor forem incompatíveis a informação não poderá decifrar-se. A chave é, assim, uma espécie de senha. As chaves podem ser públicas – se podem ser conhecidas por qualquer pessoa – ou privadas – se devem ser apenas conhecidas pela entidade que se pretende identificar. Pode haver combinação entre estas técnicas, falando-se, ora de uma Criptografia de chave simétrica, ora de uma Criptografia de chaves assimétricas. Esta ciência visa sobretudo garantir a autenticidade, integridade e confidencialidade da informação. Para mais esclarecimentos, aceder, por exemplo, a http://www.oficinadanet.com.br/artigo/443/o_que_e_criptografia e http://cartilha.cert.br/criptografia/ .

[66] Cfr. p. 25, § 10.

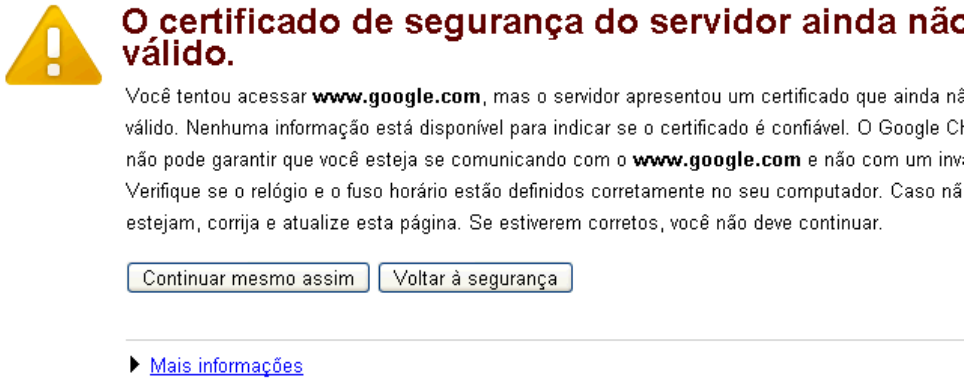


Figura 11: Mensagem retribuída pelo *browser* quando a ligação com o servidor é duvidosa.
Fonte: http://dicasmswxp.blogspot.pt/2013/10/mensagem-o-certificado-de-segurancado.html

Desta forma se vê que através deste mecanismo todos os dados são cifrados, estando protegidos por mecanismos que permitem detetar adulterações e evitar a interceção por terceiros, o que se torna particularmente relevante no comércio eletrónico.

HTTP e HTTPS

§ 15 Quando alguém se quer conectar a algum *site*, no URL aparece sempre a designação http:// ou https://. Pode até parecer que o "s" a mais é um preciosismo, mas não: a verdade é que ele faz toda a diferença, pois permite distinguir entre uma página *web* segura e maliciosa. Tal "s" é sinónimo, pois, de *security*[67].

O protocolo HTTP torna possível que se estabeleça uma troca de informações entre um computador e o servidor que aloja o *site* pesquisado. O problema é que com esse protocolo, em redes menos seguras, as conexões estabelecidas se tornam propícias a ataques como o *phishing* e o *pharming*, possibilitando a interceção de dados com uma certa facilidade por não oferecerem a certeza de que a página a que se acede é aquele que parece ser.

Assim surge o HTTPS, como forma de fazer frente a essas fragilidades, inserindo uma nova camada de proteção na transmissão de dados entre os servidores e o computador. Para tal, incorpora o protocolo SSL, que cifra as informações para as tornar seguras: o servidor envia automaticamente para o cliente a assinatura do certificado digital do *site* que alberga para autenticá-lo. Depois, o *browser* gera uma chave de sessão única que cifra todas as comunicações, incluindo a chave de sessão com a sua chave pública.

Por isso é que o utilizador vê um cadeado fechado antes do URL no *browser*, significando que a sessão é segura e que toda a comunicação será cifrada. Clicando no mesmo pode obter-se as informações do certificado da respectiva página para atestar a sua legitimidade. Este mecanismo de segurança, para além de extremamente confiável, é quase instantâneo e não requer a intervenção do utilizador.

[67] Segurança, em português.

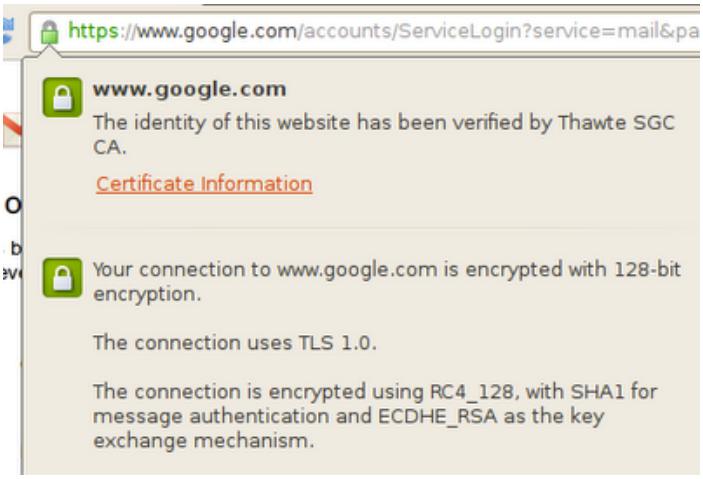


Figura 12: Cadeado de segurança emitido pelo browser perante uma página segura.
Fonte: http://sejalivre.org/google-implementa-uma-nova-tecnologia-para-suas-conexoes-https/

Portanto, quando este acede a um *site* de índole duvidosa, como não se encontram respeitados os trâmites de segurança da comunicação exigidos pelo HTTPS, o *browser* transmite um alerta, como o constante da **Figura 13**.

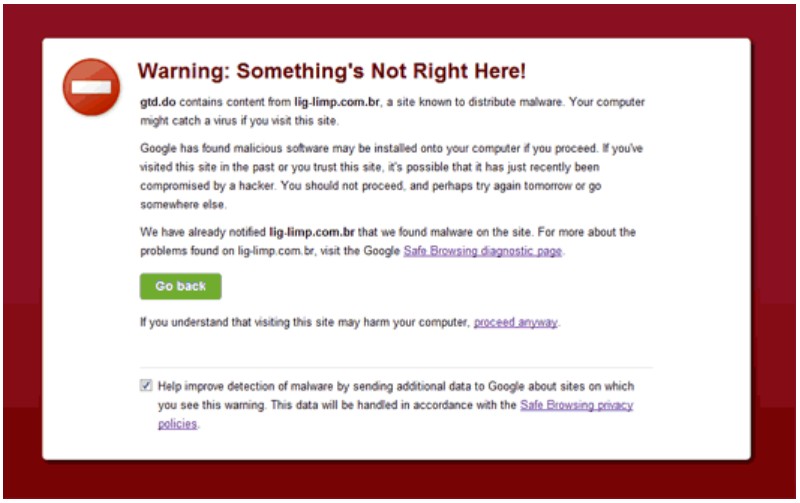


Figura 13 : Mensagem retribuída pelo browser quando está perante uma página duvidosa.
Fonte: http://ngrams.blogspot.pt/2012/02/i-am-not-my-website-warning-somethings.html

§ 16 Claro que isso só acontece nos casos em que tal mecanismo é implementado, pois nem todos os *sites* o fazem. Porém, os *sites* de acesso mais generalizado (como o *Facebook*, *Google*, etc.) já o fazem por defeito.

Por último, é ainda importante destacar que o HTTPS só protege a comunicação e não as suas extremidades, o que significa que se o servidor pretensamente protegido estiver comprometido por *software's* maliciosos, as informações passam a estar comprometidas do mesmo modo.

DNSSEC

§ 17 Este é o termo curto utilizado para designar *DNS Security Extensions* por ser uma extensão ou padrão internacional que atribui contornos de segurança ao servidor DNS, sendo, por isso, já não uma proteção de índole pessoal, mas sim da própria infraestrutura.

Esta extensão foi criada para tornar o servidor DNS mais seguro e assim fazer frente a ataques como o DNS *Cache Poisoning*, reduzindo o risco de manipulação de dados e de domínios forjados que criam a oportunidade para o furto de informações e para causar outros prejuízos de índole pessoal ou patrimonial. Para tal, este mecanismo faz uso da criptografia de chaves assimétricas e implementa a necessidade de autenticação ou validação dos dados e sua integridade, atestando ainda a sua origem. É importante referir que estas operações de validação ocorrem antes de qualquer verificação de segurança ao nível do protocolo SSL ou similar.

Estes mecanismos requerem alterações no próprio servidor DNS porque procuram validar os dados por meio de assinaturas digitais permitindo ao cliente final autenticar dados e a sua origem.

Com o objetivo de fornecer o serviço mais seguro possível, no início de 2010, a zona do ccTLD **.PT** foi garantida com DNSSEC e o DNS.PT lançou o novo serviço em Portugal para o utilizador final. Desse modo, o DNS.PT colabora com a Comunidade Portuguesa para ajudar a implementar DNSSEC nos seus domínios, além de ajudar a atingir o objetivo principal de garantir a segurança da Internet a nível mundial[68].

§ 18 Conclui-se, assim, que muitas são as ferramentas que temos ao nosso dispor para combater estes crime informáticos que descrevemos. Porém, é preciso conhecê-las e, por isso, tentar estar a par destes avanços tecnológicos tal como acontece aquando do lançamento do último *smartphone*, *tablet*, jogo ou filme. Por tal, o aumento da informatização das nossas vidas torna imperatório a necessidade de uma crescente literacia informática.

É, desse modo o *pharming* um problema a ser resolvido por todos e que requererá muito mais do que tecnologia: os utilizadores devem ser sensíveis para facto de que estas ameaças afetam, de facto, a sua vida e que a contínua informação acerca delas será sempre um ponto a fazer daqueles que a elas estão sujeitas.

Todos estes fatores, combinados, podem não eliminar completamente este ataque, mas dificultarão em grande medida a vida dos que a ele se dedicam.

[68] De referir que esta extensão não é eficaz contra o ataque DDoS nem garante a confidencialidade da informação.

Parte II

ENQUADRAMENTO JURÍDICO-PENAL

CAPÍTULO I – Enquadramento geral

§ 1 Assim, descritos os contornos técnicos do fenómeno informático que nos importa tratar, procurar-se-á perceber quais os tipos legais de crime porventura convocados perante o *pharming*.

Relembre-se, em jeito de resumo[69], que o *pharming* se traduz na intromissão em sistemas informáticos e consequente alteração dos dados que os incorporam, por forma a fornecer aos seus habituais utilizadores o serviço aparentemente normal para, depois, conseguir obter os seus dados pessoais, que poderão ser utilizados para os mais diversos fins.

Nesse sentido, este fenómeno criminoso que visa, na prática, diversos propósitos, pode subdividir-se em dois momentos distintos:

a) Um primeiro, composto pelo procedimento conducente à obtenção ilegítima de dados pessoais alheios;
b) E um segundo, caracterizado pela utilização dos dados anteriormente obtidos para múltiplos e distintos fins (de índole pessoal ou patrimonial).

O esquema que segue (**Figura 14**) resume esses momentos e suas principais etapas constitutivas.

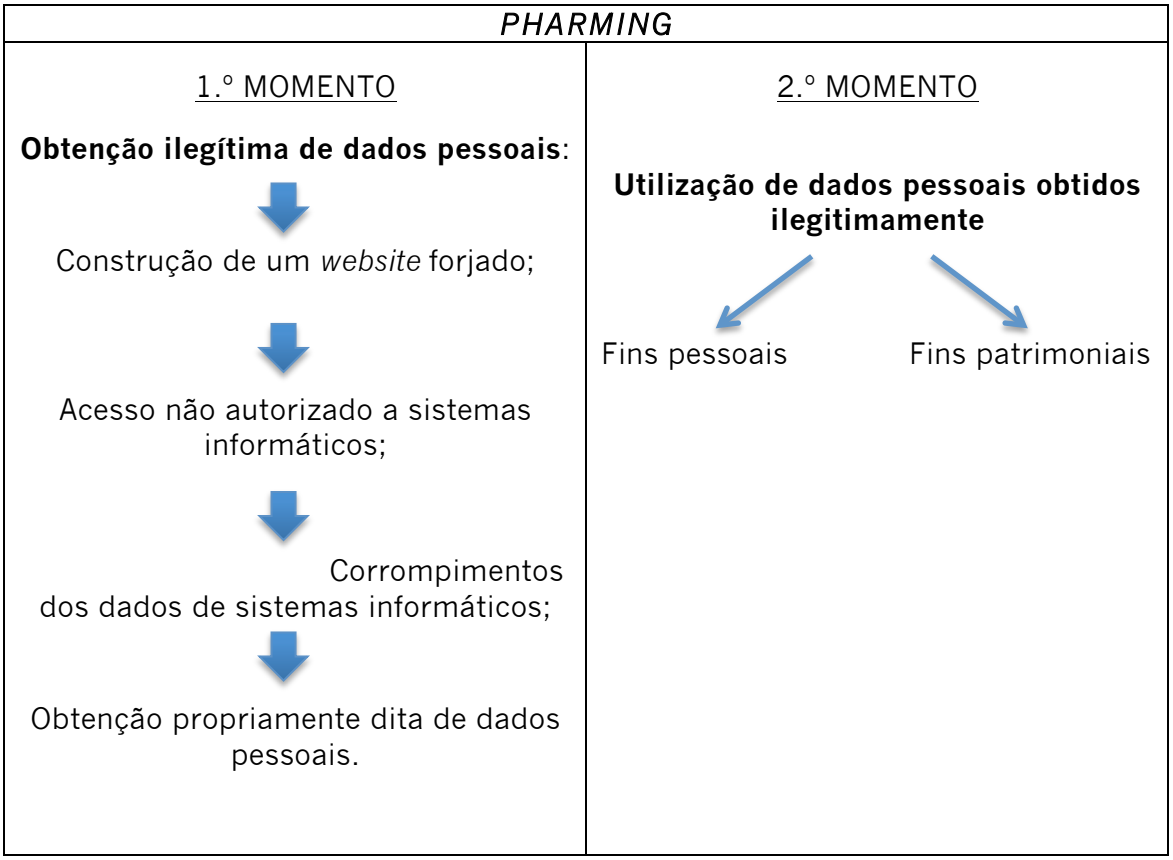


Figura 14: Momentos e etapas constitutivas do *pharming*.

[69] Cfr. pp. 29 e ss.

Deste modo, a análise que se segue passará por analisar os planos normativos que, em abstrato, se perspetivam nos diferentes momentos. Para tal, adotar-se-á como guia o percurso habitualmente seguido pelo agente para levar a cabo um ataque de *pharming*.

Tal servirá para se concluir, a final, acerca da relação existente entre as normas em questão e as próprias fases do procedimento, que trarão consigo diversas consequências a nível penal.

§ 2 Por toda a descrição que se fez anteriormente, torna-se notória a preocupação que tal fenómeno pode suscitar na vida quotidiana, nomeadamente quanto a saber o que se poderá fazer como forma de o combater, motivo pelo qual o nosso trabalho se reveste de tamanha importância.

Tal preocupação está inerente à pergunta escrita colocada por Cristiana Muscardini à Comissão Europeia já a 1 de Fevereiro de 2007[70].

"**Assunto: «Pharming» e «phishing»**

Confrontamo-nos, uma vez mais, com as «insídias» da Internet, ou melhor, com uma utilização abusiva da rede. O novo problema em matéria de Internet, extremamente grave, afeta diversas pessoas que, por razões de natureza tanto pessoal como profissional, são objeto de «phishing» ou de «Pharming» através da utilização do correio eletrónico.

Trata-se de dois métodos que são utilizados para a obtenção da «password» e do endereço IP sem autorização. São ambos muito perigosos e não devem ser confundidos, pois, embora tenham o mesmo objectivo, utilizam sistemas diferentes:

— o «phishing» afeta bancos, empresas e particulares; mediante o envio de uma mensagem eletrónica ratoeira, o remetente apodera-se literalmente dos dados do desventurado destinatário que, ingenuamente, responda à mensagem;

— o «Pharming» consiste na utilização de um software «invisível» que desvia as mensagens eletrónicas para sites fictícios, que se apropriam dos dados nelas contidos sem que o utilizador do correio eletrónico se aperceba do facto.

1. Uma vez que este fenómeno aumenta continuamente em alguns Estados-Membros da União, não considera a Comissão que seria necessário intervir com programas de informação que visem sensibilizar a opinião pública para este problema?

2. Não pensa que se deveriam reforçar as medidas já existentes em matéria de segurança dos cidadãos?

3. Não considera que, também neste caso, é necessário proteger a vida privada dos cidadãos que se servem da Internet para as suas diversas atividades?"

A Comissão respondeu a tais questões a 13 de Março de 2007[71], fornecendo as estratégias que considera adequadas para fazer frente a tais fenómenos.

"**Parliamentary questions**
13 March 2007
Answer given by Mrs Reding on behalf of the Commission

The Commission is concerned about information security and personal security problems on the Internet and, in particular, about those that put privacy at risk such as so- called 'pharming' and 'phishing' activities. The Commission highlighted the importance of ensuring trust and security as an

[70]Disponível em: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+WQ+E-2007-0319+0+DOC+XML+V0//PT .
[71]Disponível em http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2007-0319&language=PT.

integral part of Internet and information society in the i2010 communication. To this end, the Commission adopted 'A strategy for a secure information society —"Dialogue, partnership and empowerment"' to promote more coordinated efforts on network and information security at a European level.

The EU's Safer Internet plus programme aims to promote safer use of the Internet and new online technologies, particularly for the target groups of parents, teachers and children. A network of national nodes has been set up to carry out awareness-raising in the Member States. Furthermore, under the EU fraud prevention action plan 2004-07, public awareness on Internet security and cyber crime was increased by discussing these topics at the Commission's high level conference 'The EU's legal framework for e-business and innovation' in November 2006.

In November 2006, the Commission adopted a specific communication on fighting spam, spyware and malicious software. The communication seeks to ensure that these issues are given greater priority, and proposes actions that need be undertaken by Member States, private undertakings and at EU level to address these threats that undermine user confidence. These actions include countering threats such as spyware and 'phishing'. In 2007 the Commission will issue a communication on the fight against cyber crime. The communication will outline a number of actions aiming at reinforcing EU-wide and international law enforcement cooperation as well as cooperation between law enforcement authorities and Internet service providers and other private sector operators. The Commission will launch, in 2007, a comparative study on the penal legislation covering identity theft and phishing to evaluate whether to propose new harmonised rules for a specific offence of identity theft and approximate the penal sanctions. The Commission communication on the review of the regulatory framework for electronic communication already includes a number of proposals to strengthen security and privacy.

In research, under the sixth framework programme, prospects have been supported for developing knowledge and technologies to secure modern information services, systems and networks. Specific areas addressed include identity and privacy management, authentication, secure digital assets, cyber crime and biometrics as well as tools to fight identity fraud. Recently started activities concern adaptive phishing filters which can detect unknown threats. This research area will be continued under the information and communication technology (ICT) theme of the seventh framework programme (2007-13)."

Estas estratégias afiguram-se de extrema necessidade, ainda que insuficientes, já que emerge a necessidade da existência de uma visão clara e segura acerca destes fenómenos (principalmente do *pharming,* segundo a nossa opinião, pela sua maior perigosidade) e do respetivo enquadramento legal – sobretudo de natureza penal – como forma eficaz de combate, quer pela crescente ocorrência que se prevê, quer porque soluções meramente diplomáticas e programáticas que não bastam para fazer frente a estes ataques.

É tendo por base essa necessidade que a análise que se segue se mostra tão relevante.

CAPÍTULO II – Quanto à obtenção ilegítima de dados pessoais

§ 1 Para perpetrar um ataque de *pharming*, num primeiro momento, como se referiu, o criminoso tenta, interferindo num sistema informático, chegar ilegitimamente ao conhecimento de dados pessoais das vítimas.

Para isso, consegue aceder ilegitimamente ao Servidor DNS ou ao *Host File*, para seguidamente corromper o sistema em questão. Este corrompimento consistirá em alterar o nome de domínio correspondente a certo *website* fidedigno[72], que passa a designar o *site* falsificado criado de antemão, em modo *offline,* pelo próprio agente e em tudo semelhante ao original[73].

Aliando estes mecanismos, o agente criminoso engana facilmente a vítima, convencendo-a da veracidade do que lhe é apresentado: o *link* do *website* (vulgo, "nome") e o aspeto da página apresentada afiguram-se como os habituais – iguais aos que asseguram a confiança na instituição que representam –, quando, na realidade, passam a corresponder ao *site* forjado, igual ao de que o criminoso pretende obter vantagens.

Por conseguinte, a vítima acede normalmente à sua área pessoal (inserindo, para isso, as suas credenciais de acesso – o seu nome de utilizador e correspondente palavra-passe) no *website* falso e, sem que de tal tenha consciência, envia esses dados para a esfera de disponibilidade fáctica do agente – que habitualmente passam a integrar uma base de dados. É desta forma que o criminoso acaba por conseguir alcançar o seu primeiro intento, isto é, a obtenção dos dados pessoais.

As condutas atingem níveis especialmente graves se pensarmos nas atividades sensíveis que podem ser alvo das mesmas: *websites* de bancos, de contas de *e-mail*, de autoridades fiscais, sociais e civis que podem possibilitar aos criminosos o acesso a qualquer tipo de informação.

Ora, por tudo isto, diversas são as disposições normativas que abrangem, em abstrato, estas condutas.

[72] Por exemplo, www.santandertotta.pt .

[73] Por exemplo, se o agente pretender atacar o site www.santandertotta.pt com o IP x, corrompendo o serviço de resolução de nomes, o mesmo nome de domínio passa a corresponder a outro IP que designa, na realidade, o site forjado criado pelo agente e semelhante ao verdadeiro.

2.1. Quanto à criação de um *website* forjado

§ 2 Referimo-nos, então, à cópia exata do *site* original a que o agente procede, antecipadamente e em modo *offline*, para posteriormente substituir o confiável e ser apresentado perante a vítima como se do verdadeiro se tratasse.

§ 3 Primeiramente, prefigura-se um enquadramento no âmbito da Lei do Cibercrime (Lei 109/2009, de 15 de Setembro).

Esta lei, que veio substituir a anterior Lei da Criminalidade Informática (Lei 109/91, de 17 de Agosto), tem como fonte a Convenção Sobre o Cibercrime do Conselho da Europa, mais conhecida como Convenção de Budapeste, que é o primeiro trabalho internacional de fundo sobre crime no ciberespaço, pois embora tenha na sua origem, sobretudo, países membros do Conselho da Europa, tem vocação universal, pretendendo harmonizar as várias legislações nacionais sobre a criminalidade contra sistemas de computadores, redes ou dados, facilitando a cooperação internacional e as investigações criminais na matéria, dada a ausência de fronteiras que caracteriza estes crimes. De realçar que esta Convenção não só versa sobre direito material, definindo os concretos crimes, mas também contempla medidas de natureza processual e de cooperação judiciária internacional, tendo sido definitivamente subscrita a 23 de Novembro de 2001.

Assim, relativamente à criação de um *website* falso, o artigo 3.º da Lei do Cibercrime, que se refere ao crime de **Falsidade Informática**, parece, em abstrato, aplicar-se.

