Cyberlaw by CIJIC, ***Direito: a pensar tecnologicamente.***

CYBERLAW by CIJIC

EDIÇÃO N.º IX – MARÇO DE 2020

REVISTA CIENTÍFICA SOBRE CYBERLAW DO CENTRO DE INVESTIGAÇÃO JURÍDICA DO CIBERESPAÇO – CIJIC – DA FACULDADE DE DIREITO DA UNIVERSIDADE DE LISBOA

EDITOR: NUNO TEIXEIRA CASTRO

SUPORTE EDITORIAL: EUGÉNIO ALVES DA SILVA e AFONSO FREITAS DANTAS

PRESIDENTE DO CIJIC: EDUARDO VERA-CRUZ PINTO

CIJIC: CENTRO DE INVESTIGAÇÃO JURÍDICA DO CIBERESPAÇO

ISSN 2183-729

NOTAS DO EDITOR:

Globalização. Tecnologia e Inteligência artificial. Mobilidade organizacional e individual. Manipulação. A pandemia de Coronavírus. Hoje. O futuro.

Vivemos tempos "*estranhos*". Acutilantes. Irresolutos. Contingentes. Exigentes. O "tema" que nos capta, quase em exclusivo, a atenção, desde o início do ano de 2020, é a pandemia de coronavírus. Aquela dinâmica, rotineira, até agora tida como "garantida" atravessa momentos de grande indeterminação. Hora a hora somos como que bombardeados com números esmagadores: de taxas mundiais galopantes de infectados, doentes em cuidados intensivos, de mortos. No passar deste tempo, diariamente, deambulámos entre um imoderado e célere na disseminação da infecção *versus* um vagaroso e fleumático passo na demonstração de resultados animadores no seu combate. O racional económico de «custo-benefício» geralmente revelaria a perigosidade associada à extrema cautela. Porém na questão, truncada, do coronavírus é diferente[1]. "*Achatar as curvas*", "*Proteger os mais idosos e os mais vulneráveis*", "*Suster a vaga de procura do SNS por forma a dar-lhe tempo para acudir às solicitações*", mesmo que o custo seja o parar da Economia. Global. Entretanto o tempo continua o seu passo. Assim como a epidemia há-de passar.

1 Cass Sunstein @ https://www.bloomberg.com/opinion/articles/2020-03-26/coronavirus-lockdowns-look-smart-under-cost-benefit-scrutiny

E, quando aí chegados, a questão resolutiva a colocar não deverá andar muito longe de um: "*Que mundo esperar do pós-covid19*"?

O avanço da tecnologia, combinando melhores recursos de *hardware* com inteligência artificial, aos quais o Homem socorre, permitiram sequenciar o genoma do COVID-19 em menos de um mês. A inteligência artificial, por exemplo, num contexto, global, de recursos exíguos tem sido testada para suprir lacunas críticas nos recursos de saúde, ajudando à racionalidade da decisão política, alavancando centros de inovação em inteligência artificial, robótica e automação em saúde. Na Ásia[2]. Por agora.

O mesmo avanço tecnológico, por sua vez, no actual cenário de "*guerra*" ao vírus, colocou a ponderação das liberdades fundamentais num estádio de confronto titânico. Recuperando o "*achatar a curva*", um pouco por todo o mundo, os governos, democráticos, colocaram os respectivos países em *lockdown*. Sem cautelas. Entre confinamentos e quarentenas obrigatórias, um recurso parece permitir - em face da falta de meios humanos para controlo efectivo de milhões de cidadãos - fiscalizar o cumprimento das directrizes estatais. A tentação executiva por esse controlo, universal, dos cidadãos preclude a fruição de múltiplas liberdades constitucionalmente consagradas. O racional da discussão que vinha sendo tido até agora[3], deslocou-se, por via do perigo abstracto que a pandemia comporta, da questão securitária *versus* liberdades fundamentais para "*saúde pública*" *versus* liberdades fundamentais.

Um pouco por todo o ocidente democrático, a tónica recursiva tem passado pelo uso da "*vigilância digital* estadual[4]". Tal como um pouco por todo o mundo, direitos humanos fundamentais[5] são colocados em teste face à imposição destas regras "excepcionais". O Estado de emergência tende a permitir, justificando múltiplas

---

2 Eficiência, especialidade, racionalidade, sistemas capacitativos e colaborativos público-privados. O trabalho dos dados ao serviço dos povos. https://www.technologyreview.com/s/614555/ai-in-health-care-capacity-capability-and-a-future-of-active-health-in-asia/

3 « Tribunal Constitucional chumba acesso das secretas a registos de comunicações», @ https://rr.sapo.pt/2019/09/19/politica/tribunal-constitucional-chumba-acesso-das-secretas-a-registos-de-comunicacoes/noticia/165164/

4 Por exemplo: https://www.wsj.com/articles/europe-tracks-residents-phones-for-coronavirus-research-11585301401

5 Por exemplo, no contexto da América do Sul, «Sociedade civil pede que tecnologias usadas devido à pandemia respeitem os Direitos Humanos», @ https://idec.org.br/noticia/sociedade-civil-pede-governos-da-america-latina-e-caribe-que-tecnologias-digitais-aplicadas

intrusões como *adequadas*[6], *necessárias e proporcionais*[7]. A questão, sendo excepcional e de carácter limitada no tempo, deveria ser pacificamente tolerada pelos cidadãos. Afinal, sob o manto de um fundamento como o "*interesse público*" [8] e salvaguarda da "*saúde pública*" até a limitação do escopo de protecção, desde logo, da privacidade de dados pessoais sensíveis claudica[9].