Esta norma teve como fonte inspiradora o artigo 7.º da Convenção sobre Cibercrime do Conselho da Europa[74], tendo pretendido consagrar um regime idêntico ao de outras legislações.

Este não é, todavia, uma total novidade no nosso ordenamento jurídico, já que tem como seu correspondente o crime de Falsificação de Documentos, presente no artigo 256.º do Código Penal. O mesmo, apesar de se encontrar no capítulo relativo aos crimes contra a vida em sociedade, é considerado como um crime "a meio caminho entre os crimes contra os bens coletivos e os crimes patrimoniais", de acordo com FIGUEIREDO DIAS[75].

Embora o artigo 256.º do CP, na sua origem, não tenha sido pensado para realidades informáticas, a verdade é que os documentos informáticos são tratados pela lei como documentos com a mesma força probatória que os documentos escritos físicos[76].

No crime de **Falsificação de Documentos** – onde muito foi beber o crime de Falsidade informática –, quanto ao tipo objectivo, mostra-se necessária, como a sua própria designação deixa antever, a produção de um documento falso, o que poderá ocorrer através das múltiplas formas que constam das alíneas do número 1 do artigo 256.º do Código Penal. Nesse sentido, e na medida em que se exige a verificação de um resultado (falsificação de documento) para o

---

[74] *Título 2 – Infrações relacionadas com computadores*
Artigo 7.º - Falsidade Informática
Cada Parte adotará as medidas legislativas e outras que se revelem necessárias para estabelecer como infração penal, em conformidade com o seu direito interno, a introdução, a alteração, a eliminação ou a supressão intencional e ilegítima de dados informáticos, produzindo dados não autênticos, com a intenção de que estes sejam considerados ou utilizados para fins legais como se fossem autênticos, quer sejam ou não diretamente legíveis e inteligíveis. Uma Parte pode exigir no direito interno uma intenção fraudulenta ou uma intenção ilegítima similar para que seja determinada a responsabilidade criminal.

[75] COMISSÃO DE REVISÃO DO CÓDIGO PENAL, Lisboa, 1993 - **Actas e Projecto da Comissão de Revisão**. Lisboa: Ministério da Justiça, Rei dos Livros, 1993, p. 297.

[76] Cfr. artigo 3.º e 5.º do Decreto-lei 290-D/99, de 2 de Agosto.

preenchimento do ilícito-típico, estamos perante um crime de resultado ou material[77].

Relativamente ao bem jurídico tutelado, são de referir substanciais divergências doutrinais. A doutrina tradicional desde sempre defendeu que está em causa a proteção da fé pública, enquanto responsável pela manutenção de um sentimento geral de confiança nos atos públicos. Entre os defensores desta doutrina contam-se FIGUEIREDO DIAS e COSTA ANDRADE, entendendo que "o que o crime de falsificação protege é a verdade intrínseca do documento enquanto tal. Em primeiro lugar, a verdade no que toca à autenticidade e genuidade da sua origem e proveniência, que será frustrada com a chamada falsidade material (...). Em segundo lugar, a verdade necessária à função probatória específica do documento, isto é, a correspondência entre o documento e o que é documentado, independentemente da verdade, coerência, ou lógica no interior das expressões da vida que constituem o conteúdo ou o objeto do documento. E fala-se a este propósito de falsidade intelectual ou ideológica."[78] Por outra palavras, na falsificação material o documento em causa não é o genuíno, tendo havido uma alteração total ou parcial do mesmo, enquanto que na falsificação ideológica o documento é inverídico, contendo declarações falsas.

Também neste grupo se incluem autores como DONNEDIEU DE VABRES[79] ou MANZINI[80].

Porém, tal entendimento foi sendo criticado, defendendo-se que o que na realidade se protegia era a verdade da prova. Progrediu-se depois para a conclusão de que no crime de Falsificação de Documentos se defendia os meios de prova e autenticação e, por isso, limitou-se o conceito de fé pública, considerando-se a Falsificação de Documentos como um atentado à genuinidade e veracidade dos meios de prova por se entender que o que se protegia com tal incriminação era o documento com a sua específica força probatória. Nesse sentido, criou-se uma nova corrente que defende a segurança e credibilidade no tráfego jurídico-probatório como bem jurídico tutelado por este tipo legal. É neste quadrante que se inclui HELENA MONIZ[81].

Tal como esta autora, parece-nos que sendo a fé pública uma característica atinente apenas a certos documentos, é o documento como meio de prova que deve ser protegido, quer esta sua função se chegue a desempenhar ou não. Para além disso, não cabe ao Direito Penal proteger apenas os documentos dotados de força probatória plena (abrangidos pelo conceito de fé pública), mas também aqueles cuja falsidade possa vir a colocar em causa a segurança do tráfego jurídico-probatório, dadas as funções de perpetuação e de garantia relacionadas com os documentos.

Neste sentido, é este um crime de perigo[82], pois após a falsificação do documento o bem jurídico ainda não foi lesado, mas apenas foi posto em perigo: a confiança e a fé públicas já foram atingidas efetivamente, mas a segurança e a credibilidade do tráfego jurídico-probatório não. Trata-se, portanto, de um crime

---

[77] Em sentido contrário, cfr. MONIZ, Helena Isabel Gonçalves – **O crime de falsificação de documentos: da falsificação intelectual e da falsidade de documento**. Livraria Almedina, 1993, pp. 27 e ss.

[78] Cfr. DIAS, Jorge de Figueiredo / ANDRADE, Manuel da Costa – **Parecer**, *in* Colectânea de Jurisprudência, VIII, pp. 23 e seguintes.

[79] VABRES, Donnedieu de – **Essai sur la notion de préjudice dans la théorie générale du faux documentaire**. 1941, p. 227.

[80] MANZINI – **Trattato do Diritto Penale Italiano**. 1935, VI, pp. 431 e seguintes.

[81] Cfr. MONIZ, Helena Isabel Gonçalves – **Comentário Conimbricense ao Código Penal (artigo 256.º)** , § 14 a 20.

[82] Seguimos, quanto à classificação dos crimes, a categorização tradicional presente, por exemplo, em DIAS, Figueiredo – **Direito Penal: Parte Geral, Tomo I**. Coimbra: Coimbra Editora, 2007: 11 / B / § 20 e ss.

de perigo abstrato, já que o perigo não constitui elemento do tipo, mas apenas motivo da proibição. Não é, assim, necessária a verificação de um perigo concreto, mas tão-só que a conduta do agente seja apta a lesar o bem em causa, havendo, por isso, uma antecipação da tutela penal. O dano verificar-se-á quando o documento entrar efetivamente "em circulação" como se do verdadeiro se tratasse, substituindo o original no tráfego jurídico-probatório.

O mesmo entendimento adota o Supremo Tribunal de Justiça que, em sede de Uniformização de Jurisprudência[83], afirma que " o crime de falsificação de documentos é um crime contra a vida em sociedade, em que é protegida a segurança e confiança do tráfico probatório, a verdade intrínseca do documento enquanto tal, como bem jurídico. É um crime de perigo (o mero ato de falsificação põe em perigo a segurança e credibilidade no tráfico jurídico probatório) abstrato (basta que o documento seja falsificado para que o agente possa ser punido). "

Por último, quanto ao tipo subjetivo, o crime de Falsificação de Documentos é um crime doloso, pois o agente tem de atuar com conhecimento e vontade de realização do tipo objetivo, nisto se traduzindo o dolo[84]. Para além disso, é este um delito de intenção já que o agente deve ainda atuar com a motivação de "causar prejuízo a outra pessoa ou ao Estado, ou de obter para si ou para outra pessoa benefício ilegítimo".

Porém, ao contrário do que acontece no sistema alemão e no crime de Falsidade Informática constante da Lei do Cibercrime, não se requer expressamente a intenção específica de provocar engano nas relações jurídicas. Contudo, parece que, apesar da redação diversa, no plano subjetivo não se justifica tal diferença, estando tal intenção sempre implícita no caso de uma falsificação de documentos. Tal acontece uma vez que aquando da prática de condutas que preenchem o presente tipo legal (que se prendem com a criação de um documento falsificado) tal intenção está inevitavelmente presente. Caso contrário, por que motivo alguém falsificaria qualquer documento se não mesmo para provocar engano nas relações jurídicas?

O mesmo entende o Supremo Tribunal de Justiça, no Acórdão de Uniformização de Jurisprudência a que nos referimos anteriormente, mencionando que o crime de Falsificação de Documentos é "um crime intencional em que o agente necessita de atuar com «intenção de causar prejuízo a outra pessoa ou ao Estado, ou de obter para si ou para outra pessoa benefício ilegítimo» não se exigindo no entanto, uma específica intenção de provocar um engano no tráfico jurídico."

Na Alemanha, uma redação como esta existe igualmente no § 269 *StGB* onde o crime de Falsidade Informática mantém uma relação de especialidade com o crime comum de Falsificação. Porém, como mais à frente esclareceremos, parece que no nosso ordenamento jurídico não poderemos retirar a mesma conclusão quanto à relação existente entre os dois preceitos[85].

§ 4 Relativamente ao crime de **Falsidade Informática**, quanto ao tipo objetivo, é necessária a introdução, modificação, apagamento ou supressão de dados informáticos ou qualquer outra interferência num tratamento informático

[83] Cfr. Acórdão do Supremo Tribunal de Justiça de Uniformização de Jurisprudência, de 25–01–2003, disponível em https://dre.pt/application/dir/pdf1sdip/2003/02/049A00/14091419.pdf .

[84] Quanto ao dolo, enquanto modalidade da categoria da culpa jurídico-criminal, como "previsão e vontade de realização do tipo objetivo de ilícito", optamos pela orientação tradicional, que vê o dolo como uma atitude pessoal de contrariedade e indiferença face à ordem jurídico-criminal. Cfr. DIAS, Figueiredo – **Direito Penal: Parte Geral, Tomo I**. Coimbra: Coimbra Editora, 2007: 10 / 3.2 / § 65 a § 70.

[85] Cfr. *infra* § 5.

de dados. Mas, para a consumação deste ilícito-típico, mostra-se ainda necessário que, de tais condutas, resulte a produção de dados ou documentos não genuínos. Dessa forma, estamos perante um crime material ou de resultado, pressupondo-se a verificação de um resultado (ou seja, a produção de documento informático falsificado).

Quanto ao bem jurídico tutelado, podemos dizer que, na sua génese, este artigo 3.º da Lei do Cibercrime visa proteger a intangibilidade dos sistemas informáticos, ou seja, a sua "intocabilidade", neste caso, sob a forma de salvaguarda dos dados deles constantes que, falsificados, colocam em causa o sistema informático no seu todo, afetando a sua credibilidade, segurança e normal disponibilidade, características que qualquer sistema confiável pretende manter intatas para poder cumprir fielmente as funções que se propõe executar.

É este também o entendimento de autores como PEDRO DIAS VENÂNCIO[86] e PEDRO VERDELHO[87], assim como o dos nossos tribunais que, tendo-se pronunciando-se em diversos casos[88] acabam por defender que o bem jurídico tutelado com este tipo legal é a integridade dos sistemas de informação.

De facto, toda a Lei do Cibercrime tem o seu foco no sistema informático e sua proteção, visando acautelar os ataques de que estes são, cada vez mais, alvo. Tal é comprovado, não só pelas normas nela constantes, mas também pela própria designação da Decisão Quadro n.º 2005/222/JAI que com esta lei foi transposta para o nosso ordenamento jurídico: "... relativa a ataques contra **sistemas de informação**", o que pode ser lido no texto da própria Lei do Cibercrime. Isto acontece porque se sabe que atualmente a grande maioria do tratamento e utilização de dados acontece ao nível desses sistemas e que, por isso, devem estes manter-se incólumes, dada a importância do seu conteúdo e funções no mundo de hoje.

Nessa medida, concluímos que este é um crime de dano. Isto acontece porque independentemente da conduta em causa (introdução, modificação, apagamento, supressão ou outra), o que se requer é que se produza uma interferência efetiva num tratamento informático de dados, como deixa antever a letra do mesmo preceito normativo. Ora, quando tal consequência se verifica, como é imposto (através da produção de dados ou documentos não genuínos), o bem jurídico – a intangibilidade de sistemas informáticos – encontra-se, desde logo, concreta e efetivamente lesado, produzindo-se o dano.

Por conseguinte, a mera falsificação *offline* não basta para a consumação deste crime. É necessário antes que de tal resulte a interferência "num sistema informático de dados", sendo este o núcleo interpretativo desta disposição, onde se pune "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...**".

Assim, acaba esta por se distinguir do crime de Falsificação de Documentos, presente no artigo 256.º do Código Penal. Neste último, como se referiu, estamos perante um crime de perigo[89] com a mera falsificação de documentos, se se entender como bem jurídico tutelado a segurança e a credibilidade do tráfego jurídico-probatório.

Porém, na alínea e) do referido artigo, já se contempla o uso dos documentos produzidos nessas condições, só neste caso se produzindo, em

---

[86] VENÂNCIO, Pedro – **Lei do Cibercrime: anotada e comentada**. Coimbra Editora, 2011.
[87] VERDELHO, Pedro – **Comentário à Lei 109/2009, de 15 de Setembro**. In ALBUQUERQUE, Paulo Pinto de (coord.) - **Comentário às Leis Penais Extravagantes**, pp. 505-523.
[88] Cfr., por exemplo, Acórdão do Tribunal da Relação do Porto, de 24–04–2013, processo n.º 585/11.6PAOVR.P1, disponível em www.dgsi.pt .
[89] Cfr. pp. 54 e ss.

princípio, o efetivo dano. Todavia, tal pode não chegar a acontecer caso, por exemplo, o documento falsificado não chegue a conseguir cumprir a função concreta a que se destinava quando quem o receber se aperceber da falsificação, reconhecendo o esquema. Para HELENA MONIZ, esta alínea só é de aplicar caso se trate do uso de um documento por pessoa distinta do que o falsificou, sendo esta uma espécie de norma independente dentro da primeira, havendo até quem ache que entre o crime de Falsificação e o de Uso de documento poderia falar-se num caso de concurso aparente de normas[90].

De facto, parece-nos óbvio que, para a generalidade dos casos (de uso de documento falso feito pela própria pessoa que o falsificou) a existência da alínea e) se torna desnecessária uma vez que já a própria falsificação constitui um crime consumado punido pelo mesmo tipo legal, verificando-se um caso de facto posterior não punível. Porém, parece que nem sempre assim será. Tal acontecerá numa situação em que certo indivíduo falsifica um documento apenas por prazer – e, portanto, desprovido da específica intenção requerida quanto ao tipo objetivo de "causar prejuízo a outra pessoa ou ao Estado, ou de obter para si ou para outra pessoa benefício ilegítimo" – e, tempos depois, relembrando-se da sua obra, decide utilizá-la. Ora, neste caso, haverá já a aplicação da alínea e) do artigo 256.º, ao contrário do que defendia a última opinião que mencionamos.

Já em relação ao tipo subjetivo do crime de Falsidade Informática, estamos perante de um crime doloso, na medida em que se requer o conhecimento e vontade de realização do tipo objetivo, não admitindo punição a título de negligência. Requerem-se também especiais intenções do agente: num primeiro momento, relativamente à intenção de provocar engano nas relações jurídicas; e, num segundo momento, quanto à intenção de que os documentos digitais produzidos pela falsificação sejam considerados para finalidades juridicamente relevantes como se dos verdadeiros se tratassem. Não entra agora expressamente em linha de conta a intenção de obter um benefício ilegítimo ou causar prejuízo como acontece no crime de Falsificação de Documentos do Código Penal. Mas parece que também esta intenção está inerente ao ato de falsificar informaticamente. Mesmo assim, tal como neste último, estamos perante um delito de intenção, na mesma medida do que foi acima dito para o crime de Falsificação de Documentos.

Por fim, o número 3 do artigo 3.º da Lei do Cibercrime, inspirado no artigo 6.º da Convenção de Budapeste, consagra um novo crime ao punir quem usar os documentos mencionados no artigo 3.º, n.º 1 (para causar prejuízo a alguém ou para obter um benefício ilegítimo.

Do mesmo modo, e no tocante ao número 3 do mesmo artigo que agora nos suscita dúvidas, vem o Acórdão do Tribunal da Relação do Porto de 24/04/2013[91] defender que, neste número, não se exige que o engano provocado se repercuta nas relações jurídicas, como acontece no caso do número 1, acrescentando que para o preenchimento do tipo de crime do n.º 3 do artigo 3.º o que é preciso é a intenção de causar prejuízo a outrem ou de obter um benefício ilegítimo, não sendo necessário, contudo, que o prejuízo ou vantagem tenham carácter patrimonial, uma vez que tal não é o bem jurídico objeto de proteção da norma.

[90] Cfr. CORREIA, Eduardo – **A Teoria do Concurso em Direito Criminal**. 2ª edição (reimpressão). Coimbra: Livraria Almedina, 1996.
[91] Cfr. Acórdão do TRP, de 24–04–2013, processo 585/11.6PAOVR.P1, disponível em www.dgsi.pt .

§ 5 Por conseguinte, em abstrato, quanto à criação de um *site* falsificado, apresentam-se como possibilidade de enquadramento o crime de Falsificação de Documentos, constante do artigo 256.º do Código Penal, e o crime de Falsidade Informática consagrado do artigo 3.º da Lei do Cibercrime.

Ora, poderia considerar-se estarmos perante um concurso meramente aparente ou de normas (segundo a terminologia de EDUARDO CORREIA) ou perante um caso de unidade de leis (segundo a perspetiva de FIGUEIREDO DIAS)[92], já que a concreta ação de criar uma página falsificada pareceria, em abstrato e formalmente, enquadrável em mais de uma norma incriminadora.

Porém, no caso em apreço, somos forçados a admitir que tal não acontece. De facto, a nível formal, olhando exclusivamente para o elemento gramatical dos tipos legais em questão, a conduta caberia, em abstrato, em qualquer um deles. Contudo, fazendo antes uma ponderação material, verificando a natureza diversa dos dois crimes e os distintos bem jurídicos em causa, concluímos que tal não poderá suceder.

Nesse sentido, quanto à natureza de ambos os tipos legais, deparamo-nos com o crime de Falsificação de Documentos, como um crime de perigo que tutela a segurança e credibilidade no tráfego jurídico-probatório; e com o crime de Falsidade Informática, como um crime de verdadeiro dano, em que, para a sua consumação, é necessária a efetiva lesão do bem jurídico tutelado, neste caso, a integridade de sistemas informáticos, que se dá com a interferência ilegítima em sistemas desse tipo.

Nessa medida, tal interferência não chega a existir aquando da mera produção de um cópia falsa de um *site*: a integridade de tal sistema mantém-se incólume; todavia, foi a segurança e credibilidade no tráfego jurídico-probatório colocada em perigo.

Ademais, está em causa um verdadeiro documento para efeitos jurídicos e probatórios, pois as páginas *online* ao representarem a marca que as detém, contribuem para garantir que a mesma é digna de confiança pela segurança e credibilidade que fornecem. Como já se teve ocasião de referir, e apesar de o tipo legal de Falsificação de Documentos não ter sido pensado para documentos de natureza informática, a verdade é que os mesmos têm o mesmo valor jurídico e probatório que os documentos escritos propriamente ditos, sendo equiparados por lei no artigo 3.º e 5.º do Decreto-lei 290-D/99, de 2 de Agosto.

Logo, se com um mero acesso ilegítimo se produz já um efetivo dano ao bem jurídico mencionado – como abordaremos *infra*[93] –, muito mais facilmente tal acontecerá com a falsificação de um documento informático, hipótese abrangida pelo tipo legal de Falsidade Informática onde, como já se destacou, se requer que por qualquer forma haja "a interferência num tratamento informático de dados", ou seja, uma intromissão propriamente dita num sistema informático.

Não é isto, todavia, o que sucede na situação concreta de que agora nos ocupamos, pois com a mera criação de uma página *online* falsificada não que consuma qualquer ingerência num sistema informático, permanecendo o mesmo intacto do ponto de vista da sua integridade.

É assim mesmo apesar de entre as duas normas poder parecer, à primeira vista, que se estabelece uma relação de especialidade. Não há, porém, qualquer caso de concurso aparente de normas como a seguir se discorrerá.

Numa observação menos atenta, o crime de Falsificação de Documentos constante do Código Penal parece realmente um tipo fundamental de crime – na

[92] Para clarificação de ambos os entendimentos, cfr. *infra* pp. 69 e ss., § 2 e 3.
[93] Cfr. p. 61, § 7.

terminologia de EDUARDO CORREIA –, pois aparenta estar já totalmente abrangido pelo crime de Falsidade Informática, contendo este último, adicionalmente, certos elementos especializadores que têm que ver com a ilicitude da conduta, mais especificamente, com o tipo de documentos objeto de falsificação (neste caso, documentos informáticos que, dados os seus contornos e particularidades, merecerão um tratamento específico).

No caso concreto tal relação não chega sequer a verificar-se, pelo facto de ambos os preceitos protegerem bens jurídicos distintos o que faz com que estes tenham naturezas também distintas (o crime de Falsificação de Documentos como crime de perigo e o crime de Falsidade Informática como crime de efetivo dano). Por isso, os dois tipos legais acabam por proteger âmbitos ou estádios distintos e, por isso, não haverá lugar para se recorrer ao princípio "*lex specialis derogat legi generalis*", ou seja, de que a norma especial prefere à norma geral, dado não haver qualquer concurso de normas como se referiu.

A haver alguma relação entre os mesmos, seria antes de subsidiariedade, segundo o parecer de FIGUEIREDO DIAS, ou de consumpção pura, no caso de se optar pelo entendimento do Professor EDUARDO CORREIA. [94]

Portanto, no que toca à criação de um *site* forjado pelo *pharmer,* concluímos pela recondução de tal conduta ao tipo legal de Falsificação de Documentos: quer porque aquando da mesma não há ainda qualquer intervenção em sistemas informáticos, como requer o tipo legal de Falsidade Informática constante da Lei do Cibercrime, que visa tutelar a intangibilidade de tais sistemas; quer porque, o crime de Falsificação de Documentos, sendo um crime de perigo, requer um atentado contra a função de garantia e de perpetuação de um documento – mesmo que informático –, facto que sucede na presente hipótese, que põe em causa a segurança do tráfego jurídico-probatório (bem jurídico tutelado com tal disposição legal), na medida em que um *website* constitui um documento que representa a instituição que o detém, visando assegurar a confiança e a credibilidade em tal entidade, nos moldes explicitados na mesma página.

[94] Cfr pp. 69 e ss., § 2 e 3.

2.2. Quando ao acesso não autorizado ao Servidor DNS ou ao *Host File*

§ 6 Vislumbra-se, também aqui, a existência de tutela normativa de diversas naturezas.

Do que agora se trata é do acesso puro e simples a um sistema informático pelo agente, através da violação das suas regras de segurança, para que depois lhe seja possível proceder às alterações que se mostrem necessárias à continuação do projeto criminoso – nomeadamente a alteração do nome de domínio com o consequente reencaminhamento do utilizador para o *website* forjado que a conversão de nomes adulterada passará a designar.

§ 7 Em primeiro lugar, há um enquadramento no âmbito da Lei do Cibercrime, nomeadamente o artigo 6.º, que consagra o crime de **Acesso Ilegítimo**.

Quanto ao tipo objetivo, pune-se quem acede – total ou parcialmente –, sem autorização e intencionalmente, a um qualquer sistema informático. Por isso, este é um crime formal ou de mera atividade já que a simples prática da ação descrita no ilícito-típico é condição suficiente para a consumação, isto é, o acesso não autorizado ao sistema informático.

Em relação ao bem jurídico tutelado com a incriminação, consideramos que está em causa acautelar a intangibilidade do sistema informático, propria a concretamente considerado: sua segurança, confidencialidade, integridade e disponibilidade. Parece-nos que se dá aqui destaque ao sistema informáticos no seu todo e não aos dados que o incorporam. É o que a letra deste artigo deixa transparecer: "Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro **titular do direito do sistema ou de parte dele**, de qualquer modo **aceder a um sistema informático**, (...).".

Mesmo quando, no seu número 3, se apresenta uma forma qualificada do mesmo crime – agravando-se a pena de prisão até três anos – "se o acesso for conseguido através da violação de regras de segurança" (o que, sem dúvida, acontece quanto ao *pharming*[95]), está-se mais uma vez a destacar a intocabilidade do sistema informático integralmente considerado. O conhecimento e utilização dos dados dele constantes é, assim, uma mera circunstância agravante já que o acesso pode ser meramente formal, não importando o efetivo conhecimento dos dados, mas apenas que os mesmos estejam na esfera de disponibilidade fáctica do agente.

Consequentemente, estamos perante um crime de dano já que o simples acesso é condição necessária e suficiente para lesar a intangibilidade do sistema informático alvo desta conduta. Por outro lado, a tentativa é também punível, segundo o número 5 do mesmo artigo.

Já no que toca ao tipo subjetivo, não se exigem especiais intenções do agente, bastando a verificação do simples dolo, ao contrário do que acontecia na redação do artigo correspondente na Lei da Criminalidade Informática, Lei 109/91[96], onde se exigia intenção de obter um benefício ou vantagem ilegítimos.

---

[95] Cfr. *supra* pp. 29 e ss.

[96] "**Artigo 7º - Acesso ilegítimo**
1- Quem, não estando para tanto autorizado e com a intenção de alcançar, para si ou para outrem, um benefício ou vantagem ilegítimos, de qualquer modo aceder a um sistema ou rede informáticos será punido com pena de prisão até 1 ano ou com pena de multa até 120 dias.
2- A pena será a de prisão até três anos ou multa se o acesso for conseguido através de violação de regras de segurança.
3- A pena será a de prisão de um a cinco anos quando:

Portanto, é um crime doloso, não admitindo punição a título de negligência, de acordo com a letra do artigo 6.º e a determinação do artigo 13.º do Código Penal.

Por último, no número 4 deste artigo, nas suas alíneas a) e b), procede-se a um novo agravamento da pena até cinco anos. No caso da alínea a), entende-se que há um perigo agravado pelo conhecimento de segredos comerciais ou industriais ou de outros dados confidenciais. Este conhecimento não é, em si mesmo, uma utilização dos dados a que se teve acesso, mas parece que o legislador entendeu que se justificava uma proteção como que antecipada por estarem em causa bens jurídicos de diferentes naturezas protegidos por outras disposições legais, como sejam a lealdade da concorrência ou outros bens jurídicos pessoais de extrema importância.

Já na alínea b), a agravação ocorre caso a vantagem patrimonial obtida com tal acesso seja de valor consideravelmente elevado o que, não raro, vem posteriormente a acontecer. Porém, este último aspeto não está isento de críticas, pois não se está já apenas no âmbito do simples acesso, mas sim no plano da utilização dos dados obtidos com o mesmo: para que tal agravação se possa aplicar é necessário que os dados obtidos por meio de um acesso ilegítimo tenham sido utilizados e, por isso, possibilitado a obtenção de vantagens patrimoniais consideráveis. Misturam-se, desde modo, planos de atuação bastante distintos.

§ 8 Também quanto ao mesmo aspeto perspetiva-se o enquadramento na Lei de Protecção de Dados Pessoais, Lei n.º 67/98, de 26 de Outubro, a qual confere tutela penal nesta matéria, se bem que de uma perspetiva de defesa de bens jurídicos de índole estritamente pessoal.

Tendo transposto para a ordem jurídica portuguesa a Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995 – referente à proteção quanto ao tratamento de dados pessoais e à livre circulação dos mesmos – e substituído a Lei n.º 10/91, de 29 de Abril, esta lei inspira-se, em larga medida, no nosso quadro constitucional , em particular no artigo 35.º da Constituição da República Portuguesa – que confere aos dados pessoais (constantes de ficheiros pessoais ou informatizados) diversas garantias de valor jusconstitucional (dada a sensibilidade e importância de que se revestem, ainda mais num contexto de livre circulação de dados a nível europeu). Por isso se justifica a necessidade de conferir dignidade penal às infrações decorrentes destes tratamentos e transmissões de dados.

Quanto a esta Lei, o artigo 44.º, consagrando o crime de **Acesso Indevido**, fornece, abstratamente, outra possibilidade de enquadramento quanto ao acesso não autorizado a sistemas informáticos. Esta norma inspirou-se diretamente no artigo 7.º[97] da Lei da Criminalidade Informática[98], substituído pelo atual artigo 6.º da Lei do Cibercrime[99].

---

a) Através do acesso, o agente tiver tomado conhecimento de segredo comercial ou industrial ou de dados confidenciais, protegidos por lei;
b) O benefício ou vantagem patrimonial obtidos forem de valor consideravelmente elevado.
4- A tentativa é punível.
5- Nos casos previstos nos nºs 1, 2 e 4 o procedimento penal depende de queixa."

[97] **Artigo 7º - Acesso ilegítimo**
1- Quem, não estando para tanto autorizado e com a intenção de alcançar, para si ou para outrem, um benefício ou vantagem ilegítimos, de qualquer modo aceder a um sistema ou rede informáticos será punido com pena de prisão até 1 ano ou com pena de multa até 120 dias.
2- A pena será a de prisão até três anos ou multa se o acesso for conseguido através de violação de regras de segurança.
3- A pena será a de prisão de um a cinco anos quando:
a) Através do acesso, o agente tiver tomado conhecimento de segredo comercial ou industrial ou de dados

No seu número 1, quanto ao tipo objetivo, pune-se com pena de prisão até um ano ou pena de multa até cento e vinte dias dias todo aquele que, sem autorização e por qualquer meio, acede a dados pessoais que lhe estão vedados. Já não está aqui em causa, como acontecia no artigo 6.º da Lei do Cibercrime, o acesso a um sistema informático, mas sim a dados pessoais individualmente considerados. Este acesso pode ser meramente formal, não importando o efetivo conhecimento, mas apenas que os dados estejam na esfera de disponibilidade fáctica do agente. Mais uma vez, tal como no crime de Acesso Ilegítimo, é este um crime formal ou de mera atividade.

Quanto ao bem jurídico alvo de proteção, o que se visa aqui são bens jurídicos eminentemente pessoais, como sejam a privacidade e confidencialidade em relação aos dados pessoais e o direito à autodeterminação informacional do titular dos dados que deve poder saber por quem são detidos os seus dados, para que fim e em que medida.

Neste sentido, é um crime de perigo porque com o acesso não autorizado que se requer neste artigo não se exige o efetivo conhecimento dos dados, bastando, por isso, a simples colocação em perigo do bem jurídico.

À semelhança deste do crime de Acesso Ilegítimo previsto na LC, também se procede a uma agravação da pena no caso da violação das regras de segurança (número 2), agravação esta que, no caso do *pharming*, sempre se aplicaria uma vez que existe "a violação de regras técnicas de segurança" (alínea a)).

Relativamente ao tipo subjetivo, exige-se o simples dolo e não especiais intenções do agente. Podem é algumas circunstâncias posteriores causar a agravação da medida abstrata da pena, como sejam a obtenção de vantagens patrimoniais que, não raro – e até, diríamos, na grande maioria das vezes – existem aquando da realização de um ataque de *pharming* (artigo 44.º, n.º 2, alínea c)) – já não sendo aqui necessário que tais vantagens sejam de valor consideravelmente elevado como acontecia no artigo 6.º da Lei do Cibercrime. Este aspeto merece, desta forma, a mesma crítica que dirigimos ao artigo 6.º, número 4, alínea b) da Lei do Cibercrime já que se excede o âmbito do acesso e se pressupõe a utilização dos dados a que se acedeu ilegitimamente.

É este, por conseguinte um crime doloso, não admitindo punição a título de negligência de acordo com a sua letra e a normas constantes, respectivamente, dos artigos 13.º e 23.º do Código Penal.

Porém, este artigo distingue-se do artigo 6.º da Lei do Cibercrime a que nos referimos em primeiro lugar. Tal parece acontecer sobretudo quanto ao objeto. No primeiro, aparece protegida a intangibilidade do sistema informático[100] e, neste último, protegem-se os dados em particular e sua confidencialidade. Desse modo, o artigo 44.º parece manter uma relação de especialidade com o artigo 6.º da Lei do Cibercrime: no artigo 44.º acautelam-se somente dados de carácter pessoal, enquanto que no artigo 6.º se protegem, em abstrato, todos os dados, de índole pessoal, comercial, industrial, etc., desde que constantes de sistemas informáticos. Para além disso, há uma proteção mais intensificada neste último artigo, parecendo operar aqui uma revogação

---

confidenciais, protegidos por lei;
b) O benefício ou vantagem patrimonial obtidos forem de valor consideravelmente elevado.
4- A tentativa é punível.
5- Nos casos previstos nos nºs 1, 2 e 4 o procedimento penal depende de queixa.
[98] Lei 109/91, de 17 de Agosto.
[99] Lei 109/2009, de 15 de Setembro.
[100] Cfr. Acórdão do Tribunal da Relação de Coimbra, de 15-10-2008, processo n.º 368/01.8TAFIG.C1, disponível em www.dgsi.pt.

tácita, pelo menos parcial, do artigo 44.º da Lei de Protecção de Dados Pessoais pelo artigo 6.º da Lei do Cibercrime, pois o primeiro parece esvaziado de utilidade prática por ser quase totalmente abrangido pelo artigo 6.º. Isto acontece porque, tendencialmente, todo o tratamento de dados pessoais se faz a partir de sistemas informáticos.

Assim, quanto a tratamentos de dados a partir de sistemas informáticos, os factos suscetíveis de preencher o crime do artigo 44.º da Lei 67/98, seriam também, em abstrato, subsumíveis ao artigo 6.º da Lei do Cibercrime[101], exceto quando o tratamento de dados pessoais fosse feito a partir de ficheiros não informatizados.

§ 9 Conclui-se, deste modo, que quanto ao acesso sem a permissão necessária ao Servidor DNS ou ao *Host File*, pelo que atrás se referiu, deverá prevalecer a punição no âmbito da Lei do Cibercrime quanto ao crime previsto de Acesso Ilegítimo, que nos parece mais adequado aos contornos referidos por melhor traduzir o desvalor a ser dirigido à conduta do agente, já que o verdadeiro e principal atentado se dá contra a intangibilidade do sistema informático implicado e não tanto contra os dados dele integrantes. Para além disso, podem não estar em causa apenas dados pessoais, mas também outro tipo de dados, não estando, assim, reunidos os pressupostos de aplicação do artigo 44.º da Lei de Protecção de Dados Pessoais por não estarmos perante um tratamento não informatizado de dados, dado que optamos pela existência de uma revogação tácita, ainda que parcial, deste artigo 44.º pelo artigo 6.º da Lei do Cibercrime.

Deste modo, esta parece-nos a forma mais adequada de resolver as presentes dúvidas de aplicação quanto às normas mencionadas.

[101] Crf. VERDELHO, Pedro – **Comentário à Lei 67/98, de 26 de Outubrro**. In ALBUQUERQUE, Paulo Pinto de (coord.) - **Comentário às Leis Penais Extravagantes**, pp. 446 – 10.

2.3. Quanto ao corrompimento dos dados do Servidor DNS ou do *Host File*

§ 10 Tal corrompimento traduz-se na alteração do nome de domínio de um *website*, mais comummente designado por *link*, que passa a corresponder ao *site* forjado previamente criado pelo agente de antemão e já não ao *site* original. Para tais condutas perspetivam-se diferentes âmbitos de incriminação.

Primeiramente, no que toca à Lei do Cibercrime várias são as disposições a ter em conta, nomeadamente o crime de **Falsidade Informática** já que são modificados os dados existentes e inseridos outros em sua substituição, com o intuito de "provocar engano nas relações jurídicas" e de serem "utilizados para finalidades juridicamente relevantes" tal como consta da configuração da própria norma do artigo 3.º da Lei do Cibercrime. Por isso, dir-se-á, quanto à análise desse tipo legal, o mesmo que foi referido quanto à criação de uma página *online* falsificada[102].

§ 11 Também o crime de **Dano relativo a programas ou outros dados informáticos**, que mais sucintamente designaremos por crime de **Dano Informático**, constante do artigo 4.º da Lei do Cibercrime, pode suscitar algumas dúvidas de aplicação neste âmbito. Todavia, deve concluir-se pela sua não aplicação.

Na verdade, este artigo 4.º corresponde ao antigo artigo 5.º da LCI[103] e visa conferir tutela penal às ações em que existe uma atuação não autorizada em relação a programas ou outros dados informáticos (como, por exemplo, para apagar, alterar, destruir, danificar, suprimir ou tornar não utilizáveis ou não acessíveis), havendo, assim, uma aproximação à legislação internacional na estruturação do tipo objetivo.

Por isso, relativamente ao tipo objetivo pune-se com pena de prisão até três anos ou com pena de multa quem, sem autorização, afetar a capacidade de uso de programas ou dados informáticos alheios através de uma das hipóteses anteriormente elencadas.

É este, por isso, um crime de resultado já que se pressupõe a verificação de um certo efeito, no caso, a destruição de dados ou programas informáticos alheios.

Aqui se inclui, por exemplo, a já falada propagação de *malware*[104] - especialmente no seu n.º 3 - ocorrendo uma antecipação da tutela penal, já que se pune a difusão, sem que seja necessária a produção de efeitos nocivos, incluindo-se aqui normalmente os atos preparatórios de outros crimes de dano.

O bem jurídico tutelado é, novamente, a intangibilidade dos sistemas informáticos, que está na base de toda a Lei do Cibercrime, como já referimos quanto ao crime de Falsidade Informática e de Acesso Ilegítimo.

---

[102] Cfr. *supra* pp. 54 e ss., § 4.

[103] **Artigo 5º - Dano relativo a dados ou programas informáticos**
1- Quem, sem para tanto estar autorizado, e atuando com intenção de causar prejuízo a outrem ou de obter um benefício ilegítimo para si ou para terceiros, apagar, destruir, no todo ou em parte, danificar, suprimir ou tornar não utilizáveis dados ou programas informáticos alheios ou, por qualquer forma, lhes afetar a capacidade de uso será punido com a pena de prisão até três anos ou pena de multa.
2- A tentativa é punível.
3- Se o dano causado for de valor elevado, a pena será a de prisão até 5 anos ou de multa até 600 dias.
4- Se o dano causado for de valor consideravelmente elevado, a pena será a de prisão de 1 a 10 anos.
5- Nos casos previstos nos nºs 1, 2 e 3 o procedimento penal depende da queixa.

[104] Cfr. *supra* p. 21, § 4 e nota de rodapé n.º 6.

Por conseguinte, estamos perante um crime de dano já que com o preenchimento dos elementos pressupostos pelo tipo objetivo o bem jurídico acautelado é imediatamente lesado.

No que toca ao tipo subjetivo, o crime de Dano Informático é doloso, não se exigindo especiais intenções do agente.

Por tudo isto, e apesar da aparente semelhança terminológica, este crime distingue-se bem do crime de Falsidade Informática.

A consagração deste crime tem por base o crime de Dano constante do artigo 212.º do Código Penal. Desse modo, o que se pune é a destruição pura e simples de coisa alheia e, no caso, de sistemas informáticos e dados dele integrantes para impedir o normal uso, embora, ainda assim, o sistema mantenha o funcionamento, ainda que deficiente (o que não acontece na Sabotagem Informática).

Tal como no crime de Dano do Código Penal, o que se pretende é condicionar o uso, não entrando em consideração intenções enganosas. Da mesma forma que prescreve o artigo 212.º do Código Penal, o que se pretende é "desfigurar ou tornar não utilizável coisa alheia", com a particularidade de no Dano Informático a coisa não ter natureza física, mas sim incorpórea, ou seja, ser um sistema informático. Portanto, aqui a intenção esgota-se na produção como que de um efeito incómodo, consequente da destruição ou da imposição de uma utilização condicionada e não perfeita de coisa alheia pelo agente que não passará despercebida à própria vítima.

Ora, tal não acontece quanto ao *pharming* já que há apenas uma modificação de dados (matéria abrangida pelo crime de Falsidade Informática) e não a sua destruição ou inutilização. Os danos provocados com tais condutas, a existirem, serão consumidos por serem meros actos preparatórios.

Por conseguinte, no crime de Falsidade Informática exige-se, para além do dolo, especiais intenções do agente em provocar engano e de que o documento falso seja considerado para finalidades juridicamente relevantes em substituição do autêntico, sem que de tal a vítima possa suspeitar, pois isso impediria a utilização do sistema forjado como verdadeiro, essencial objetivo do *pharmer*.

Ora, por tudo o que foi dito e também como tal exigência de provocar engano não está presente no crime de Dano Informático, embora seja essencial para caracterizar a conduta em questão, o crime de Dano Informático não é, no nosso caso, aplicável.

§ 12 Consideramos ainda que, quanto a este aspeto, o *pharming* não é enquadrável nos contornos do artigo 5.º da Lei do Cibercrime, relativo ao crime de **Sabotagem Informática**, embora a sua formulação possa, num primeiro momento, causar essa impressão.

Do seu tipo objetivo fazem parte as condutas em que o agente, sem permissão legal, perturba ou impede o funcionamento de um sistema informático através da introdução, transmissão, deterioração, danificação, alteração, apagamento, impedimento de acesso ou supressão de programas ou outros dados informáticos. Estas ações são punidas com pena de prisão até cinco anos ou pena de multa até seiscentos dias. É, portanto, um crime de resultado, traduzindo-se, este último, no impedimento ao normal funcionamento do sistema.

O bem jurídico acautelado é, da mesma forma – e neste caso mais evidentemente –, a intangibilidade do sistema informático globalmente considerado. Nessa medida, estamos perante um crime de dano, pois com a

interferência num sistema informático já foi o bem jurídico plenamente posto em causa.

Por fim, quanto ao tipo subjetivo, deparamo-nos com um crime doloso, onde não se faz qualquer referência a especiais intenções do agente, mas em que está implícito o simples dolo como conhecimento e vontade de realização do tipo objetivo.

Nessa medida, o caso concreto não se poderá subsumir a este ilícito-típico porque no crime de Sabotagem Informática está em causa a integridade de um sistema informático na sua globalidade, atendendo aos interesses do proprietário e dos utentes, nos casos em que há uma interferência no mesmo que causa uma perturbação no seu funcionamento. Ao contrário do crime de Dano Informático, aqui o objetivo do agente é impedir o funcionamento do sistema propriamente dito para que este não realize as funções que lhe são características. Um exemplo é o ataque DoS ou DDoS[105] a que já nos referimos anteriormente.

Ora, no caso do *pharming*, os sistemas informáticos em questão permanecem totalmente funcionáveis, são apenas os dados neles constantes que são alvo da ação criminosa. Aliás, o criminoso, para perfeição do seu objetivo, espera calorosamente que o sistema informático mantenha o seu funcionamento.

De referir ainda que, no n.º 2 do artigo 5.º da Lei do Cibercrime, há, novamente, uma antecipação da tutela penal, aí se enquadrando a já mencionada distribuição de *botnets*[106].

§ 13 Em segundo lugar, a Lei de Protecção de Dados Pessoais parece conferir igualmente tutela penal a este nível, em especial no seu artigo 45.º onde se consagra o crime de **Viciação ou Destruição de Dados Pessoais**. Todavia, será também de concluir pela sua não aplicação.

Do tipo objetivo fazem parte as ações que se traduzam em apagar, destruir, danificar, suprimir ou modificar dados pessoais, de forma a torná-los inutilizáveis ou afetando a sua capacidade de uso. Assim, estamos perante um crime material ou de resultado.

Para além disso, o bem jurídico a acautelar com esta norma é a integridade e a fiabilidade dos dados pessoais. Nessa medida, é este um crime de dano já que com a viciação ou destruição propriamente dita o bem jurídico já se encontra lesado.

Quanto ao tipo subjetivo, estamos perante um crime doloso, sendo indiferente a intenção de causar prejuízo ou obter benefício ilegítimo, bastando, por isso, o simples dolo, dirigido aos actos materiais que compõem o tipo objetivo.

Deste modo, este crime, pela particularidade do seu objeto (os dados pessoais), mantém com o crime de Dano Informático da Lei do Cibercrime uma relação de exclusão ou alternatividade.

Quanto à alteração dos dados constantes do Servidor DNS ou do *Host File* a que nos estamos agora a referir, estará em causa a modificação dos dados para afetar a sua capacidade de uso e não a sua destruição e inutilização como anteriormente referimos.

Por tal, pelo mesmo motivo apontado quanto ao crime de Dano Informático consagrado na Lei do Cibercrime, concluímos que este também não deverá aplicar-se para punir o corrompimento de dados constantes de sistemas

[105] Cfr. *supra* página 20, nota de rodapé n.º 7.
[106] Cfr. *supra* página 19, nota de rodapé n.º 6.

informáticos como o Servidor DNS e o *Host File* uma vez que o tipo objetivo não é sequer preenchido.

§ 14 Por todas as conclusões anteriormente avançadas parece que deverá optar-se pela aplicação do artigo relativo ao crime de Falsidade Informática, dada a total amplitude desta fase, já que o comportamento do agente não se esgota na alteração de dados pessoais, mas antes inclui uma intenção de que esses dados provoquem engano, passando a desempenhar a função dos verdadeiros, e que, ao mesmo tempo, lhe permitam obter uma certa vantagem.

Assim, o desvalor presente na norma que consagra o crime de Falsidade Informática é o que melhor se adequa ao desvalor que deve ser dirigido à atuação concreta do agente.

Isto coaduna-se com o entendimento do crime de Falsidade Informática como um crime de dano, pois no caso em apreço, com a adulteração dos dados do Servidor DNS ou do *Host File* que passam a substituir os confiáveis perante os utilizadores que pretendem aceder ao *website* atacado, a interferência no sistema informático consumou-se como é imposto pela letra do artigo 3.º da Lei do Cibercrime. Desta forma, é a intangibilidade de tal sistema imediatamente lesada, verificando-se ainda a intenção de provocar engano, ou seja, de que tais dados sejam considerados para finalidades juridicamente relevantes, como se dos verdadeiros se tratassem, sendo tal intenção essencial para caracterizar a referida conduta.

Parece-nos, portanto, que tal conclusão é a que melhor se ajusta à mencionada conduta pelas particularidades descritas.