---

6 No parecer 32/2020, a CNPD, delimitando geograficamente a aplicação de videovigilância por drones ao concelho de Ovar, dada a excepcionalidade da cerca sanitária entretanto imposta, reitera que "(…)as restrições aos direitos fundamentais devem limitar-se ao estritamente necessário às finalidades visadas com este sistema de videovigilância ", recomendando, adicionalmente, "que se garanta que a captação de imagens assim realizada salvaguarde a privacidade daqueles que se encontrem nas respectivas habitações", e, "que se garanta o direito de acesso às imagens gravadas , nos termos legalmente previstos", bem como que se adoptem "medidas adequadas a garantir a integridade das imagens gravadas no processo de transferência dos registos(…) para o "contentor de informação encriptado"" . @ https://www.cnpd.pt/home/decisoes/Par/PAR_2020_32.pdf

7 Por exemplo, em Espanha, a AEPD: «(…)*Los fundamentos que legitiman/hacen posible dichos tratamientos son la necesidad de atender las misiones realizadas en interés público, así como la de garantizar los intereses vitales de los propios afectados o de terceras personas.* ***Las finalidades para las que pueden tratarse los datos son, únicamente, las relacionadas con el control de la epidemia****, entre ellas, las de ofrecer información sobre el uso de las aplicaciones de autoevaluación realizadas por las administraciones públicas o la obtención de estadísticas con datos de geolocalización agregados para ofrecer mapas que informen sobre áreas de mayor o menor riesgo.* ***Los datos que pueden obtenerse y utilizarse han de ser los que las autoridades públicas competentes consideren proporcionados/necesarios para cumplir con dichas finalidades.*** *Estos datos sólo podrán ser facilitados por quienes sean mayores de 16 años. En el caso de tratar datos de menores de 16 años, se requeriría de la autorización de sus padres o representantes legales.* ***Únicamente podrán tratar dichos datos las autoridades públicas competentes para actuar conforme a la declaración del estado de alarma****, es decir, el Ministerio de Sanidad y las Consejerías de Sanidad de las Comunidades Autónomas, que podrán cederse datos entre ellas, y a los profesionales sanitarios que traten a los pacientes o que intervengan en el control de la epidemia.****Las entidades privadas que colaboren con dichas autoridades sólo podrán utilizar los datos conforme a las instrucciones de estas y, en ningún caso, para fines distintos de los autorizados.»*** @ https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/aepd-apps-webs-autoevaluacion-coronavirus-privacidad

8 A limitação ao tratamento de dados sensíveis, por exemplo, de saúde sucumbe ante "*razões de interesse público nos domínios da saúde pública*", desde que «(…)***Tais atividades de tratamento de dados sobre a saúde autorizadas por motivos de interesse público não deverão ter por resultado que os dados sejam tratados para outros fins por terceiros, como os empregadores ou as companhias de seguros e entidades bancárias»*** (Considerando 54 in fine) .

Considerando *(54) « O tratamento de categorias especiais de dados pessoais pode ser necessário por razões de interesse público nos domínios da saúde pública, sem o consentimento do titular dos dados. Esse tratamento deverá ser objeto de medidas adequadas e específicas, a fim de defender os direitos e liberdades das pessoas singulares. Neste contexto, a noção de «saúde pública» deverá ser interpretada segundo a definição constante do Regulamento (CE) n.o 1338/2008 do Parlamento Europeu e do Conselho (11), ou seja, todos os elementos relacionados com a saúde, a saber, o estado de saúde, incluindo a morbilidade e a incapacidade, as determinantes desse estado de saúde, as necessidades de cuidados de saúde, os recursos atribuídos aos cuidados de saúde, a prestação de cuidados de saúde e o acesso universal aos mesmos, assim como as despesas e o financiamento dos cuidados de saúde, e as causas de mortalidade(…)****».***

9 Confirmando o Considerando (54), ainda, da leitura conjunta **das alíneas g) e i) do Art.o 9, n.º2, RGPD**: «**G)** *Se o tratamento for necessário por motivos de interesse público importante, com base no direito da União ou de um Estado-Membro, que deve ser proporcional ao objetivo visado, respeitar a essência do direito à proteção dos dados pessoais e prever medidas adequadas e específicas que salvaguardem os direitos fundamentais e os interesses do titular dos dados*;», e**, i)** « *Se o tratamento for* ***necessário por motivos de interesse público no domínio da saúde pública, tais como a proteção contra ameaças transfronteiriças graves para a saúde*** *ou para assegurar um elevado nível de qualidade e de*

Mas há um "*senão*". O receio de que a excepcionalidade vire regra é real[10]. Com efeito, é inegável que, neste momento, os receios de Yuval Harari [11], criador de *Homo Deus*, sejam partilhados por muitos de nós. Tal como as considerações de Joel P. Trachtman, quanto aos benefícios de um mundo global[12]: benéfico se mais cooperativo, com capacidades regulatórias internacionais reforçadas ao nível da saúde, cibersegurança, proteção ambiental e crises financeiras.