CAPÍTILO III - Obtenção, *strictu sensu*, de dados pessoais: concurso de crimes

§ 1 Após concluir todas as ações anteriormente referidas, o agente consegue alcançar o seu (primeiro) fulcral intento: acedendo ao Servidor DNS ou *Host File* e depois de alterar os seus dados, convence com facilidade o utilizador-vítima que, tentando depois aceder ao falso serviço *online*, envia os seus dados para o criminoso.

Todo o esforço inicial destina-se exclusivamente à concretização deste objetivo, que permitirá posteriormente atingir outro(s) verdadeiramente prioritário(s) e que sem estes dados seria(m) de quase impossível conquista (pelo menos por estas vias).

Como bem se percebe, já se acumularam, por esta altura, várias normas que punem, em abstrato, as mencionadas condutas: um crime de Falsificação de Documentos (presente no artigo 256.º do Código Penal), quanto à criação de um *website* forjado[107]; um crime de Acesso Ilegítimo (constante do artigo 6º da Lei do Cibercrime), quanto ao acesso não autorizado ao Servidor DNS ou ao *Host File*[108]; e um crime de Falsidade Informática (consagrado no artigo 3.º da Lei do Cibercrime), quanto à modificação dos dados constantes de sistemas informáticos[109], com vista à criação de um estado de erro.

Neste sentido, para concluir a análise deste primeiro momento, é necessário perceber qual a punição a final. Para tal, há que averiguar se estamos perante um concurso real ou meramente aparente entre as referidas disposições. Porém, quanto a essa problemática, não encontramos uma abordagem unívoca e unânime, perspetivando-se, essencialmente, duas doutrinas. A tradicional, de EDUARDO CORREIA, e uma mais recente de FIGUEIREDO DIAS, que passaremos sumariamente a analisar para que possamos depois tirar as conclusões desejadas.

§ 2 Para EDUARDO CORREIA, há um concurso efetivo ou real quando estamos perante uma pluralidade de infrações cometidas pelo mesmo agente antes de qualquer delas ter sido objeto de uma sentença transitada em julgado. E, nesse sentido, para se averiguar se estamos perante o cometimento de um ou mais crimes, este autor propõe que o número de infrações "determinar-se-á pelo número de valorações que, no mundo jurídico-criminal, correspondem a uma certa atividade"[110].

Ainda para o mesmo autor, o concurso aparente corresponderia então a um mero concurso de normas, pois a simples análise abstrata dos tipos legais de crime em conflito permitiria concluir acerca da norma a aplicar em definitivo, independentemente dos contornos concretos do caso. Entre as relações que se podem estabelecer de forma aparente entre as diversas normas contam-se a de especialidade, consumpção – pura e impura –, subsidiariedade e alternatividade.

A relação de especialidade existe, para o referido autor, quando, entre dois preceitos, um funciona como tipo fundamental e o outro ou outros enquanto norma que, para além de abranger o tipo fundamental, contém certos

---

[107] Cfr. *supra* pp. 59 e ss.
[108] Cfr. *supra* pp. 64 e ss.
[109] Cfr. *supra* pp. 68 e ss.
[110] CORREIA – Eduardo: **Direito Criminal: Volume II** (com colaboração de Figueiredo Dias). Almedina, 2010: §10 / 35.

elementos especializadores. Neste caso, preferir-se-á, naturalmente, a lei especial.

Haverá também casos em que uma norma poderá já conter outra, protegendo-se, em ambas as disposições, os mesmos valores. Ao contrário da especialidade, só em concreto se poderia afirmar estar-se perante este caso, designado por relação de consumpção (pura), no qual a norma que consome derroga a consumida.

Por outro lado, falar-se-á antes de uma consumpção impura sempre que da aplicação da norma que consome resulte uma menor proteção do bem jurídico pela pena aí prescrita ser inferior à da norma consumida. Nesse caso, aplicar-se-á a pena da norma consumida como forma de correção da lei. EDUARDO CORREIA chega até a referir-se a este mecanismo como a "válvula de segurança de todo o sistema do concurso aparente".

Fala também ainda na relação de alternatividade quando estamos perante duas normas que, quanto à proteção do mesmo bem jurídico, são meios distintos para alcançar um mesmo fim, embora os seus elementos constitutivos sejam incompatíveis.

Por fim, ainda uma relação de subsidiariedade: expressa, quando certos preceitos condicionam expressamente a sua eficácia ao facto de outros não se aplicarem; ou tácita, englobando aquelas relações cuja eficácia se apoia numa relação lógica entre as normas criminais.

Apesar de distinguir estas relações entre normas, EDUARDO CORREIA acaba por excluir a de subsidiariedade e a e alternatividade. Isto acontece pois no que toca à subsidiariedade expressa, ela nada adianta à problemática do concurso e a tácita porque vem a coincidir com a princípio da consumpção. Já quanto à relação de alternatividade, admite o autor que se bem que ela possa ajudar à interpretação das normas, não pode atuar como fator de exclusão das normas que, isoladamente consideradas, são efetivamente infringidas, embora seja só este o problema do concurso.

Fica, então, a doutrina do concurso aparente de EDUARDO CORREIA circunscrita às relações de especialidade e consumpção – pura e impura.

§ 3 Para FIGUEIREDO DIAS, o concurso efetivo define-se pela existência de uma pluralidade de sentidos sociais autónomos de ilícitos-típicos cometidos, de normas típicas concretamente aplicáveis que, para efeitos de punição, devem ser integralmente valorados.

Por outro lado, fala-se antes de um concurso aparente quando ocorre um concurso de ilícitos que, face à situação concreta, se podem sobrepor total ou parcialmente. Este Professor abandona o critério baseado na unidade ou pluralidade de tipos legais violados ou de unidade e pluralidade de ações praticadas pela agente, substituindo-os pelo critério da unidade ou pluralidade de sentidos sociais de ilicitude jurídico-penal do comportamento global.

Logo, a unidade ou pluralidade de infrações deixa de ser uma unidade ou pluralidade de crimes e passa a ser uma unidade ou pluralidade de factos puníveis: é a "unidade ou pluralidade de sentidos de ilicitude típica, existente no comportamento global do agente submetido à cognição do tribunal, que decide em definitivo da unidade ou pluralidade de factos puníveis e, nesta aceção, de crimes."[111]

[111] DIAS, Figueiredo – **Direito Penal: Parte Geral, Tomo I**. Coimbra: Coimbra Editora, 2007: 41 / § 26.

O concurso aparente caracteriza-se, assim, pela existência de um único sentido autónomo de ilicitude a que corresponde uma unidade fundamental de sentido dos concretos ilícitos-típicos praticados.

Por conseguinte, o concurso aparente, nos contornos apresentados, pouco que tem que ver com a velha forma de entendimento. De acordo até com a interpretação do Supremo Tribunal de Justiça[112], esta nova figura parece tão só abarcar os casos tradicionais de consumpção. Já os casos de concurso aparente por especialidade e subsidiariedade passam a integrar a simples "concorrência de normas" que, pela simples interpretação das normas em questão se resolveria.

Quanto ao que este autor considera como concorrência de normas, a relação de especialidade e de subsidiariedade são entendidas de forma semelhante à doutrina de EDUARDO CORREIA. De destacar o entendimento da subsidiariedade implícita para FIGUEIREDO DIAS, como a relação entre tipos legais abrangentes de factos que representam "estádios evolutivos, antecipados ou intermédios, de um crime consumado; ou como formas menos intensas de agressão ao mesmo bem jurídico"[113].

São as hipóteses de consumpção que se integram, de acordo com esta interpretação doutrinal, no verdadeiro concurso aparente. Este engloba, por isso, os casos em que o "conteúdo do ilícito-típico inclui em regra o de outro facto, de tal modo que, em perspetiva jurídico-normativa, a condenação pelo ilícito-típico mais grave exprime já de forma bastante o desvalor de todo o comportamento: *lex consumens derogat legi consuntae*"[114]. Ora, neste caso trata-se de uma pluralidade de normas concretamente aplicáveis e não de um caso de unidade de leis, pois há uma unidade do sentido social de ilicitude do facto punível porque "os sentidos singulares de ilicitude típica presentes no comportamento global se conexionam, se intercessionam ou parcialmente se cobrem, de forma tal que, em definitivo, se deve concluir que aquele comportamento é dominado por um único sentido de desvalor jurídico-social"[115].

Os critérios para a determinação do sentido de ilicitude absolutamente dominante são, segundo FIGUEIREDO DIAS, diversos: critério da unidade de sentido do acontecimento ilícito global-final; critério do crime instrumental ou crime-meio; critério da unidade de desígnio criminoso; critério da conexão espácio-temporal das realizações típicas, e critério dos diferentes estádios de evolução ou de intensidade da realização global.

Por isso, de acordo com esta posição, apenas em face da situação concreta poderemos saber se o ilícito dominado constitui ou não uma conduta que se integre numa "unidade do sucesso ou acontecimento" em que o agente se serve de meios já em si puníveis ou se integre numa unidade de desígnio criminoso.

Apesar da distinção, quer o concurso real quer o concurso aparente se reconduzem ao artigo 30.º do Código Penal, mas o artigo 77.º, ainda na opinião deste autor, é apenas aplicável ao concurso real.

§ 4 Antes de se dar uma resposta definitiva à questão do concurso na primeira fase da nossa hipótese de estudo, é importante atentar em algumas considerações prévias que condicionarão a conclusão.

---

[112] Acórdão Supremo Tribunal de Justiça, de 30–10–2014, processo n.º 32/13.9JDLSB.E1.S1, disponível em www.dgsi.pt.
[113] DIAS, Figueiredo – **Direito Penal: Parte Geral, Tomo I**. Coimbra: Coimbra Editora, 2007: 42 / §15.
[114] DIAS, Figueiredo – **Direito Penal: Parte Geral, Tomo I**. Coimbra: Coimbra Editora, 2007: 42 / §18.
[115] DIAS, Figueiredo – **Direito Penal: Parte Geral, Tomo I**. Coimbra: Coimbra Editora, 2007: 43 / §11.

Em primeiro lugar, importa destacar que estamos perante crimes de diversas naturezas: um crime de Falsificação de Documentos, enquanto crime de perigo; um crime de Falsidade Informática, enquanto crime de dano; e um crime de Acesso Ilegítimo como crime de dano. Nos dois últimos tipos legais o bem jurídico tutelado é o mesmo: a intangibilidade dos sistemas informáticos globalmente considerados. Já no crime de Falsificação de Documentos, como concluímos anteriormente, protege-se a segurança e credibilidade do tráfego jurídico-probatório.

Também a pena estabelecida em ambos os preceitos é bastante distinta. No crime de Falsidade Informática está em causa pena de prisão até cinco anos ou pena de multa de cento e vinte a seiscentos dias. Já no crime de Acesso Ilegítimo é aplicável pena de prisão até um ano e pena de multa até cento e vinte dias. A pena, porém, neste último caso, pode ser agravada até cinco anos no caso do número 4 do artigo 6.º da Lei do Cibercrime, aproximando-se, assim, do crime de Falsidade Informática. Por último, no crime de Falsificação de Documentos estabelece-se uma incriminação de três anos de pena de prisão ou pena de multa.

Portanto, parece-nos que enquanto no crime de Acesso Ilegítimo e no crime de Falsidade Informática o desvalor central reside no resultado alcançado – já que ambos são crimes de dano –, no crime de Falsificação de Documentos a reprovação se dirige principalmente à ação em si praticada, aos meios de que o criminoso de serve para provocar o erro, essencial à prossecução dos seus intentos. Há, ao invés, um desvalor de ação neste último caso.

Por tudo isto, e quanto à intangibilidade de sistemas informáticos enquanto bem jurídico, parece que este se encontra mais protegido com o crime de Falsidade Informática.

Por outro lado, é essencial analisar a intenção do agente com a prática de tais condutas. De facto, o objetivo fundamental nesta primeira fase é provocar o erro, já que é com base no mesmo que o agente conseguirá, mais tarde, realizar o seu verdadeiro intento, ou seja, obter dados alheios. Este erro é, portanto, criado com base na falsificação do *site* e, depois, com a alteração do nome de domínio.

No caso da Falsificação de Documentos, a falsificação do *site* original não requer a prática de qualquer outro crime para a perfeição da resolução criminosa, pois o agente para o copiar basta ter acesso à sua visualização pelos meios permitidos a qualquer utilizador.

Já no último caso – com a adulteração do nome de domínio – o acesso ao sistema que lhe está vedado é mero instrumento para realização desse fim: o crime de Falsidade Informática é o crime-fim e o crime de Acesso Ilegítimo é o crime instrumental ou crime-meio, isto apesar de o primeiro não ser um crime complexo e, nessa medida, não implicar o preenchimento de outro tipo legal para a sua consumação.

§ 5 Assim, entre o crime de Acesso Ilegítimo e o crime de Falsidade Informática para alteração do nome de domínio (constante do Servidor DNS ou do *Host Filei)*, parece de concluir que estamos perante um caso de concurso aparente pelo critério do crime-meio proposto por FIGUEIREDO DIAS. Isto acontece porque existe um único sentido autónomo de ilicitude: a condenação pelo crime de Falsidade Informática exprime já de forma bastante o desvalor de todo o comportamento.

Como o crime de Acesso Ilegítimo é puramente instrumental, já que utilizado unicamente como forma de alcançar o verdadeiro intento criminoso, o

crime de Falsidade Informática, uma vez que traduz o sentido de ilícito dominante, traduzido na criação de um estado de erro, acaba por absorvê-lo: *lex consumens derogat legi consuntae*.

Por conseguinte, podemos dizer de forma geral que quando o crime de Acesso Ilegítimo é usado exclusivamente para consumar o crime de Falsidade Informática, este último consome o primeiro ocorrendo um concurso meramente aparente. Mas se o acesso indevido ultrapassa a medida necessária à efetiva criação de um estado de erro estaremos já perante um concurso real.

Nesse sentido, por exemplo, se A acede a um sistema informático que lhe está vedado e com tal ataque apenas altera o nome de domínio do *site* de que pretende futuramente obter vantagem com a consumação de um ataque de *pharming*, ocorre um caso de concurso aparente pois o acesso é mero instrumento para perpetrar a falsificação. O crime de Falsidade Informática absorveria o de Acesso Ilegítimo, sendo o agente apenas punido a esse título.

Por outro lado, se A acede ilegitimamente a um sistema informático com o intuito de falsificar o nome de domínio, mas aproveita tal acesso para tomar conhecimento de dados confidenciais que lhe permitem obter segredos comerciais, industriais ou outros, estaremos perante um concurso real já que o acesso excederia, nesta hipótese, o necessário para consumar a falsificação.

Nesse sentido, perante este último caso, poderá estar em causa a aplicação de certos tipos legais que contendem com a proteção de bens jurídicos de carácter pessoal e que visam conferir proteção legal contra tal tipo de acesso indevido a informações pessoais e privadas[116].

Adicionalmente, como o bem jurídico tutelado é igual, mesmo ocorrendo um concurso aparente o bem jurídico continua plenamente tutelado com a aplicação exclusiva do tipo legal de Falsidade Informática até porque este contém uma proteção mais reforçada do que o crime de Acesso Ilegítimo, como já mencionamos.

Pode falar-se ainda numa unidade de desígnio criminoso e uma conexão espácio-temporal mesmo que este seja um critério com valor meramente residual para reforçar a nossa conclusão.

§ 6 Pela doutrina de EDUARDO CORREIA, a solução seria a mesma já que o crime de Acesso Ilegítimo é consumido pelo crime de Falsidade Informática, verificando-se um caso de consumpção pura pelas mesma razões que avançamos anteriormente, ou seja, pela instrumentalidade do primeiro em relação ao segundo, exprimindo este último já o desvalor adequado à conduta do agente.

§ 7 Resta saber qual a solução a dar relativamente à relação existente entre o crime de Falsidade Informática e o crime de Falsificação de Documentos que se consuma aquando da criação de uma página forjada, semelhante ao *site* de que se pretende obter vantagem.

Mais uma vez, importará a intenção e o projeto criminoso do agente.

Assim, a criação de um estado de erro – verdadeiro intento e essencial para a obtenção dos dados da vítima – através da falsificação do nome de domínio, só faz sentido quando exista de antemão um *site* falsificado para substituir e fazer corresponder ao original. Logo, conclui-se que há aqui uma unidade de desígnio criminoso que apenas se torna possível pela união perfeita dos dois mecanismos.

[116] Cfr. pp. 62 e ss.

Na realidade, a criação do erro é uma espécie de resultado que se obtém exclusivamente pela soma destes dois fatores: nome de domínio adulterado + *site* falsificado, que apenas juntos conseguem obter a reação desejada, formando, assim, uma espécie de simbiose. Tal reação consiste na criação de um estado de erro no utilizador-vítima que o leva a utilizar o sistema forjado como se do verdadeiro se tratasse e, com isso, sem que de tal possa ter consciência, possibilitar ao agente a obtenção dos seus dados pessoais. E isto apesar de entre a realização das duas condutas poder mediar bastante tempo, pois, como se sabe, este é um critério meramente indicativo.

Por isso, optamos pela via da existência de um concurso aparente no qual o agente deverá ser punido apenas por um crime de Falsidade Informática devido à unidade do seu desígnio criminoso. De facto, estamos perante uma unidade de sentido social autónomo: há uma unidade de sentido de ilicitude-típica.

§ 8 Também no âmbito da doutrina de EDUARDO CORREIA se obteria a mesma conclusão, ou seja, a existência de um concurso aparente que culminaria com a punição única por um crime de Falsidade Informática já que, em concreto, o projeto criminoso mostra a unidade de desvalor a atribuir a toda a conduta: verifica-se, assim, uma relação de consumpção pura.

§ 9 Por isso, concluindo a análise desta primeira fase constituinte do ataque de *pharming*, entendemos que a punição em concreto se deve fazer pela aplicação única e exclusiva do artigo 3.º da Lei do Cibercrime que consagra o crime de Falsidade Informática, por este exprimir suficientemente a censura a ser dirigida ao comportamento global do agente por todo o rol de motivos anteriormente expostos.

CAPÍTILO IV - Quanto à utilização dos dados obtidos ilegitimamente

§ 1 A obtenção de dados pessoais sensíveis pelo agente não é a finalidade última que preside ao projeto criminoso do *pharmer*, pois este quando leva a cabo um ataque de *pharming*, quer sempre (ou, pelo menos, quase sempre) utilizar esses dados para satisfazer interesses maiores.

Esses dados vão, por isso, servir para a prática de outros crimes, podendo estes, por conseguinte, lesar bens jurídicos de índole pessoal ou patrimonial.

Nesse sentido, a análise que se segue absorverá essa dicotomia, já que examinaremos primeiramente, a título sumário e meramente exemplificativo, os tipos legais que podem estar em causa aquando da prática de condutas que contendem com a lesão de bens jurídicos não patrimoniais, para depois prosseguir – e aí de forma mais exaustiva e pormenorizada, dado ser este, em específico, o tema que aqui nos trouxe – para o estudo dos tipos legais implicados com a lesão de bens jurídicos patrimoniais, por serem estes, de facto, chamados a intervir na maioria da vezes.

4.1. Quanto à lesão de bens jurídicos não patrimoniais

§ 2 De facto, vários são os tipos legais que podem ser preenchidos e que contendem com a colocação em causa de bens jurídicos não patrimoniais, como sejam a liberdade pessoal, a honra, a reserva da vida privada, etc.

Assim, após ter em sua posse os dados pessoais das vítimas que podem ter natureza diversa, o *pharmer*, poderá cometer vários crimes, dependendo das finalidades que estão na base da sua conduta.

A) Crimes contra a liberdade pessoal

§ 3 Depois de deter os dados pessoais de várias pessoas segundo os métodos a que anteriormente nos referimos, pode o agente, A, intencionalmente ou sem que de tal tenha consciência, verificar que no rol dessas vítimas está B, com o qual sempre manteve más relações. Por tal, e detendo informações relevantes para o efeito, ameaça B com a prática de um crime de forma a provocar-lhe medo ou inquietação, o que facilmente conseguirá provando que detém o controlo sobre dados que lhe respeitam e de carácter tão sensível.

Desta forma, estará aqui em causa a prática de um crime de **Ameaça**, constante do artigo 153.º do CP.

Quanto ao tipo objetivo, é necessário que se trate de uma ameaça relativa a um mal (que tem de configurar um facto ilícito típico, de natureza pessoal ou patrimonial), futuro, cuja ocorrência dependa da vontade do agente.

O crime objeto da ameaça, segundo o n.º 1 do artigo 153.º, tem de ser um crime "contra a vida, a integridade física, a liberdade pessoal, a liberdade e a autodeterminação sexual ou bens patrimoniais de considerável valor".

O sujeito passivo do crime de Ameaça é o destinatário da ameaça, que se distingue da pessoa objeto do crime ameaçado que podem não coincidir, devendo contudo estar, para com o ameaçado, numa relação de proximidade existencial.

No que toca ao bem jurídico, protege-se nesta disposição a liberdade de decisão e de ação já que as ameaças, ao provocarem um sentimento de insegurança, afetam a paz individual que é condição essencial para uma verdadeira liberdade.

Na medida em que se requer que a ameaça seja adequada a provocar o erro ou inquietação, estamos perante um crime material ou de resultado – relativamente ao objeto da ação, para que haja a consumação do crime – e de perigo concreto, já que parece só haver uma ameaça relevante quando esta, concretamente, representa uma efetiva ameaça para o bem jurídico[117].

Quanto ao tipo subjetivo, trata-se de um crime doloso que requer apenas a representação e conformação da adequação da ameaça a provocar a intranquilidade, sendo irrelevante que o agente pretenda ou não concretizar a ameaça.

A lei estabelece, como medida da pena, pena de prisão até um ano ou pena de multa até cento e vinte dias, dependendo o correspondente procedimento criminal de queixa nos termos do número 2 do artigo 153.º.

§ 4 Pode, por outro lado, o agente usar as mesmas ameaças referidas anteriormente, mas com o intuito de conformar a atuação da vítima num certo

[117] Cfr. CARVALHO, Américo Taipa de – **Comentário Conimbricense ao Código Penal,** (artigo 153.º, § 25).

sentido, ou seja, levá-la a praticar ou omitir certa ação ou a suportar uma atividade.

Se A se dirige a B e lhe exige determinada ação ou omissão ou que suporte certa atividade, ameaçando-o com a divulgação de fotografias ou outro tipo de informações a que teve acesso com a obtenção indevida de dados pessoais, há a prática de um crime de **Coacção**, constante do artigo 154.º do Código Penal.

Por isso, no que toca ao tipo objetivo, é necessário que, por meio de violência ou da formulação de uma ameaça, se vise constranger outra pessoa a um determinado comportamento, não sendo necessário que tal ameaça configure um ilícito-típico (ao contrário do que acontecia no crime de Ameaça), bastando a ameaça com um mal importante ou a violência. Nesse sentido, trata-se de num crime de execução vinculada.

Por conseguinte, o bem jurídico tutelado com tal norma é também a liberdade pessoal, nomeadamente a liberdade de decisão e de acção.

Já que se exige a consumação, ou seja, que se chegue a "constranger outra pessoa", o crime de Coacção é um crime de resultado.

Por último, quanto ao tipo subjetivo, é este um crime que exige o dolo, no sentido em que o agente tem de ter consciência de que a violência ou a ameaça que exerce é apta a constranger e que com tal se conforme.

Contudo, o facto não é punível se a utilização do meio para atingir o fim visado não for censurável (artigo 154.º, n.º3, alínea a).

Apesar de poder existir um concurso aparente entre este crime e o de Ameaça, este último cederá perante o primeiro[118].

Este crime é punido com pena de prisão até três anos ou com pena de multa, dependendo o procedimento criminal de queixa.

B) Crimes contra a honra

§ 5 Com o artigo 180.º do Código Penal, inicia-se o capítulo dos crimes contra a honra, alvo de tutela na nossa Constituição, no seu artigo 26.º.

No referido artigo 180.º do Código Penal português, consagra-se o crime de Difamação que pode também ser convocado a intervir na problemática que aqui nos traz.

De facto, se A – que obteve, numa primeira fase de um ataque de *pharming*, dados pessoais com os quais poderá aceder facilmente a contas de *e-mail*, *Facebook*, bancos, etc., das vítimas –, com base nos dados a que teve acesso e disso se aproveitando, dirige-se a terceiro, ofendendo B, imputando-lhe factos ou formulando outro tipo de juízos desvaliosos, estamos perante a prática de um crime de **Difamação**.

Podem também estas ofensas ou juízos desvaliosos se concretizarem sem a intervenção de um terceiro, isto é, diretamente perante a vítima. Nesse caso, estaremos já num caso de preenchimento do tipo legal de **Injúria**, constante do artigo 181.º do CP.

Como se bem entende, em ambos os casos, é a honra o bem jurídico tutelado, embora existam várias conceções acerca desta: conceção fáctica, conceção normativa e a conceção interpessoal de honra[119].

---

[118] Entre outros, cfr. Acórdão Tribunal da Relação de Coimbra, de 22–10–2008, processo n.º 282/07.7 GAALB.C1, disponível em www.dgsi.pt..

[119] Para mais desenvolvimentos, cfr. COSTA, José Faria – **Comentário Conimbricense ao Código Penal,** (artigo 180.º, § 3 e ss.

Parece que, dadas as críticas a dirigir às demais teorias, esta última conceção interpessoal, que entende a honra de uma perspetiva normativo-social, ou seja, como um aspeto da personalidade de cada um, que lhe pertence desde o nascimento, e como a relação de reconhecimento (*Anerkennungsverhaltnis)* com outras pessoas baseada na dignidade humana e na autonomia da pessoa, aparenta ser a mais adequada. Esta autonomia só se concretiza, nas palavras de JOSÉ FARIA COSTA, "na relação de reconhecimento que a interpessoalidade proporciona". Assim, a comunidade onde cada um se insere, não é a fonte de honra, mas o lugar onde esta se exercita.

Ora, a distinção entre ambos os preceitos normativos far-se-á então com base na imputação, direta ou indireta, dos factos ou juízos desonrosos: se estes últimos se praticam perante a vítima de forma direta e isolada, falamos em Injúria; mas se esta se faz por intermédio de uma terceira pessoa (indiretamente), que serve de instrumento para a prossecução dos seus objetivos, já se falará em Difamação.

Neste último crime, essa particularidade atinente ao tipo objetivo faz com que tal conduta reflita uma maior gravidade pela desconsideração externa que possibilita, pela ofensa que se concretiza através da imputação de um facto ofensivo por meio de formulação de um juízo igualmente lesivo ou pela reprodução dessa imputação, sendo que em ambos os casos é necessário que tais comportamentos se dirijam a terceiros.

Por conseguinte, é este um crime de dano e material, sendo necessário, para além do preenchimento do tipo objetivo, que tais condutas seguem ao conhecimento da pessoa sobre quem recaem as imputações desvaliosas ou de um terceiro.

Logo, o legislador inverteu a lógica seguida na grande maioria da estruturação incriminadora da parte especial do Código Penal, inaugurando, como se compreende, o capítulo dos crimes contra a honra com o crime mais grave.

Quanto ao tipo subjetivo, é este claramente um crime doloso, requerendo-se o conhecimento e vontade de realização do tipo objetivo.

A Difamação não é punível se feita para realizar interesses legítimos e o agente provar a verdade da imputação (artigo 180.º, n.º 2), exceto quando se tratem de factos relativos à intimidade da vida privada e familiar (número 3).

Para as condutas referidas, a lei estabelece pena de prisão até seis meses e pena de multa até duzentos e quarenta dias.

§ 6 Como já se disse, quanto ao tipo objetivo, se o agente imputa factos ou formula juízos ofensivos perante e apenas a própria vítima, estaremos já perante um crime de **Injúria**, consagrado no artigo 181.º do CP.

No que toca ao tipo subjetivo, tal como na Difamação, é este um crime essencialmente doloso, punido com pena de prisão até três meses ou com pena de multa até cento e vinte dias, uma das mais baixas molduras penais abstratas previstas em todo o Código Penal.

C) Crimes contra a reserva da vida privada

§ 7 No caso de A, *pharmer*, detendo ilegitimamente os dados de B, passar a controlar as mensagens ou outro tipo de informações de correio eletrónico, *Facebook* ou outras, tomando conhecimento de outras de natureza privada / íntima com e/ou as divulgar, comete um crime de **Devassa da Vida Privada**,

presente no artigo 192.º do Código Penal, como eco da descoberta da privacidade como emanação da exigência direta da pessoa, ou seja, como merecedor de tutela jurídica decorrente da dignidade humana como valor supremo.

Quanto ao tipo objetivo, fazem parte as condutas através das quais alguém, com intenção de invadir a vida privada de outrem, toma conhecimento ou divulga informações íntimas, sendo estas as duas modalidades de violação do bem jurídico, independentes entre si.

Portanto, quanto à intromissão, estamos perante a configuração de um crime de execução vinculada, só assumindo importância as intromissões constantes das alíneas a), b) e c) do n.º 1 do artigo 192.º. Já quanto à divulgação, parece reconduzir-se ao modelo de um crime de execução livre, podendo esta última ser feita por qualquer forma.

Porém, a divulgação não é punível se praticada "como meio adequado para realizar um interesse público legítimo e relevante"[120].

Ao contrário do que acontecia nos crimes contra a honra, a verdade dos factos não elimina a responsabilidade penal, uma vez que, nas palavras de ARZT, "só as afirmações verdadeiras atingem de forma típica a esfera da intimidade".

Protege-se aqui, enquanto bem jurídico, a privacidade / intimidade como uma liberdade fundamental e que, segundo o Parecer 121/80 (de 23 de Julho de 1981) da Procuradoria Geral da República: "a intimidade da vida privada de cada um, que a lei protege, compreende aqueles atos que, não sendo secretos em si mesmos, devem subtrair-se à curiosidade pública por naturais razões de resguardo e melindre, como os sentimentos e aspetos familiares, os costumes da vida e as vulgares práticas quotidianas, a vergonha da pobreza e as renúncias que ela impõe e até, por vezes, o amor da simplicidade, a parecer em desconforme com a natureza dos cargos e a elevação das posições sociais. Em suma, tudo: sentimentos, acções e abstenções" (*BMJ* 309º 142).

Podendo falar-se em privacidade em sentido material e formal, com uma dimensão positiva e negativa, estática ou dinâmica[121], acolhe a lei portuguesa a teoria das três esferas, formulada pelos tribunais alemães e que goza hoje quase plena aceitação.

Esta teoria parte da imagens de três esferas concêntricas, preconizando como centro a área nuclear da vida privada, ou seja, a intimidade. Na esfera mais exterior, oposta à primeira, está a esfera social que corresponde à dimensão pública da pessoa. Por último, a esfera central representa uma tutela fragmentária atinente à proteção intermédia da privacidade.

Quanto ao tipo legal que agora nos ocupa, estamos perante um crime de dano pois em todas as suas modalidades se pressupõe a efetiva lesão do bem jurídico.

Relativamente ao tipo subjetivo, o artigo referido faz depender a punibilidade da existência da intenção de devassar a vida privada alheia. Nesse sentido, é este um delito de intenção.

Dependendo o correspondente procedimento criminal de queixa, estabelece-se como punição pena de prisão até um ano ou pena de multa até duzentos e quarenta dias.

§ 8 Também se mostra pertinente abordar a possibilidade de aplicação do artigo 193.º neste âmbito, já que este consagra o crime de **Devassa por meio de informática**.

---

[120] Artigo 192.º, número 2, *in fine* do Código Penal.

[121] Cfr. ANDRADE, Manuel da Costa – **Comentário Conimbricense ao Código Penal** (artigo 192.º, § 9 a 12).

Aqui se incluem as condutas através das quais se obtém acesso a conteúdos de dados pessoais, punindo-se tanto quem cria um ficheiro automatizado para esse efeito, como aquele que mantém um ficheiro desse tipo (mesmo que não tenha sido por ele criado) ou ainda aquele que o utiliza, tendo a ele acedido por qualquer forma.

Em resumo, quanto ao tipo objetivo, pune-se a criação de ficheiro automatizado ou qualquer outra conduta que se possa traduzir num acesso (legítimo ou ilegítimo) a um sistema informático que tenha como conteúdo dados individualmente identificáveis respeitantes a determinados assuntos absolutamente proibidos: *convicções políticas, religiosas ou filosóficas, filiação partidária ou sindical, vida privada ou origem étnica*. Não é necessário que o ficheiro tenha como conteúdo exclusivamente esses temas.

No que toca ao bem jurídico, parece estar-se perante um conceito mais amplo de reserva da vida privada, pois trata-se aqui, nas palavras de J. M. DAMIÃO DA CUNHA, de "garantir a interdição absoluta, constitucionalmente imposta, do tratamento informático de um conjunto de dados pessoais que a CRP afirma como insindicáveis e da total e plena disponibilidade da pessoa a que se reportam". Trata-se de garantir o direito de autodeterminação informacional à pessoa humana, já que esta deve ter o direito de disposição sobre este tipo de dados. Estamos, assim, perante um crime de dano.

Quanto ao tipo subjetivo, não sendo necessária qualquer intenção específica para o preenchimento do tipo, exige-se a existência de dolo, bastando o dolo eventual.

A tentativa é punível nos termos do n.º 2 do artigo 193.º, sendo este crime punido com pena de prisão até dois anos ou com pena de multa até duzentos e quarenta dias, prevendo ainda o artigo 197.º uma agravação da pena[122].

Porém, com a entrada em vigor da Lei de Protecção de Dados Pessoais – Lei 67/98 – já anteriormente analisada, com um conjunto de tipificações criminais relativas à informática e aos dados pessoais (nos seus artigos 43.º e ss.), parece que estas se sobrepõem ao tipo legal de Devassa por meio de informática constante do Código Penal.

Em particular, o artigo 43.º dessa lei, com a epígrafe "Não cumprimento de obrigações relativas a proteção de dados", abrange de forma clara, e até mais aprofundada, a incriminação do artigo 193.º do CP, tendo sido o seu conteúdo útil substituído pelo mesmo.

Portanto, parece ter-se verificado uma revogação implícita do crime de Devassa por meio de Informática.

§ 9 Por conseguinte, para enquadrar a conduta através da qual A, tendo obtido um conjunto de dados numa primeira fase de uma ataque de *pharming*, aproveita para criar, manter ou utilizar um ficheiro informático do tipo mencionado, será mais adequado reconduzi-la ao artigo 43.º da Lei de Protecção de Dados Pessoais no que toca ao **Não cumprimento de obrigações relativas a proteção de dados**.

Do tipo objetivo fazem parte as diversas condutas que integram as alíneas a) a f) do mesmo artigo, que contendem com o desrespeito pelas regras acerca do tratamento de dados pessoais.

[122] Autores como J. M. DAMIÃO DA CUNHA entendem que se deve interpretar corretivamente a agravação deste artigo, não a considerando aplicável ao artigo 193.º. Cfr. CUNHA, J. M. Damião da – **Comentário Conimbricense ao Código Penal** (artigo 193.º § 26 a 28).

O bem jurídico protegido é também a reserva da vida privada no sentido do direito à autodeterminação informacional do titular dos dados de carácter tão sensível. Tal preocupação reflete-se, nomeadamente, na agravação constante do número 2 do artigo 43.º quando as condutas referidas incidirem sobre dados de natureza sensível, determinados nos artigos 7.º e 8.º da Lei 67/98.

Quanto ao tipo subjetivo, exige-se o dolo enquanto conhecimento e vontade de realização do tipo objetivo.

Tais condutas são punidas com pena de prisão até um ano ou pena de multa até cento e vinte dias.

§ 10 Por último, assemelha-nos ainda possível que o *pharmer*, através dos dados obtidos, possa tomar conhecimento da correspondência eletrónica ou de outro tipo de escritos de carácter pessoal e privado que circulam em sistemas informáticos cuja acesso é possível através das credenciais de acesso a esses sistemas que o *pharming* permite obter como já se descreveu.

Nesse sentido, poderia colocar-se a hipótese de estarmos perante um crime de **Violação de correspondência ou de telecomunicações**, presente no artigo 194.º do Código Penal.

Quanto ao tipo objetivo, aqui se incluem as condutas através das quais alguém, sem consentimento, toma conhecimento de escritos privados ou de telecomunicações, impede, por qualquer método, o recebimento pelo legítimo destinatário, intromete-se no conteúdo da telecomunicação ou divulga o respetivo conteúdo.

Para o que aqui nos importa tratar, é a telecomunicação, no sentido de proteção da privacidade à distância, o objeto da ação, onde se incluem o *e-mail*, os SMS, etc.

A inviolabilidade das telecomunicações compreende, assim, tanto os dados de tráfego como os dados relativos ao conteúdo propriamente dito da comunicação, como é o caso das específicas mensagens de correio eletrónico.

O bem jurídico aqui alvo de tutela é também a privacidade, punindo-se não só a intromissão arbitrária, mas também a divulgação arbitrária na área da correspondência e da telecomunicação.

Quanto ao tipo subjetivo, o delito só é punível a título de dolo, bastando o dolo eventual.

Estabelece-se como punição pena de prisão até um ano ou pena de multa até duzentos e quarenta dias, dependendo o correspondente procedimento criminal de participação ou queixa (artigo 198.º CP).

A distinção entre este tipo legal e o de Devassa da vida privada parece dever fazer-se pela especificidade do objeto de proteção do crime de Violação de correspondência ou de telecomunicações. Parece, neste último, proteger-se mais a privacidade à distância em relação às intromissões em comunicações em curso, que ainda não estão, pelo menos totalmente, ao alcance e dispor do seu legítimo destinatário.

D) Crimes contra a vida em sociedade

§ 11 Perspetiva-se ainda a possibilidade de o agente, com os dados obtidos, proceder à falsificação de documentos de identificação (passaportes e outros) para, posteriormente, com maior encobrimento da verdadeira identidade, proceder à prática de outros crimes.

Nesse sentido, estaremos perante um crime de **Falsificação de Documentos,** constante do artigo 256.º do Código Penal.

Acerca desse tipo legal e sua caracterização, a que já nos referimos anteriormente, remetemos agora para o que aí foi dito[123].

[123] Cfr. pp.54 e ss. § 4.

4.2. Quanto à lesão de bens jurídicos patrimoniais

§ 12 Apesar de, como se disse, um ataque de *pharming* poder servir para a lesão de bens jurídicos de natureza não patrimonial, a verdade é que este, na esmagadora maioria das vezes e nos casos típicos, é praticado com vista à posterior realização de condutas atentatórias a bens jurídicos de carácter patrimonial, por motivos que bem se compreendem.

Por isso, interessa-nos particularmente analisar a **conduta através da qual o *pharmer*, tendo conseguido obter os dados de acesso à conta bancária de vários utilizadores, utiliza os mesmos para proceder, sem intervenção da vítima, a operações de cariz financeiro (como a transferência de valores monetários ou a compras através de cartão de crédito alheio).**

Assim, após ter em seu poder os dados pessoais das vítimas, o agente acede à verdadeira plataforma *online* do banco que foi alvo de ataque com os mesmos dados e, conseguindo assim entrar na área pessoal do utilizador-vítima, pode levar a cabo qualquer operação que estaria também na disponibilidade do verdadeiro titular.

Portanto, poderá optar pela transferência de valores monetários para a sua própria conta ou, preferencialmente, para outra que impossibilite a descoberta da sua verdadeira identidade. Por outro lado, também a possibilidade de realizar compras a crédito com cartão alheio se poderá, em abstrato, colocar.

Importa, por conseguinte, perceber a que tipos legais se subsumem tais condutas, já que tal análise se mostra, para além de necessária, bastante pertinente.

Tal acontece porque chegam já muitos casos aos nossos tribunais em que se discute, perante certo procedimento criminoso, se se está perante um caso de *phishing* ou de *pharming*[124], dada a semelhança aparente de ambas as condutas criminosas, como já se teve oportunidade de realçar.

Desta querela, e analisando algumas das situações que a convocam, não parecem muito claras, quer as conclusões a que se chegam, quer os argumentos que as suportam. Para além disso, os debates jurisprudenciais acerca destas questões situam-se ainda meramente no plano civil, estando em falta tal apreciação ao nível da responsabilidade criminal, onde o *phishing* aparece já, ainda que insignificantemente abordado, mas onde nada se escreve sobre o *pharming*, ficando sem se perceber a que disposições legais se deve reconduzir.

Por tal, e dado prever-se que este tipo de crimes cresçam exponencialmente – como aliás se tem verificado – importa clarificar tal enquadramento, para o qual se mostra essencial analisar estas últimas condutas que se apresenta com contornos bastante dúbios.

§ 13 Importa atentar para o facto de podermos ter casos em que o agente, ameaçando com as informações a que teve acesso, compele a vítima a realizar, ela própria, as transferências bancárias referidas, caso em que não terá qualquer limitação de índole técnica. Nesse caso, facilmente se dirá que estamos perante um crime de **Extorsão**[125], sem que, contudo, este possa ser

[124] Cfr. Acórdão do STJ, de 18–12–2013, processo 6479/09.8TBBRG.G1.S1 ou Acórdão do TRP, de 29–04–2014, processo 225/12.6TJVNF.P1, ambos disponíveis em www.dgsi.pt .

[125] Para maiores detalhes quanto à análise deste tipo legal, cfr. **Comentário Conimbricense ao Código Penal** (artigo 223.º CP).

convocado para a problemática do *pharming* pelas razões a seguir apresentadas, tal como o crime de Burla.

Tal crime, previsto e punido no artigo 223.º do Código Penal, aparece como *lex specialis* face ao crime de Coacção. Para além disso, este tipo legal mantém afinidades ainda com o crime de Roubo (artigo 210.º) e com o crime de Burla (artigo 217.º).

No primeiro caso conclui-se que ambos os preceitos têm como meios de execução a violência ou a ameaça (embora no crime de Roubo esta tenha de ser, cumulativamente, contra a vida ou integridade física e de execução eminente), lesando ambos a liberdade de disposição patrimonial. Contudo, enquanto que o objeto do roubo tem de ser uma coisa móvel, no crime de Extorsão podem ser quaisquer bens patrimoniais. Para além disso, o crime de Roubo exige a intenção de apropriação de coisa alheia, ao passo que no de Extorsão vale tanto a intenção de apropriação como a mera intenção de uso, não se visando, neste caso – ao contrário do crime de Roubo – uma entrega imediata do bem em questão.

Consequentemente, para a conduta que descrevemos no início deste §parágrafo pode colocar-se a questão da sua subsunção ao crime de Extorsão ou de Roubo. Todavia, dado que tais comportamentos nada têm que ver com o ataque de *pharming*, tal reflexão parece situar-se fora do nosso âmbito de estudo.

Já no caso do crime de Burla, embora ambos os crimes sejam contra o património em geral e pressuponham a cooperação da vítima e o enriquecimento do agente (lesando a liberdade de decisão e de ação), distinguem-se essencialmente pelos meios utilizados: violência ou ameaça com mal importante, no caso da Extorsão, e erro ou engano, no caso da Burla.

Em suma, quanto ao tipo objetivo do crime de Extorsão pune-se todo aquele que, para conseguir enriquecimento ilegítimo, constrange outra pessoa com violência ou mal importante. Sendo um crime comum e que requer um processo típico para a sua realização, tem como objeto um ato de disposição patrimonial – que se pode traduzir numa ação ou omissão – que constitua simultaneamente um enriquecimento ilegítimo e um prejuízo (para a vítima de coação ou para terceiro).

O bem jurídico tutelado é a liberdade de disposição patrimonial e, quanto ao tipo subjetivo, requer-se a existência de dolo.

A pena estabelecida é de cinco anos de pena de prisão, apesar de no número 2 e 3 do mesmo artigo se estabelecerem as qualificações do crime de Extorsão.

§ 14 Porém, dado que o *pharmer* pode, atendendo às informações que possui, proceder ele mesmo às transferências que lhe aprouverem sem qualquer intervenção da vítima (que decerto gerará mais controvérsia), é esta fatualidade – também a mais frequente neste tipo de casos – que levanta maiores dúvidas de enquadramento jurídico-penal e que, como se percebe, faz desde logo afastar o preenchimento do crime de Extorsão já que, neste caso, para lograr o enriquecimento ilegítimo o agente prescinde do constrangimento à vítima, sendo ele o único responsável pela condução do mesmo procedimento.

§ 15 Antes de analisar concretamente quais os tipos legais em questão aquando da realização, pelo *pharmer*, de transferências bancárias sem a intervenção do legítimo titular, importa perceber quais os mecanismos de

segurança inerentes às mesmas. Quanto a essas ferramentas verifica-se, desde logo, que não existe uniformidade entre as diferentes instituições bancárias.

Algumas – como, por exemplo, o *SantanderTotta* – optam pela necessidade de certificação dos destinatários, para garantir que o titular da conta deposita a sua confiança nos mesmos, sem a qual se requer a inserção de um código de segurança de alguns dígitos enviado par o número de telefone do titular, fornecido previamente no balcão do banco respetivo. Esse código tem a particularidade de ser válido apenas durante um curto espaço de tempo, ainda que para a mesma operação, para garantir que não há apropriações e utilizações indevidas dos mesmos. Mesmo para certificar um destinatário é também necessária a introdução de um código do mesmo tipo pelo titular do serviço.

Já outros bancos, como a *Caixa Geral de Depósitos* e o *Montepio*, preferem atribuir um cartão matriz exclusivo a cada cliente. Este, contendo um conjunto de colunas e linhas, cada um com três dígitos, é essencial para proceder a qualquer transferência bancária a partir do serviço *online* do banco.

Figura 14 : Exemplo de cartão matriz.
Fonte: https://www.montepio.pt/SitePublico/pt_PT/empresas/montepio24/cartao-matriz.page?altcode=10006E

Assim, aquando de cada transferência, o sistema *online* pede números aleatórios para que a mesma possa ser realizada, como mostra a imagem seguinte.

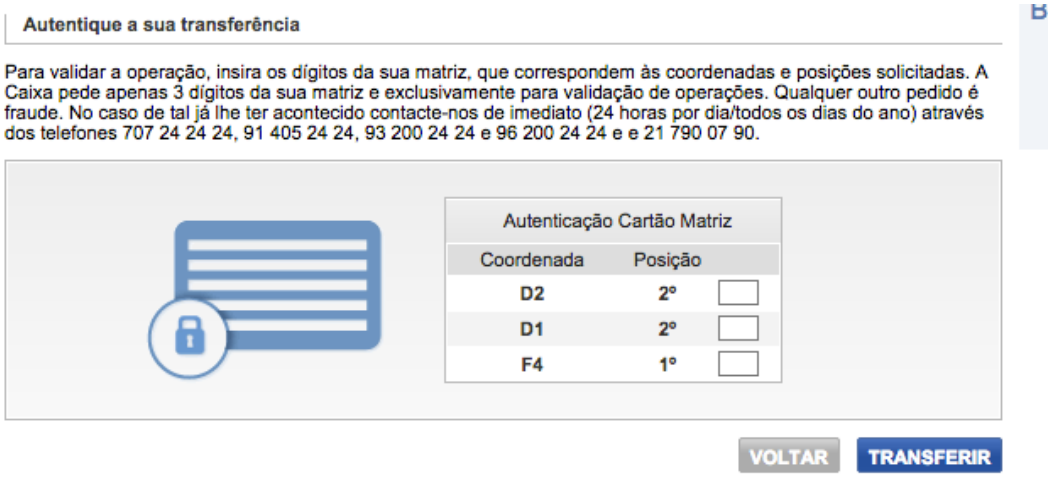


Figura 15 : Mecanismo *online* de autenticação de transferência por cartão matriz.
Fonte: www.cgd.pt

Este cartão matriz, impossível de obter na plataforma *online* do banco na área pessoal do próprio titular por razões de segurança, pode porventura ser obtido utilizando técnicas de *phishing*, tendo por base uma solicitação feita pelo criminoso de todo o cartão matriz, através de *e-mails* enviados para o(s) alvo(s) fazendo-se passar pela correspondente instituição bancária e acreditando que a ingenuidade prevalecerá.

Embora já em poucos casos – por razões que bem se compreendem – algumas instituições impõe um limite apenas acima do qual se requer um código para a efetivação das transferências[126]. Nesses casos, se pensarmos que o agente pode repetir tal ataque perante inúmeras vítimas concluímos que as vantagens de tal conduta são óbvias, dado também o anonimato proporcionado por estes meios.

§ 16 Assim, quanto à conduta através da qual o *pharmer*, com os dados pessoais obtidos ilegitimamente acede ao *website* do banco do titular dos dados e, na sua área pessoal, procede às transferências monetárias desejadas, para além de termos já excluído de aplicação o crime de Extorsão, outros tipos legais há que se podem, ainda que à primeira, vista suscitar dúvidas pertinentes de aplicação.

Em primeiro lugar, poderemos referir-nos ao crime de **Abuso de Confiança**, constante do artigo 205.º CP.

Para o preenchimento deste tipo legal é necessária a apropriação ilegítima de coisa alheia que o agente detém ou possui em nome alheio, mas com a particularidade de que se requer a existência de uma relação de fidúcia entre o agente e o proprietário, sendo este, nessa medida, um delito especial pois o seu autor só pode ser aquele que se liga ao proprietário por uma relação de confiança que o fez receber a coisa por título não translativo da propriedade que fundamenta o dever de restituição. Assim, a posse ou detenção tem de preexistir à apropriação, traduzindo-se sempre numa situação de inversão do título da posse.

O bem jurídico tutelado é aqui a propriedade, sendo, quanto ao tipo subjetivo, necessário o dolo, já que a intenção de restituir exclui este último desde logo. A tentativa é sempre punível segundo o n.º 2 do mesmo artigo e estabelece-se ainda uma pena de prisão até três anos ou pena de multa.

Nos números 4 e 5 estabelecem-se as qualificações deste crime, casos em que a pena de prisão pode ir até oito anos e a pena de multa até seiscentos dias.

§ 17 Como bem se percebe, não é este tipo legal aplicável à situação em análise. Mesmo que se possa discutir se os dados pessoais em causa são ou não coisas em sentido jurídico segundo o artigo 202.º do Código Civil, ainda que se desse uma resposta afirmativa, nunca se poderia afirmar que havia a entrega voluntária da coisa pelo seu titular a alguém com quem detém ou mantém uma relação de confiança. Muito pelo contrário: os dados são, como já vimos, obtidos pelo agente sem que de tal a vítima possa ter consciência, é isso que

[126] Dependendo das instituições bancárias, é comum, para transferências acima de um determinado valor, exigir-se o preenchimento com um código de segurança enviado na hora para o telemóvel do titular da conta e que expira depois de algum tempo. Esta é uma forma de garantir que só o verdadeiro titular pode movimentar valores mais consideráveis. Todavia, como em qualquer mecanismo de segurança, existem técnicas que permitem adulterar tal método com vista à prática de crimes.

verdadeiramente caracteriza este comportamento. Ora, tal elemento, como já falamos quanto ao tipo objetivo, é essencial para se poder falar em Abuso de Confiança.

Também, por isso, não há aqui, consequentemente, uma renúncia à restituição, havendo antes uma utilização indevida dos dados pessoais obtidos, já que, pela sua natureza, os dados não deixam de continuar a estar na disponibilidade do seu titular. Nem sequer o agente passa a comportar-se como legítimo titular inerente à inversão do título da posse referido, ele atua sabendo que se comporta ilegitimamente, pois nada a tal o habilita.

Assim se exclui a aplicação do referido tipo legal.

§ 18 Pode ainda colocar-se como hipótese a subsunção da conduta em apreço ao tipo legal de **Abuso de cartão de crédito ou de garantia**, presente no artigo 225.º do CP.

Ultrapassando, desde logo, o facto de tal tipificação não ser a mais pacífica[127], pune-se nessa disposição todo aquele que abuse de cartão de crédito ou de garantia, extravasando a possibilidade que o emitente tem de fazer um pagamento, causando prejuízo ao titular do cartão de crédito ou de garantia ou a terceiro.

O bem jurídico aqui tutelado é o património individual e não a proteção da confiança no tráfego deste tipo de cartões bancários, podendo apenas dizer-se que este último beneficia apenas de uma proteção reflexiva.

Quanto ao tipo subjetivo, é necessário o dolo, que tem de abarcar o abuso e o prejuízo patrimonial.

Sendo a tentativa punível, é este crime punido com pena de prisão até três anos ou com pena de multa, dependendo o correspondente procedimento criminal de acusação particular por força da remissão para o artigo 207.º CP.

Do artigo 225.º, n.º 5 constam ainda algumas agravações em razão do valor, casos em que, no máximo, a pena poderá ir até oito anos de prisão.

§ 19 É certo que através do *pharming* vários são os dados privados que podem ser obtidos, como já se teve ocasião de referir.

Contudo, é importante perceber se entre esse tipo de dados se podem incluir os códigos constantes de um cartão de crédito que permitem realizar compras *online,* uma vez que a partir de tal conclusão será possível afastar ou não a aplicação do tipo legal referido no artigo 225.º CP.

Para efetuar uma compra *online* é sempre necessária a inserção do código de dezasseis dígitos e a validade – presentes na frente dos cartões de crédito –, o chamado CVV[128] (código de três ou quatro dígitos constante do verso do cartão normalmente na linha de assinatura) e eventualmente o nome do titular, dados estes que são pedidos aquando da mesma compra.

Ora, tal demonstra com que facilidade pode alguém que detenha indevidamente o cartão, causar sérios prejuízos ao seu titular, realizando as mais diversas compras.

Porém, mesmo que o *site* alvo de ataque seja fornecedor deste tipo de serviços[129], não será possível a obtenção dos dados do cartão de crédito a partir da verdadeira plataforma *online*, mesmo com as credenciais de acesso da

[127] Cfr. CUNHA, J. M. Damião da - **Comentário Conimbricense ao Código Penal** (artigo 225.º § 1 a 5).
[128] Sigla para *Card Verification Value*. Traduz-se num código de segurança do cartão que proporciona maior proteção nas transações eletrónicas.
[129] Como é o caso da *Amazon*, lojas de roupa, etc.

vítima. Isto acontece porque em momento algum – e por motivos de segurança – o *website* guarda tal informação, dado o perigo inerente a tal opção.

Os dados do cartão têm obrigatoriamente de ser inseridos no ato de cada compra, mesmo estando já o utilizador registado e mesmo que se trate de um cliente frequente.

Apesar disso, existe a possibilidade de o utilizador pretender guardar determinado cartão para uma próxima transação. Nesse caso, tratando-se da maioria das empresas que se prezem minimamente confiáveis e atualizadas, apenas é guardado o código de dezasseis dígitos e a validade, sendo ainda sempre necessário inserir o CVV.

Por isso mesmo, neste caso concluímos que o crime de Abuso de cartão de garantia ou de crédito não é aplicável à nossa hipótese de estudo.

Porém, claro que se se tratarem de *websites* pouco seguros e até com intenções menos aconselháveis, pode ser que os mesmos guardem todas as informações do cartão de crédito, já que ao nível da conformação técnica nada o impede.

Nesses casos, o tipo legal presente no artigo 225.º do Código Penal torna-se aplicável.

§ 20 Neste sentido, pode colocar-se ainda em hipótese a aplicação do crime de **Burla.**

Este crime, constante do artigo 217.º foi introduzido pela Reforma ao Código de 1995 – para substituir o anterior artigo 313.º, já do velho Código Penal de 1982, embora mantendo a mesma linha de orientação. Esta norma teve como fontes principais o artigo 146.º (*Betrug*) do StGB Suíço, o § 146.º (*Betrug*) do StGB Austríaco e o § 263.º (*Betrug*) do StGB Alemão.

No que a este respeita, o bem jurídico tutelado é o património[130] globalmente considerado – como o próprio nome do Capítulo correspondente deixa antever –, por meio da punição das ações em que o respetivo agente vise alcançar um enriquecimento ilegítimo (próprio ou alheio) através da indução em erro da vítima, que a leva a praticar atos de diminuição patrimonial, para ela própria ou para terceiro, podendo, nesse sentido, falar-se no crime de burla como um crime com participação da própria vítima.

É este um crime de dano, só se consumando se houver um efetivo prejuízo patrimonial, traduzido na saída dos bens da esfera de disponibilidade fáctica do sujeito passivo ou vítima, sendo, também por isso, um crime de resultado. Por outro lado, e apesar de se exigir uma intenção de enriquecer ilegitimamente[131], tal enriquecimento não é necessário para a consumação do crime, bastando que haja um empobrecimento, ou seja, o dano, falando-se, por tal, de um crime de resultado parcial ou cortado pela descontinuidade entre os tipos objetivo e subjetivo, já que apesar o agente atuar com intenção de um enriquecimento ilegítimo, tal não precisa de se verificar.

É considerado ainda um crime de execução vinculada na medida em que para a consumação é necessária a execução do concreto *modus operandi* descrito (indução em erro que possibilita os posteriores prejuízos patrimoniais), havendo um duplo nexo de imputação objetiva a que subjaz os pressupostos da Teoria da Adequação (artigo 10.º, n.º1 do CP): entre a conduta enganosa do criminoso de

[130] Quanto ao conceito de património, cfr. COSTA, A. M. Almeida – **Comentário Conimbricense ao Código Penal**, pp. 275, § 5-8.

[131] A burla consubstancia um delito de intenção (*Absichtsdelikt*), sendo necessária a intenção de enriquecer ilegitimamente para se preencher o tipo subjetivo necessariamente doloso, não bastando o prejuízo patrimonial.

que advém a prática de atos, pelo burlado, de atos de diminuição patrimonial; e entre estes e o efetivo prejuízo patrimonial[132].

É, por fim, apenas punível a título de dolo (artigo 217.º, n.º 1, 13.º e 14.º do CP), mas sempre punível a mera tentativa (artigo 217.º, n.º 2 e 23.º do CP), vigorando ainda as regras gerais relativas à matéria da comparticipação (artigo 26.º e seguintes do CP).

§ 21 Pelo que se disse, concluímos então que quando à utilização dos dados obtidos ilegitimamente com intuito de aceder à verdadeira plataforma *online* e causar prejuízo patrimonial ao seu titular com um consequente enriquecimento ilegítimo, não poderemos aceitar que estamos perante um crime de Burla. Tal acontece uma vez que especificamente nesta conduta não há a criação de um estado de erro pelo agente para proceder ao prejuízo patrimonial sobre a vítima, pois prescinde-se da participação da própria vítima (que, tipicamente, no crime de Burla causa o próprio prejuízo patrimonial, ainda que inconscientemente) que permanece alheada de tudo o que está a ser realizado.

§ 22 Por outro lado, afigura-se como opção o artigo 221.º do Código Penal, relativo à **Burla Informática**, que merece algumas considerações.

Foi esta norma introduzida pela Reforma de 1995 ao CP (Decreto-lei 48/95, de 15 de Março), inspirando-se na ""burla de computadores" (*Computerbetrug*) do §263-a do StGB alemão.

Também aqui, o bem jurídico protegido é o património, distinguindo-se, dessa forma, de algumas disposições da Lei de Protecção de Dados e da Lei do Cibercrime de que já se discorreu. É este um crime de dano, já que depende, para a efetiva consumação, de um efetivo prejuízo patrimonial. Contudo, é também um crime de resultado ou material, pois este prejuízo só se verifica se houver a saída dos bens da esfera de disponibilidade fáctica da vítima, tal como acontece no tradicional crime de burla. Do mesmo modo, trata-se de um crime de execução vinculada, devendo obedecer ao concreto *modus operandi* descrito: intervenção num tratamento informático de dados com uma intenção ilegitimamente lucrativa. Esta descrição, também presente no artigo 221.º, n.º1 do CP, vem acompanhada de circunstâncias meramente exemplificativas que podem integrar esta fatualidade típica. Portanto, a vinculação da execução diz apenas respeito à exigência de lesão do património por meios informáticos. Neste sentido, importa concluir acerca da diferença entre este ilícito típico e o da Burla.

Pode dizer-se que na burla tradicional há um atentado indireto ao património da vítima pela criação prévia de um estado de erro para que a vítima traga a sua própria ruína, havendo, como se referiu, um duplo nexo de imputação objetiva. Já na Burla Informática este atentado ao património é feito diretamente, possibilidade dada pelos atuais e sofisticados meios informáticos. Não há necessidade, desta vez, para a lesão do bem jurídico, de qualquer intervenção em estado de erro da vítima.

Logo, no caso em que os meios informáticos sirvam para induzir a pessoa em erro, para que posteriormente, se produza a lesão patrimonial, fala-se, ainda assim, num caso de burla. Assim, entre ambas as figuras-de-delito há uma relação de exclusividade típica (*tatbestandliche Exklusivitat*), sendo a designação de "burla" no caso deste último elenco, imprópria.

---

[132] Não se segue a orientação pela existência de um triplo ou mesmo quádruplo nexo de causalidade. Cfr. COSTA, A. M. Almeida – **Comentário Conimbricense ao Código Penal**, pp. 293 e ss., § 13.

É este um crime doloso, sem punição a título de negligência segundo uma interpretação conjugada dos artigos 221.º, n.º 1 e 13.º do CP. Para além disso, tal como no desenho clássico da burla, estamos perante um delito de intenção, de resultado parcial ou cortado (*kupiertes Erfolgsdelikt*) pela descontinuidade entre o tipo subjetivo e objetivo, pois exige-se a intenção de um enriquecimento ilícito que subjaz à ação do agente, mas tal enriquecimento não é de necessária verificação.

Estabelece-se como punição pena de prisão até três anos ou pena de multa.

A tentativa é sempre punível (artigo 221.º, n.º 3 e 23.º do CP) e quanto à comparticipação vigoram as regras gerais do artigo 26.º e seguintes do Código Penal.

§ 23 Como já se referiu no início desta secção, para a realização de transferências bancárias podem existir certos mecanismos de segurança que visam garantir que as mesmas são apenas feitas pelo titular da respectiva conta. As principais ferramentas utilizadas são a certificação do destinatário, que requer a inserção de um código de segurança enviado para o telemóvel do titular, e a existência de um cartão matriz.

No primeiro caso, não se nos afigura muito fácil que alguém consiga contornar tal entrave de segurança. No limite, pode o *pharmer* ser funcionário de uma das operadoras de rede que, aproveitando-se das vantagens inerentes à sua profissão, consiga alterar o percurso da mensagem que contém o código de segurança (que permitirá concluir a transferência) e encaminhá-la para um número de telemóvel que ele próprio detém.

Outra possibilidade, embora não muito comum[133], mas que é potenciada pelo cada vez mais fácil acesso a todo o tipo de tecnologias, é a compra de uma torre que imita a torre fidedigna das operadoras telefónicas e que passa a receber todo o tráfego desta última, sendo possível selecionar as informações que se pretendam, inclusive de um número de telemóvel em específico.

Nesta hipótese, o *pharmer,* ao tentar realizar uma transferência, sabe de antemão que será necessária a inserção do código de segurança temporário enviado para o titular da conta respectiva. Como – através das informações que obteve – o criminoso pode descobrir o número de telemóvel do titular da conta alvo de ataque, acaba por conseguir ter também acesso a todas as mensagens a ele destinadas, assim como a operadora telefónica fidedigna, já que o todo tráfego passa a circular também na torre forjada.

§ 24 Em primeiro lugar, saliente-se que estas duas hipóteses se reconduzem ao tipo legal de **Intercepção Ilegítima**, constante do artigo 7.º da Lei do Cibercrime.

Quanto ao tipo objetivo, pune-se "quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do sistema ou de parte dele, e através de meios técnicos, intercetar transmissões de dados informáticos que se processam no interior de um sistema informático, a ele destinadas ou dele provenientes", situação que, nos casos que se referiram, sucede. Não se exige aqui a efetiva obtenção de informação, bastando o mero ato de proceder de forma a que tal aconteça.

Quanto ao bem jurídico, à semelhança do que acontecia com os outros tipos legais constantes da Lei da Cibercrime, é alvo de proteção a intangibilidade

[133] Nos Estados Unidos da América, tal mecanismo seja já usado pelas entidades públicas para a obtenção de meios de prova, discutindo-se, por isso, a validade de tal ferramenta nestes moldes.

do sistema informático globalmente considerado, fazendo eco do artigo 34.º, número 4 da CRP e do artigo 8.º da CEDH. Nesse sentido, podemos considerar este preceito como um crime de dano.

Quanto ao tipo subjetivo, é necessário o dolo enquanto conhecimento e vontade de realização do tipo objetivo, não sendo requeridas especiais intenções do agente.

Estabelece-se como punição pena de prisão até três anos ou pena de multa.

Para além disso, em qualquer destes casos, ou quaisquer outros que se afigurem possíveis para contornar por meios técnicos do código de segurança enviado para o telemóvel do titular da conta de realização da transferência (já que o avanço tecnológico neste sentido é constante e imprevisível), concluímos que o tipo legal de Burla Informática implicado é chamado à colação.

Primeiro, porque se verifica a intenção de obter benefício ilegítimo inerente à produção de um prejuízo patrimonial à própria vítima aquando da realização ilegítima de transferências bancárias pela utilização de dados pessoais alheios.

Em segundo lugar, há aqui uma interferência em sistemas informáticos para conseguir tal prejuízo e consequente enriquecimento, mas tal não serve para provocar o erro (caso em que estaríamos perante um crime de Burla), mas sim como ataque direto, ou seja, para conseguir, sem qualquer participação da vítima, a realização dos intentos que já se referiram.

Por isso, no tocante à letra do artigo 221.º CP, é a parte "... interferindo no resultado de tratamento de dados ou mediante a estruturação incorreta de programa informáticos, (...) **utilização de dados sem autorização** ou intervenção por qualquer outro modo não autorizada no processamento ..." especificamente aplicável à conduta alvo de estudo, assim se passando a conhecer âmbito de aplicação para a mencionada disposição legal.

§ 25 Já no caso do cartão matriz, único para cada cliente, e sua obtenção, levantam-se as mesmas questões.

Assim, parece-nos que a única forma de conseguir contornar tal ferramenta de validação seria um ataque de *phishing* em que, através de um *e-mail* fraudulento para múltiplos destinatários, o *phisher* se faria passar pela correspondente instituição bancária a solicitar o cartão matriz para efeitos supostamente legítimos. A partir daí esperaria que alguém mais ingénuo acreditasse e retornasse os dados referidos.

Neste caso, embora acreditemos que seja cada vez mais difícil obter sucesso nestes moldes já que tal grau de ingenuidade tende a ser menos frequente, a punição da conduta referida reconduzir-se-ia à própria punição específica do ataque de *phishing*, panorama este que foge do âmbito de análise do presente trabalho.

Ainda que possa pensar-se na possibilidade de o *pharmer* obter acesso de forma ilegítima à base de dados do banco referido para obter as informações contidas no próprio cartão matriz, em tal caso, deixaria de fazer sentido falar sequer num ataque de *pharming*, uma vez que se o criminoso conseguisse ter acesso à base de dados do banco, desde logo conseguiria realizar todas e quaisquer operações sem necessidade de empregar qualquer das técnicas arrojadas que o *pharming*, como se mostrou, pressupõe.

A acontecer, neste caso, não falaríamos em *pharming*, mas na existência de um crime de Acesso Ilegítimo e, subsequentemente, de um crime de Burla Informática, o que não apresenta relevo para o nosso cenário de estudo.

Contudo, como as possibilidades que a tecnologia fornece ultrapassam, por vezes, a própria imaginação humana do momento presente, não podemos assegurar não existir já ou vir a existir alguma possibilidade de manipulação técnica que permita obter exclusivamente e globalmente os dados do cartão matriz.

Se tal situação for ou vier a ser possível, mais uma vez o tipo legal de Burla Informática se torna aplicável, pelas razões que no parágrafo § 22 já se expuseram.

CAPÍTULO V – Utilização ilegítima de dados pessoais para fins patrimoniais: Concurso de crimes

§ 1 Quanto às condutas atentatórias de bens jurídicos de índole patrimonial, os principais tipos legais implicados foram, como dissemos, o de **Abuso de cartão de crédito ou de garantia** e o de **Burla Informática**, podendo este, ou não, implicar o cometimento de um crime de **Intercepção Ilegítima** – quanto às hipóteses que avançamos relativas ao funcionário de operadora telefónica que se aproveita da possibilidade de acesso a informações confidenciais (inerente à sua função profissional) ou à torre que forja tal serviço, como formas de controlar o conteúdo do titular da conta alvo, para o recebimento do código de segurança que permite proceder a transferências bancárias sem a intervenção do respetivo titular[134]. Este crime aparece previsto no artigo 7.º da Lei do Cibercrime.

Neste último caso, o crime de Intercepção Ilegítima funciona pois como mero crime instrumental ou crime-meio já que só é cometido por forma a viabilizar o preenchimento do crime de Burla Informática, verdadeiro intento do criminoso que pretende a movimentação ilegítima, por processos técnicos, de valores monetários, sendo este último, por isso, o crime principal ou crime-fim.

Assim, parece de concluir que estamos perante um caso de concurso aparente entre os referidos tipos legais já que a simples análise abstrata dos tipos legais de crime em conflito permite concluir acerca da norma a aplicar em definitivo, independentemente dos contornos concretos do caso, no entendimento de EDUARDO CORREIA; ou, na esteira de FIGUEIREDO DIAS, ocorre um concurso de ilícitos que, face à situação concreta, se podem sobrepor total ou parcialmente, tendo por base o critério da unidade ou pluralidade de sentidos sociais de ilicitude jurídico-penal do comportamento global, de factos puníveis[135].

A opção pela existência de tal concurso far-se-á, portanto, por recurso ao critério do crime-meio proposto por FIGUEIREDO DIAS. Isto acontece porque existe um único sentido autónomo de ilicitude: a condenação pelo crime de Burla Informática exprime já de forma bastante o desvalor de todo o comportamento.

Porém, poderia também problematizar-se, de acordo com o entendimento deste último autor, estarmos perante um caso de subsidiariedade[136], podendo argumentar-se a tal favor defrontarmo-nos com fases distintas de proteção do bem jurídico. Nesse sentido, a intangibilidade de sistemas informáticos poderia ser entendida como mero bem jurídico meio a utilizar com o propósito de lesão do bem jurídico fim, o património (tutelado com o tipo legal de Burla Informática ou de Abuso de cartão de crédito ou de garantia). Neste caso, falar-se-ia já, para FIGUEIREDO DIAS, de uma situação de concurso de normas – resolvida pela mera apreciação abstrata das normas em conflito – e não de concurso aparente.

Contudo, dada a solução em concreto acabar por ser a mesma em ambas as hipóteses, não nos parece importante aprofundar tal panorama, sendo indiferente, na prática, a opção por qualquer uma das vias.

Por conseguinte, tal como se disse a propósito da resolução do concurso de crimes quanto à obtenção ilegítima de dados pessoais – primeira fase do ataque de *pharming* –, como o crime de Intercepção Ilegítima é puramente

[134] Cfr. *supra* p. 90, § 23.
[135] Para maior detalhe cfr. p. 69, § 2 e 3.
[136] Cfr. *supra* p. 70, § 3.

instrumental, já que utilizado unicamente como forma de alcançar o verdadeiro intento criminoso, e o crime de Burla Informática traduz já o sentido de ilicitude dominante – traduzido na produção de prejuízos patrimoniais por intromissão não autorizada, através de processos técnicos, num sistema informático – acaba o último por absorvê-lo: *lex consumens derogat legi consuntae*.

Mesmo de acordo com a opinião de EDUARDO CORREIA, a solução manter-se-ia já que estamos perante um caso em que, da análise da situação concreta, ressalta a conclusão de que a norma que descreve o tipo legal de Burla Informática acaba por englobar satisfatoriamente a de Intercepção Ilegítima pela relação que ambos os preceitos estabelecem entre si na conduta em apreço.

Logo, podemos falar na ocorrência de uma relação de consumpção (pura), no qual a norma que consome derroga a consumida pois colocamo-nos perante um caso em que o "conteúdo do ilícito-típico inclui em regra o de outro facto, de tal modo que, em perspetiva jurídico-normativa, a condenação pelo ilícito-típico mais grave exprime já de forma bastante o desvalor de todo o comportamento"[137].

Não há lugar para a aplicação do mecanismo da consumpção impura uma vez que os dois tipos legais estabelecem como punição pena prisão até três anos ou pena de multa, ficando o bem jurídico igualmente acautelado mesmo com a aplicação exclusiva de um dos tipos legais, como acabamos por concluir.

Nesse seguimento, podemos dizer de forma geral que quando o crime de Intercepção Ilegítima é usado exclusivamente para consumar o crime de Burla Informática, este último o consome ocorrendo um concurso meramente aparente. Todavia, se a Intercepção Ilegítima ultrapassa a medida necessária à efetiva consumação do tipo legal de Burla Informática, aproveitando o agente para ter acesso a outro tipo de informações que não contendem com o ataque de *pharming*, estaremos já perante um concurso real ou efetivo.

§ 2 Tal raciocínio será de aplicar em todos os casos em que o preenchimento de tipos legais que se relacionam com a lesão do património pressuponha a prática de outros crimes que, por esse motivo, são puramente instrumentais e acabarão por ser absorvidos pelos correspondentes crimes-fim.

Este panorama poderá verificar-se nas hipóteses que deixamos em aberto quanto ao contorno por meios técnicos das ferramentas de segurança inerentes às transferências bancárias e à obtenção dos dados do cartão de crédito que se mostram essenciais para proceder a compras *online* e que a nossa imaginação não deixa ainda antever.

§ 3 A solução de enquadramento que avançamos para o fenómeno de *pharming* é, como dissemos, uma total novidade no contexto da jurisprudência portuguesa, quer a nível penal e cível, quer em termos da existência de uma definição fáctica precisa de tal ataque.

Tal acontece porque, de entre a jurisprudência que se tem debruçado sobre estes temas[138], o que sucede é que acaba por permanecer a dúvida sobre se determinada hipótese se deve reconduzir ao fenómeno de *phishing* ou de *pharming*, pela incerteza proveniente do facto do desenho de ambos que se revelar muito próximo.

---

[137] DIAS, Figueiredo – **Direito Penal: Parte Geral, Tomo I**. Coimbra: Coimbra Editora, 2007: 42 / §18.

[138] Cfr., por exemplo, o Acórdão do Supremo Tribunal de Justiça de 18–11–2013, processo 6479/09.8TBBRG.G1.S1, disponível em www.dgsi.pt..

O que agora se menciona é confirmado por uma citação retirada do último acórdão referido: "Desta materialidade o segundo grau concluiu o seguinte «(...) Assim é nossa convicção que não se apurou, de entre as técnicas de fraude referidas (*phishing* e *pharming*), o modo como aconteceu aquela transferência da conta da A.» (...) Quer dizer, as instâncias retiraram uma presunção judicial: a transferência ocorrida da conta da Autora foi devida a uma fraude informática, tendo admitido que tal fraude **pudesse** ser caracterizada de phishing."

Por outro lado, em matéria penal, os nossos tribunais não conseguem ainda reconduzir especificamente o *phishing* – e muito menos o *pharming* – aos concretos tipos legais. Uns falam em Falsidade Informática[139], em Burla, outros ainda em Burla Informática[140], confundindo os diversos tipos legais sem que haja uniformidade acerca da melhor interpretação a seguir.

Exemplo paradigmático é o Acórdão do Tribunal da Relação de Lisboa de 16-04-2015[141] em que, para além de se confundir *phishing* com as técnicas que o podem complementar para alcançar outros intentos e com o próprio *pharming*, não se está alerta para as questões que, por exemplo, as alegações do réu levantaram. Isto acontece porque este não conseguiu explicar como foi possível obter os dados do cartão matriz, problema este que nos causou bastante apreensão devido às dificuldades inerentes. Com a utilização de *key-loggers*[142], como sugere o réu, não seria possível obter as referidas credenciais já que, como com tal ferramenta maliciosa só se obtêm as teclas digitadas, não se sabe a que coluna e linha correspondem as mesmas no cartão matriz do titular.

Para além disso, neste acórdão, ora se reconduz o *phishing* (ataque que se verifica segundo a opinião do tribunal) ao tipo legal de Burla informática, ora ao de Burla.

Já quanto ao *pharming*, na generalidade da nossa jurisprudência e em termos de enquadramento penal, verifica-se um total vazio, permitindo, por isso, a conclusão que avançamos a tal propósito o preenchimento de tais lacunas, esperando evitar lapsos e erros que porventura se possam ainda suscitar.

[139] Cfr., por exemplo, o Acórdão do Tribunal da Relação do Porto, de 21–11–2012, com o processo RP201211211001/11.9JAPRT.P1, disponível em www.dgsi.pt..
[140] Cfr. Acórdão do Tribunal da Relação de Guimarães, de 30–05–2015, processo 6479/09.8TBBRG.G1, disponível em www.dgsi.pt..
[141] Cfr. Acórdão do TRL, processo 971/13.7TJLSB.L1-8, de 16-04-2015, disponível em www.dgsi.pt.
[142] Cfr. *supra* p. 22 e nota de rodapé n.º 20.

CAPÍTULO VI – Punição concreta resultante de ponderação global

§ 1 O ataque de *pharming*, como tivemos ocasião de referir subdivide-se em dois momentos: um primeiro, destinado à obtenção ilegítima de dados pessoais alheios; e um segundo, em que se usam tais dados para prática de condutas que podem lesar bens jurídicos de diversa índole, embora nos tenhamos circunscrito à lesão de bens jurídico-patrimoniais, por ser esse o âmbito do nosso trabalho.

Vimos, porém, que tais momentos implicam o preenchimento de vários tipos legais. O referido em primeiro lugar convocou o tipo legal de Falsificação de Documentos, quanto à criação de um *site* forjado; o tipo legal de Acesso Ilegítimo, relativo ao acesso não autorizado ao Servidor DNS ou *Host File;* e, por fim, o crime Falsidade Informática, referente ao corrompimento dos dados de tais sistemas informáticos.

Ao concluir dessa primeira fase, e resolvendo a problemática do concurso de crimes, optamos pelo entendimento da existência de um concurso aparente entre tais normas que se resolveu com a absorção do crime de Falsificação de Documentos e do crime de Acesso Ilegítimo pelo tipo de Falsidade Informática por este englobar já o desvalor que deve ser dirigido a toda a conduta concreta do agente[143].

Já na fase relativa à utilização de tais dados pessoais obtidos ilicitamente foram chamados a intervir, quanto à lesão de bens jurídicos patrimoniais, o crime de Abuso de cartão de crédito ou de garantia ou o crime de Burla Informática, acabando estes por absorver qualquer outro crime que visasse garantir a sua consumação e, consequentemente, a consumação de um ataque de *pharming*.

É fulcral, assim, perceber como se deverá realizar a punição final e concreta de tais condutas já que, até ao momento, se confronta o crime de Falsidade Informática (que consumiu os restantes na primeira fase) com o crime de Abuso de cartão de crédito ou de garantia ou o de Burla Informática, conforme sejam os intentos do *pharmer*.

§ 2 Para alcançar tais conclusões importa olhar para cada um desses tipos legais abstratamente. Desse modo, verificamos que, por um lado, o crime de Falsidade Informática aparece como um crime de dano que visa proteger a intangibilidade dos sistemas informáticos, prescrevendo como punição pena de prisão até cinco anos e pena de multa entre cento e vinte e seiscentos dias.

Por outro lado, o crime de Abuso de cartão de crédito ou de garantia, ao estabelecer pena de prisão até três anos e pena de multa, prefigura-se como um crime de dano que tem como bem jurídico tutelado o património individual.

Por último, o crime de Burla Informática, visando proteger o património e sendo um crime de dano, determina como punição pena de prisão até três anos e pena de multa.

Assim, independentemente do objetivo do *pharmer*, vemos que toda a sua conduta e todos os crimes que vai sucessivamente praticando visam, do ponto de vista patrimonial, um de dois intentos: condutas que integram a tipificação do crime de Abuso de cartão de crédito ou de garantia ou condutas que

[143] Cfr. pp. 69 e ss.

preenchem tipo legal de Burla Informática. Todos os outros crimes são "um mal necessário", meios que têm em vista um objetivo maior. Assim, todos os crimes anteriores são meras ferramentas, instrumentos para a concretização de determinada finalidade.

Independentemente de qual seja essa finalidade, somos da opinião de que estamos perante um concurso aparente entre o crime de Falsidade Informática e o crime final a aplicar resultante da conduta do *pharmer*. Tal acontece pelos mesmos motivos que avançamos também no capítulo anterior, ou seja, verifica-se um concurso de ilícitos que, face à situação concreta, se podem sobrepor total ou parcialmente, tendo por base o critério da unidade ou pluralidade de sentidos sociais de ilicitude jurídico-penal do comportamento global, de factos puníveis existentes. Na presente situação estamos perante a existência de um único sentido social de ilicitude jurídico-penal, se olharmos para o comportamento global concreto, pois a concorrência de normas se dá exclusivamente a um nível abstrato.

Recorrendo aos critérios de FIGUEIREDO DIAS, é o do crime-meio o necessário para se resolver a presente questão já que, como se afirmou, os crimes cometidos numa primeira fase constituem unicamente instrumento de realização do crime final.

Ora, estamos então perante um caso de consumpção – quer segundo a doutrina tradicional de EDUARDO CORREIA, quer segundo o entendimento de FIGUEIREDO DIAS – já que, pelo que se referiu anteriormente, o crime final (de Abuso de cartão de crédito ou de garantia ou de Burla Informática) acabará por absorver o crim anterior, isto é, o crime de Falsidade Informática que já engloba os crimes praticados anteriormente com vista à obtenção ilegítima de dados pessoais.

Porém, não estaremos agora perante um caso de consumpção pura ou própria, mas será sim chamada a intervir, usando a terminologia de EDUARDO CORREIA, a "válvula de segurança de todo o sistema do concurso aparente". Tal acontece porque o crime final ou que consome, qualquer que seja das hipóteses apresentadas, prescreve uma pena menor do que o crime que é consumido (o de Falsidade Informática) e, com isso, ocorrerá uma menor proteção do bem jurídico.

Para acautelar tal situação aplicar-se-á então a pena mais elevada, embora seja essa a do crime consumido. Importa salientar, tal como foi avançado em primeira linha por A. M. ALMEIDA COSTA (e o mesmo conclui FIGUEIREDO DIAS[144]), e que diverge da doutrina tradicional, que "esta operação se limita ao plano da determinação da pena aplicável e deixa intocado o específico conteúdo de ilícito da situação, que continua a integrar o tipo de dano consistente na lesão do bem jurídico, limitando-se a regra da consunção *impura* ao problema da pena aplicável"[145].

Assim, concluímos também que o plano da ilicitude permanece intocado com a presente solução, sendo apenas da punibilidade (que alguns autores defendem autonomizar) que sofre adaptações: o tipo legal aplicável a final ao ataque de *pharming* é o de Burla Informática e não o de Falsidade Informática. O que acontece é que, por razões de melhor tutelar o bem jurídico, a pena a aplicar será a deste último crime por ser também mais elevada.

A referida interpretação coaduna-se com o princípio geral da interpretação jurídica que defende que se deve presumir que o legislador

[144] Cfr. DIAS, Jorge de Figueiredo - **Direito Penal: Parte Geral, Tomo I**. Coimbra: Coimbra Editora, 2007: 43.º / II / 2.3. / § 36.
[145] Cfr. COSTA, A. M. Almeida – **Comentário Conimbricense ao Código Penal**, II, artigo 262.º, § 6 e § 7.

pretendeu sempre consagrar a melhor e mais adequada solução (artigo 9.º, número 3 do Código Civil), sempre respeitando o princípio da legalidade e por forma a obter um entendimento harmonioso.

Dessa forma, a punição a final do ataque de *pharming*, com os contornos elencados, acaba por se resumir à punição única pelo crime de Burla Informática ou de Abuso de cartão de crédito ou de garantia, mediante a conduta praticada pelo *pharmer*, embora a pena a aplicar seja a do crime de Falsidade Informática para que se evite a menor proteção do bem jurídico.

Assim, ainda que o agente veja atribuído ao seu comportamento o tipo legal de Burla Informática ou de Abuso de cartão de crédito ou de garantia, deverá ser punido com pena de prisão até cinco anos ou pena de multa de cento e vinte a seiscentos dias.

§ 3 Por outro lado, se o agente com os dados obtidos ilegitimamente opta e aproveita para levar a cabo condutas que preenchem ambos os tipos legais mencionados – Abuso de cartão de crédito ou de garantia e de Burla Informática – ou várias vezes o mesmo tipo legal, teremos, nesse caso, não um concurso aparente, mas um concurso real ou efetivo de crimes.

Tal acontece porque estamos perante uma pluralidade de infrações cometidas pelo mesmo agente antes de qualquer delas ter sido objeto de uma sentença transitada em julgado. Para tal averiguação, EDUARDO CORREIA, como referimos em local anterior, propõe que o número de infrações "determinar-se-á pelo número de valorações que, no mundo jurídico-criminal, correspondem a uma certa atividade"[146].

Já para FIGUEIREDO DIAS, o concurso real de infrações define-se pela existência de uma pluralidade de sentidos sociais autónomos de ilícitos-típicos cometidos, de normas típicas concretamente aplicáveis que, para efeitos de punição, devem ser integralmente valorados[147].

Independentemente da opinião que se acolha, pensamos que a conclusão mais meritória será a de que, nesta última hipótese, temos infrações completamente autónomas e que, por isso, merecem ser valoradas como tal, cabendo a cada uma delas um sentido autónomo de ilicitude.

[146] CORREIA – Eduardo: **Direito Criminal: Volume II** (com colaboração de Figueiredo Dias). Almedina, 2010: §10 / 35.
[147] Cfr. DIAS, Jorge de Figueiredo - **Direito Penal: Parte Geral, Tomo I**. Coimbra: Coimbra Editora, 2007:

CONCLUSÃO

Com este trabalho pretendíamos, em primeiro lugar, esclarecer as nuances técnicas que dão forma a um ataque informático que possui, para além de considerável perigosidade, uma ocorrência que se equaciona cada vez mais frequente: o *pharming*.

A existência de tal objetivo prendia-se com o facto de, até ao momento, nos casos que surgiram nos tribunais portugueses, existirem grandes dificuldades de qualificação dos comportamentos pela proximidade aparente entre o *pharming* e o *phishing*, embora o primeiro se mostre bem mais sofisticado e lesivo.

Por esse motivo, começámos por distinguir os dois ataques – que, apesar de semelhantes, divergem em múltiplos aspetos –, para que assim se possam delimitar concretamente os dois planos fácticos o que, em termos de decisões judiciais, acarreta consequências jurídicas bastante díspares.

Para além disso, e porque ainda não existem decisões judiciais capazes de conduzir o ataque de *pharming* a tipos legais definidos (havendo um vazio de enquadramento de tal conduta informática do ponto de vista penal), visou a nossa dissertação, num segundo momento, subsumir os comportamentos concretos do *pharmer* aos respetivos tipos legais.

Subdividimos então a atuação do agente em duas fases essenciais: a primeira, que visa a obtenção não autorizada de dados pessoais; e a segunda, na qual o criminoso utiliza esses dados para diversos fins. Como pela experiência se sabe que estes ataques têm em vista, na esmagadora maioria dos casos, o enriquecimento próprio e/ou de terceiros, circunscrevemo-nos às condutas aptas a lesar bens jurídicos de carácter patrimonial, tendo abordado os tipos legais lesivos de bens jurídicos pessoais a título meramente exemplificativo.

Colocamos ainda em perspetiva os tipos legais que, em abstrato, poderiam abarcar os diversos comportamentos levados a cabo pelo criminoso, para percebermos os que importavam concretamente para se resolverem as questões que se levantavam acerca do concurso aparente ou de normas entre as disposições legais que considerámos aplicáveis.

Concluímos, por isso, que o tipo legal de Burla Informática ou de Abuso de cartão de crédito ou de garantia – conforme as situações – são os mais adequados à punição de um ataque de *pharming* já que esses tipos englobam de forma bastante todo o juízo de desvalor que deve ser dirigido à atuação do *pharmer*.

Com tais conclusões, pensamos ter atingido todas as metas a que nos propusemos, esperando ter contribuído com uma interpretação clara e elucidativa, em termos de caracterização técnica, e útil, em termos de enquadramento jurídico-penal para que, com isso, se evitem futuras dúvidas a este tema atinentes e se opte pela correta punição que certamente confortará os decisores com a certeza de uma resolução justa e acertada, preocupação que deverá estar na base de qualquer processo de tomada de decisão.

Por fim, serviu ainda este trabalho para perceber que muito há ainda a fazer em termos de consciência tecnológica, uma vez que o atual êxtase perante os incontáveis progressos informáticos não é acompanhado pela correspondente compreensão das implicações que lhes estão inerentes.

Nessa medida, nunca bastarão unicamente os meios técnicos de segurança para evitar os atentados perpetrados através da Internet, sendo talvez

mais importante um uso prudente e informado de tais ferramentas, de que pensamos não poder prescindir, mas que devem ser encaradas como possíveis ameaças quando utilizadas de forma leviana.

BIBLIOGRAFIA

AA.VV. – **Cibercriminalidade: Debate**. [Em linha]. 14 de Março de 2014. [Consulta: 27 Jun. /2014] Disponível em
http://www.justicatv.com/index.php?p=4399 ;
http://www.justicatv.com/index.php?p=4402 .

ASCENSÃO, José de Oliveira – **Criminalidade Informática**. In **Estudos sobre Direito da Internet e da Sociedade de Informação**. Almedina, 2001.

ASLAM, Baber; WU, Lei; C. ZOU, Cliff – **PwdIP-Hash: A Lightweight Solution to Phishing and Pharming Attacks**. [Em linha]. In **Network Computing and Applications (NCA), 2010 9th IEEE International Symposium on Computing and Applications**. Cambridge MA: IEEE, pp. 198-203. [Consulta: 27 Jun. /2014] Disponível em https://webvpn.uminho.pt/http/80/ieeexplore.ieee.org/xpl/articleDetails.jsp?reload=true&arnumber=5598209

BARREIROS, J. A. – **Crimes contra o património**. Universidade Lusíada, 1996.

BLOOMBECKER, J.J. Buck – **Computer crime and abuse**. In HOLLINGER, Richard C., (ed.) -, **Crime deviance and the computer**. Aldershot / Brookfield USA / Singapore / Sydney, Dartmouth: 1997.

BRODY, Richard G. ; MULIG, Elizabeth ; KIMBALL, Valerie – **Phishing, Pharming and identity theft**. [Em linha]. Academy of Accounting and Financial Studies Journal, September 2007. Volume 11 (3), pp. 43 – 56 (14). [Consulta: 27 Jun. /2014]. Disponível em
http://www.freepatentsonline.com/article/Academy-Accounting-Financial-Studies-Journal/166823523.html .

CENTRALSERVER – **Certificado SSL**. [Em linha]. [Consulta: 16 Out. /2014] Disponível em
http://www.centralserver.com.br/ferr_ssl_o_que_e.php .

COMISSÃO DE REVISÃO DO CÓDIGO PENAL, Lisboa, 1993 - **Actas e Projecto da Comissão de Revisão**. Lisboa: Ministério da Justiça, Rei dos Livros, 1993.

CORREIA, Eduardo – **Direito Criminal: Volume I** (com colaboração de Figueiredo Dias). Almedina, 2014.

– **Direito Criminal: Volume II** (com colaboração de Figueiredo Dias). Almedina, 2010.

– **A teoria do concurso em Direito Criminal**. 2ª edição (reimpressão). Coimbra: Livraria Almedina, 1996.

COSTA, Francisco Bruto da ; BRAVO, Rogério – **Spam e Mail Bomb: Subsídios para um perspectiva criminal**. Lisboa: Quid Iuris, 2005.

COSTA, José Faria – **Formas do crime**. In **Jornadas de Direito Criminal: O novo Código Penal Português e Legislação Complementar**. Fase I. Lisboa: CEJ, 1983.

COSTA, José Faria ; MONIZ, Helena – **Algumas reflexões sobre a criminalidade informática em Portugal**. In **Boletim da FDUC**. Volume LXXIII (separata). Coimbra: 1997.

DENNING, Dorothy E. – **The United States vs. Craig Neidorf: a debate on electronic publishing constitutional rights and hacking**. In HOLLINGER, Richard C. (ed.) - **Crime deviance and the computer**. Aldershot / Brookfield USA / Singapore / Sydney, Dartmouth: 1997, pp.471-489.

DESCONHECIDO – **Ataque de negação de serviço**. [Em linha]. [Consulta: 16 Out. /2014] Disponível em
http://pt.wikipedia.org/wiki/Ataque_de_nega%C3%A7%C3%A3o_de_servi%C3%A7o .

DESCONHECIDO – **Autoridade de Certificação**. [Em linha]. [Consulta: 29 Nov. /2014] Disponível em
http://pt.wikipedia.org/wiki/Autoridade_de_Certifica%C3%A7%C3%A3o .

DESCONHECIDO – **Bit**. [Em linha]. [Consulta: 14 Nov. /2014] Disponível em
http://pt.wikipedia.org/wiki/Bit .

DESCONHECIDO – **Criptografia**. [Em linha]. [Consulta: 29 Nov. /2014] Disponível em
http://cartilha.cert.br/criptografia/ .

DESCONHECIDO – **DNSSEC**. [Em linha]. [Consulta: 29 Nov. /2014] Disponível em
http://pt.wikipedia.org/wiki/DNSSEC .

DESCONHECIDO – **Dynamic Host Configuration Protocol**. [Em linha]. [Consulta: 14 Nov. /2014] Disponível em
http://pt.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol .

DESCONHECIDO – **IPv6**. [Em linha]. [Consulta: 14 Nov. /2014] Disponível em
http://pt.wikipedia.org/wiki/IPv6 .

DESCONHECIDO – **Firewall**. [Em linha]. [Consulta: 29 Nov. /2014] Disponível em
http://pt.wikipedia.org/wiki/Firewall .

DESCONHECIDO – **List of Internet Top-Level Domains**. [Em linha]. [Consulta: 25 Nov. /2014] Disponível em
http://en.wikipedia.org/wiki/List_of_Internet_top-level_domains .

DESCONHECIDO – **O que é Criptografia**? [Em linha]. [Consulta: 29 Nov. /2014] Disponível em
http://www.oficinadanet.com.br/artigo/443/o_que_e_criptografia .

DESCONHECIDO – **Proxy**. [Em linha]. [Consulta: 16 Out. /2014] Disponível em
http://pt.wikipedia.org/wiki/Proxy .

DESCONHECIDO – **Root Zone Database**. [Em linha]. [Consulta: 25 Nov. /2014] Disponível em
http://www.iana.org/domains/root/db .

DESCONHECIDO – **Servidor Web**. [Em linha]. [Consulta: 16 Out. /2014] Disponível em
http://pt.wikipedia.org/wiki/Servidor_web .

DESCONHECIDO – **Sistema de Numeração Binário**. [Em linha]. [Consulta: 14 Nov. /2014] Disponível em
http://pt.wikipedia.org/wiki/Sistema_de_numera%C3%A7%C3%A3o_bin%C3%A1rio .

DESCONHECIDO – **Sistema Operativo**. [Em linha]. [Consulta: 14 Nov. /2014] Disponível em
http://pt.wikipedia.org/wiki/Sistema_operativo .

DESCONHECIDO – **Spam**. [Em linha]. [Consulta: 16 Out. /2014] Disponível em
http://pt.wikipedia.org/wiki/Spam .

DESCONHECIDO – **Spyware**. [Em linha]. [Consulta: 16 Out. /2014] Disponível em
http://pt.wikipedia.org/wiki/Spyware .

DESCONHECIDO – **Top-level Domain**. [Em linha]. [Consulta: 25 Nov. /2014] Disponível em
http://en.wikipedia.org/wiki/Top-level_domain .

DESCONHECIDO – **URL**. [Em linha]. [Consulta: 16 Out. /2014] Disponível em
http://pt.wikipedia.org/wiki/URL .

DESCONHECIDO – **Vírus de computador**. [Em linha]. [Consulta: 16 Out. /2014] Disponível em
http://pt.wikipedia.org/wiki/V%C3%ADrus_de_computador .

DESCONHECIDO – **What is DNSSEC?** [Em linha]. [Consulta: 25 Nov. /2014] Disponível em
http://www.dnssec.net/ .

DESCONHECIDO – **.arpa**. [Em linha]. [Consulta: 25 Nov. /2014] Disponível em
http://en.wikipedia.org/wiki/.arpa .

DIAS, Jorge de Figueiredo – **Direito Penal: Parte Geral, Tomo I**. Coimbra: Coimbra Editora, 2007.

- **Direito Penal Português: as consequências jurídicas do crime**. Coimbra: Coimbra Editora.
- **Sumários e notas das Lições do Professor Doutor Jorge de Figueiredo Dias ao 1º ano do curso complementar de Ciências Jurídicas da Faculdade de Direito de 1975-1976**.
- (coord.) **Comentário Conimbricense do Código Penal**. Coimbra: Coimbra Editora.

DIAS, Vera Marques – **A problemática da investigação do cibercrime**. Lisboa: Universidade de Lisboa, 2010.

DURHAM, Cole – **The emerging structures of criminal information law: tracing the contours of a paradigm**. In Revue International de Droit Penal. Nº 1-2, 1993, pp. 79-117.

DUQUE, Jorge - **Cibercriminalidade**. [Em linha]. 14 de Março de 2014. [Consulta: 27 Jun. /2014] Disponível em http://www.justicatv.com/index.php?p=4401 .

ELLIOTT – **Elliot's and Woods cases and materials on criminal law**. 7th edition. London: Sweet & Maxwel, 1997.

EUROPA, Conselho da – **Minuta em Português do Relatório Explicativo da Convenção sobre Cibercrime**. 23/11/2001.

EUROPEIA, Comissão – **Comunicação da Comissão ao Parlamento Europeu e ao Conselho – Estratégia de segurança interna da EU em acção: cinco etapas para uma Europa mais segura**. Bruxelas: 2010, COM 673 final.

- **REGULAMENTO (CE) Nº 1023/2009 de 29 de Outubro de 2009** que aplica o Regulamento (CE) n.o 808/2004 do Parlamento Europeu e do Conselho relativo às estatísticas comunitárias sobre a sociedade da informação. 2009.
- **Resposta à pergunta escrita apresentada por Cristiana Muscardina à Comissão Europeia**. 13 de Março de 2007. Disponível em http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2007-0319&language=PT
- **Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions: A strategy for a Secure Information Society – ''Dialogue, partnership and empowerment''**. 2006 (251).

FAZENDA, Maria Helena – **Cibercriminalidade**. [Em linha]. 14 de Março de 2014. [Consulta: 27 Jun. /2014] Disponível em http://www.justicatv.com/index.php?p=4390 .

FLOR, Roberto – **Phishing, Identity Theft and Identity Abuse: Le Prospecttive applicative del diritto penale** vigente. In **Revista Italiana di diritto e procedura penale**. Fasc 2/3, Aprile-Settembre 2007, 899/946.

FOX, Mark A. – **Phishing, Pharming and Identity Theft in the Banking Industry**. In **Journal of International Banking Law and Regulation**. Issue 9, 548/552, Sweet and Maxwel, 2006.

GASTELLIER – PREVOST, Sophie ; LAURENT, Maryline. – **Defeating pharming attacks at the client-side**. [Em linha]. In **Networking and Information Technology (ICNIT), International Conference on Networking and Information Technology**. France: 2011. [Consulta: 27 Jun. /2014] Disponível em https://webvpn.uminho.pt/http/0/ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6059957 .

GONÇALVES, M. Maia – **Código Penal Português Anotado e Comentado: Legislação Complementar**. 11ª Edição. Coimbra: Livraria Almedina, 1997.

GRABOSKY, P. N. ; SMITH, Russel G. – **Crime in Digital Age**. New Jersey / Annandale: Transaction Publishers, 1998.

GUIMARÃES, Maria Raquel – **Cadernos de Direito Privado, nº41**. Janeiro/Março de 2013.

HAFNER, Katie – **Morris Code**. In HOLLINGER, Richard C. (ed.) – **Crime, deviance and the computer**. Aldershot / Brookfield USA / Singapore/ Sydney, Dartmouth: 1997, pp. 433-434.

HAFT, Fritjof - Das Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität (2 WiKG). In Neue Zeitschrift fur Strafrecht. Heft 1, 1987, pp. 6-10.

HAN, Weili ; CAO, Ye ; YONG, Jianming – **Using automated individual white-list to protect web digital identities.** [Em linha]. In **Expert Systems with Applications**. 39 (2012), pp. 11861-11869. [Consulta: 27 Jun. /2014] Disponível em www.sciencedirect.com/science/article/pii/S0957417412002643 .

HOLLINGER, Richard C. ; LANZA-KADUCE, Lonn – **The process of criminalization: the case of computer crime laws**. In HOLLINGER, Richard C. (ed.) – **Crime, deviance and the computer**. Aldershot / Brookfield USA / Singapore / Sydney, Dartmouth: 1997, pp. 59-119.

HUREWITZ, Barry J. ; LO, Allen M. – **Computer-related crimes**. In HOLLINGER, Richard C. (ed.) – **Crime, deviance and the computer**.

Aldershot / Brookfield USA / Singapore / Sydney, Dartmouth: 1997, pp. 313-339.

INTERNATIONAL, McConnell – **Cyber Crime… and Punishment? Archaic Laws Threaten Global Information**. Washington, 2000. McConnell International LLC.

KOŠČIK, Michal – **European ICT Law 2012: texts, cases, materials**. Masaryk University, 2012.

LAMB, Gregory M. – **New twist on 'phishing' scam – 'pharming'**. [Em linha]. In **Christian Science Monitor**. 5/5/2005, Volume 97, Issue 113, pp. 13-14. [Consulta: 27 Jun. /2014] Disponível em https://webvpn.uminho.pt/http/0/web.b.ebscohost.com/ehost/detail/detail?sid=c302a4bc-66c8-4199-9a3c.68916e762dbd%40sessionmgr198&vid=0&hid=112&bdata=JnNpdGU9ZWhvc3QtbGl2ZSZzY29wZT1zaXRl .

LINANT DE BELLEFORDES, Xavier – **A informática e o Direito**. GB&A, 2001.

LLOYD, Ian J. · **Information technology law**. London / Dublin / Edinburgh, Butterworths: 1993.

MACEDO, João Carlos Cruz Barbosa de – **Algumas considerações acerca dos crimes informáticos em Portugal**. In M.d.C.A.e.l.c. Neves, (ed.), **Direito Penal Hoje – Novos desafios e novas respostas**. Coimbra: Coimbra Editora, 2009.

MAGAZINE, Harper's – **Is computer hacking a crime?** In HOLLINGER, Richard C. (ed.) – **Crime, deviance and the computer**. Aldershot / Brookfield USA / Singapore / Sydney, Dartmouth: 1997, pp.435-446.

MANZINI – **Trattato do Diritto Penale Italiano**. 1935, VI.

MARQUES, Lourenço Martins Garcia – **Direito da Informática**. In **Lições de Direito da Comunicação**. 2ª Edição. Coimbra: Almedina, 2006.

MARTINS, A. G. Lourenço – **Criminalidade Informática**. In **Direito da Sociedade de Informação**. Coimbra: Coimbra Editora, 2003.

MARTINS, Lourenço ; GARCIA, Marques – **Direito da Informática**. 2ª Edição. Coimbra: Almedina, 2006.

MATHEW, A.R. ; AL HAJJ, A. ; AL RUQEISHI, K. – **Cyber crimes: Threats and protection**. [Em linha]. In **Networking and Information Technology (ICNIT), International Conference on Networking and Information Technology**. Manila: 2010, pp. 16-18. [Consulta: 27 Jun. /2014]. Disponível em https://webvpn.uminho.pt/http/0/ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=5508568 .

MATOS, José António Alves de – **Dicionário de Informática e de Novas Tecnologias.** Lisboa: L. FCA, Editora de Informática, Lidel – Edições Técnicas, Lda., 2009.

MONIZ, Helena - **Internet e globalização: problemas jurídico-penais. Notas breves**. In MONTEIRO, António Pinto (coord.) - **As telecomunicações e o direito na sociedade da informação**. Actas do Colóquio organizado pelo ICJ em 23 e 24 de Abril de 1998. Coimbra: Instituto Jurídico da Comunicação, Faculdade de Direito, Universidade de Coimbra, 1999, pp. 367-385.

– **O crime de falsificação de documentos: da falsificação intelectual e da falsidade de documento**. Livraria Almedina, 1993.

MUSCARDINI, Cristiana – **Pergunta escrita E-0319/07 apresentada à Comissão Europeia, ''Phishing'' e ''Pharming''.** [Em linha]. 2007. [Consulta: 27 Jun. /2014] Disponível em http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+WQ+E-2007-0319+0+DOC+XML+V0//PT .

MÜHLEN, Rainer A. H. von zur ; SCHOLTEN, Rainer - **Computer-Manipulationen aus strafrechtlicher Sicht**. In Neue Juristische Wochenschrift. Heft 37, 1971, pp. 1642-1643.

NUNES, Carlos - **Cibercriminalidade**. [Em linha]. 14 de Março de 2014. [Consulta: 27 Jun. /2014] Disponível em http://www.justicatv.com/index.php?p=4397 ; http://www.justicatv.com/index.php?p=4395 .

NELSON, Brenda - **Straining the capacity of the law: the idea of computer crime in the age of the computer worm**. In HOLLINGER, Richard C. (ed.) - **Crime, deviance and the computer**. Aldershot / Brookfield USA / Singapore / Sydney, Dartmouth: 1997, pp. 273-295.

NILSSON, Hans G. - **Computer crimes and other crimes against information technology within the working programme of the Council of Europe**. In **Revue International de Droit Pénal**. N° 1-2, 1993, pp. 119-125.

OBIED, Ahmed ; ALHAJJ, Reda – **Fraudulent and malicious sites on the web**. In **Applied Intelligence**. [Em linha]. April 2009, Volume 30, Issue 2, pp. 112-120. [Consulta: 27 Jun. /2014] Disponível em https://webvpn.uminho.pt/http/0/link.springer.com/article/10.1007/s10489-007-0102-y .

OLIVEIRA, Wilson – **Técnicas para Hackers: Soluções para segurança**. 1ª edição. Centro Atlântico, 2000.

OLLMANN, Gunter – **The Phising Guide: Understanding & Preventing Phishing attacks**. IBM Global Technology Services. USA, 2007.

- **The Pharming Guide: Understanding & Preventing DNS-related attacks by Phishers**. 2005, Next Generation Securuty Software Ltd.

PALMA, Maria Fernanda ; PEREIRA, Rui Carlos - **O crime de burla no código penal de 1982-95**. In **Revista da Faculdade de Direito da Universidade de Lisboa**. Volume XXXV, 1994, pp. 321-333.

PARKER, Donn B. - **Computer-related white-collar crime**. In GEIS, Gilbert ; STOTLAND, Erza (eds.) - **White-collar crime**, Theory and research («Sage Criminal Justice SystemAnnuals»). London: Sage Publications, 1980, pp. 199-220.

PÊGO, Fernanda - **Cibercriminalidade**. [Em linha]. 14 de Março de 2014. [Consulta: 27 Jun. /2014] Disponível em
http://www.justicatv.com/index.php?p=4394;
http://www.justicatv.com/index.php?p=4396 ;
http://www.justicatv.com/index.php?p=4398 .

PEREZ MANZANO, Mercedes - **Acerca de la imputación objetiva de la estafa**. In **Hacia un derecho penal económico europeo**. Jornadas en honor del Profesor Klaus Tiedemann. Madrid: Boletín Oficial del Estado, 1995, pp. 285-309.

PERLINGEIRO, Ricardo ; RIBEIRO, Fernanda ; NETO, Luísa – **Direito e Informação: que responsabilidade(s)?**. Editora UFF, 2013.

PFISTER, Wally – **Transcendence**. Warner Bros. Productions, 2014, DVD Blue Ray, 120 minutos.

PFUHL, JR., Erdwin H. - **Computer abuse: problems of instrumental control**. In HOLLINGER, Richard C. (ed.) - **Crime, deviance and the computer**. Aldershot / Brookfield USA / Singapore / Sydney, Dartmouth: 1997, pp. 107-121.

PORTELA, Irene – **A intercepção legal de comunicações em redes IP**. In **Têkhne**, Revista de Estudos Politécnicos. IPCA, 2008.

PRADA, Ignácio Flores – **Criminalidad Informática: Aspectos substantivos y procesales**. Editorial Tirant lo Blanch, S. L.m 2012.

PROVEN SECURITY, McAfee – **Phishing and Pharming: Understanding phishing and pharming**. 2006.

RENDING, Comissão Europeia – **Answer to the questions of Cristiana Muscardini**. [Em linha]. 2007. [Consulta: 27 Jun. /2014] Disponível em http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2007-0319&language=PT .

RENGIER, Rudolf - **Strafrecht. Besonderer Teil I. Vermögensdelikte**, München, C. H. Beck'Sche Verlagsbuchhandlung, 1997.

ROCHA, Manuel Lopes da - **Direito da informática nos tribunais portugueses (1990-1998)**. Lisboa: Edições Centro Atlântico, 1999.

- Cibercriminalidade. In Justiça TV, 14 de Março de 2014.[Em linha]. [Consulta: 27 Jun. /2014] Disponível em http://www.justicatv.com/index.php?p=4393 .

RODRIGUES, Ana Paula - **Cibercriminalidade**. [Em linha]. 14 de Março de 2014. [Consulta: 27 Jun. /2014] Disponível em http://www.justicatv.com/index.php?p=4400 .

RODRIGUES, Benjamim Silva – **Direito Penal, Parte especial: Tomo I – Informático-digital**. Rei dos Livros, 2009.

ROUSE, Margaret – **HTTPS (HTTP over SSL or HTTP Secure**. [Em linha]. [Consulta: 29 Nov. /2014] Disponível em http://searchsoftwarequality.techtarget.com/definition/HTTPS .

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

SCHACKELFORD, Steve - **Computer-related crime: an international problem in net international solution**. In HOLLINGER, Richard C. (ed.) - **Crime, deviance and the computer**, Aldershot / Brookfield USA / Singapore / Sydney, Dartmouth: 1997, pp. 347-373.

SCHULTZ, Hartmut C. - **Beck EDV-Berater. Basiswissen: Computerkriminalität**. München: Deutscher Taschenbuch Verlag, 1992.

SILVA, Germano Marques - **Direito Penal Português. Parte Geral. Introdução e teoria da lei penal**. 1ª Edição, Reimpressão. Lisboa: Editorial Verbo, 2001.

SILVA, Júlio Reis - **Direito da informática: Legislação e deontologia**. Lisboa: Edições Cosmos, 1994.

SMITH, Graham J. H. - **Internet Law and Regulation**. Reprinted. London: FT Law & Tax, 1996.

SOTTO-MAYOR, Belmiro ; FERREIRA, Paulo ; LESSA, André – **Aspectos sociais da Informática: Criminalidade Informática – Desafios**

de uma nova geração. Porto: Faculdade de Engenharia da Universidade do Porto, 2006. Prova académica.

STAMM, Sid ; RAMZAN, Zulfikar ; JAKOBSSON, Markus – **Drive-by Pharming**. Technical Report TR641. Indiana University: Department of Computer Science, 2006.

TEIXEIRA, Paulo Gonçalves – **O fenómeno do Phishing, enquadramento jurídico-penal**. Lisboa: Universidade Autónoma de Lisboa, 2013. Dissertação de Mestrado.

UFRGS, Departamento de Engenharia Química da – **Engenharia social (segurança da informação).** [Em linha]. [Consulta: 03 Out. /2014] Disponível em
http://www.enq.ufrgs.br/files/Engenharia%20Social.pdf .

VABRES, Donnedieu de – **Essai sur la notion de préjudice dans la théorie générale du faux documentaire**. 1941.

VENÂNCIO, Pedro – **Lei do Cibercrime: anotada e comentada**. Coimbra Editora, 2011.

VERDELHO, Pedro – **A Convenção sobre cibercrime do Conselho da Europa – Repercussões na lei português**. In **Direito da Sociedade de Informação**. Coimbra: Coimbra Editora, 2006.

- ; BRAVO, Rogério ; ROCHA, Manuel Lopes da - **Leis do Cibercrime**. Volume I, Centro Atlântico, 2003.

- **A obtenção da prova no meio digital**. In Revista do Ministério Público. Nº 99, Julho/Setembro 2004.

- **Phishing e outras formas de defraudação nas redes de comunicação**. In **Direito da Sociedade de Informação**. Volume VIII, 407/419.

- **Comentário à Lei 67/98, de 26 de Outubrro**. In ALBUQUERQUE, Paulo Pinto de (coord.) - **Comentário às Leis Penais Extravagantes**, pp. 438-458.

- **Comentário à Lei 5/2004, de 10 de Fevereiro**. In ALBUQUERQUE, Paulo Pinto de (coord.) - **Comentário às Leis Penais Extravagantes**, pp. 465-469.

- **Comentário à Lei 109/2009, de 15 de Setembro**. In ALBUQUERQUE, Paulo Pinto de (coord.) - **Comentário às Leis Penais Extravagantes**, pp. 505-523.

- **Cibercriminalidade**. [Em linha]. 14 de Março de 2014. [Consulta: 27 Jun. /2014] Disponível em
http://www.justicatv.com/index.php?p=4391 ;
http://www.justicatv.com/index.php?p=4392 .

VIOLINO, Bob – **After Phishing? Pharming! Security experts are concerned about pharming, a technically sphisticated DNS-based attack**. New York: CSO, 2005.

WEISBURD, David [et. al.] - **Crimes of the middle classes: White-collar offenders in the Federal Courts**. New Haven / London: Yale University Press, 1991.

WESSELS, Johannes ; HILLENKAMP, Thomas - **Strafrecht Besonderer Teil / 2. Straftaten gegen Vermögenswerte («Schwerpunkte»)**. 26, Neubearbeitete. Aufl., Heidelberg: C. F. Müller Juristischer Verlag, 2003.

WILSON, Darryl C. - **Viewing computer crime: where does the system error really exist?** In **Computer / Law Journal**. Volume XI, n.° 2, 1991, pp. 265-285.

WISE, Edward M. - **Computer crimes and other crimes against information technology in the United States**. In Revise International de Droit Pénal. N.° 1-2, 1993, pp. 647-669

Wnews – **Você sabe a diferença entre HTTP e HTTPS?** [Em linha]. [Consulta: 29 Nov. /2014] Disponível em http://www.dnt.adv.br/noticias/cibercultura/voce-sabe-a-diferenca-entre-http-e-https/ .

YAR, Majid – **Cybercrime and society**. 2nd edition. SAGE Publications, 2013.

YOUNG-GAB, Kim [et.al] – **A quantitative approach to estimate a website security using whitelist**. In **Security and Communication Networks: Next Generation Communication and Network Security**. [Em linha]. Fevereiro 2012, Volume 5. [Consulta: 27 Jun. /2014] Disponível em http://onlinelibrary.wiley.com/doi/10.1002/sec.420/full .

ZÚQUETE, André – **Segurança em redes informáticas**. 2ª Edição. FCA – Editora de Informática, 2010.