Ambos convergem na necessidade de compromisso, de partilha, cooperação e solidariedade global. O que se conclui espontaneamente dos apontamentos citados, através de um silogismo categórico: ameaça sobre todos os países, ameaça global, logo, resposta de todos os países, global. Não obstante, será que hoje temos líderes políticos mundiais à altura dos desafios[13] pungentes que se nos colocam nestes termos?

E no futuro?

---

segurança dos cuidados de saúde e dos medicamentos ou dispositivos médicos, com base no direito da União ou dos Estados-Membros que preveja medidas adequadas e específicas que salvaguardem os direitos e liberdades do titular dos dados, em particular o sigilo profissional;». @ https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679

10 Yuval Harari:«(…) *Many short-term emergency measures will become a fixture of life. That is the nature of emergencies. They fast-forward historical processes. Decisions that in normal times could take years of deliberation are passed in a matter of hours. Immature and even dangerous technologies are pressed into service, because the risks of doing nothing are bigger.", @* https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75

11 Harari: «(…) *In this moment of crisis, the crucial struggle takes place within humanity itself. If this epidemic results in greater disunity and mistrust among humans, it will be the virus's greatest victory. When humans squabble – viruses double. In contrast, if the epidemic results in closer global cooperation, it will be a victory not only against the coronavirus, but against all future pathogens*.», @ https://time.com/5803225/yuval-noah-harari-coronavirus-humanity-leadership/

12 Joel P. Trachtman, «(…) *Not all global problems result from globalization. For those that do, globalization itself can ameliorate them to some extent. Furthermore, we can establish international laws and institutions to minimize those problems that do arise from globalization: globalized governance to respond to globalization-induced problems. This is smart globalization, and once we do it this way, it is likely that globalization should be retained because, on net, it will make us better off*.", @ https://www.bostonglobe.com/2020/03/30/opinion/not-all-global-problems-result-globalization/

13 Ainda Harari: «(…)*Today humanity faces an acute crisis not only due to the coronavirus, but also due to the lack of trust between humans. To defeat an epidemic, people need to trust scientific experts, citizens need to trust public authorities, and countries need to trust each other. Over the last few years, irresponsible politicians have deliberately undermined trust in science, in public authorities and in international cooperation. As a result, we are now facing this crisis bereft of global leaders that can inspire, organize and finance a coordinated global response*.», *idem*.

Gerd Leonhard, num exercício curioso reproduzido no Diário de Notícias, destaca dois aspectos cruciais. Circunscrevendo-nos à tecnologia, esta *"tornou-se a nova religião"*. "*Estamos a entrar num novo Renascimento*". *O próximo passo será regulamentá-la de forma mais apertada com o objetivo de que humanos e o próprio planeta beneficiem do progresso tecnológico.* Não obstante, esta relação acabará seduzir-se ante uma *vigilância estatal por meios tecnológicos* (que) *irá tornar-se o novo normal após as medidas extraordinárias que foram tomadas para controlar esta pandemia*[14].

E como já vai longo, para concluir, convocamos, novamente, a questão fundamental: "*Que mundo esperar do pós-covid19*"?

A provocação desconcertante e acutilante que se impõe, inclusive politicamente, não poderia ser outra: «*Of course, even if we disappear, it will not be the end of the world. Something will survive us. Perhaps the rats will eventually take over and rebuild civilization. Perhaps, then, the rats will learn from our mistakes. But I very much hope we can rely on the leaders assembled here, and not on the rats.*» [15]

Nesta nova edição da «Cyberlaw by CIJIC», procuramos sustentar o crescimento paralelo que o Mestrado de Segurança da Informação e Direito do Ciberespaço[16] vai granjeando. É pois, com orgulho, que passaremos a destacar produção deste, com maior regularidade. Afinal, este é um desígnio da própria criação da revista. Provavelmente, num futuro não muito distante, estará na calha a edição em papel de futuras edições. Se há questão que se nos colocou com o teletrabalho foi: qual a redundância digital? *Ie*, sem acesso à internet, ou sem eletricidade/bateria, como é que seria possível aceder

14 «Não haverá normal: futuristas preveem mudanças permanentes pós-coronavírus», @ https://www.dn.pt/dinheiro/nao-havera-normal-futuristas-preveem-mudancas-permanentes-pos-coronavirus-11987179.html

15 Yuval Harari: «Yuval Harari's blistering warning to Davos», @ https://www.weforum.org/agenda/2020/01/yuval-hararis-warning-davos-speech-future-predications/

16 Mais informações @ : https://fenix.tecnico.ulisboa.pt/cursos/msidc

a conteúdos para efeitos de estudo? Como ler(aceder) nestas circunstâncias? Como mitigar a "info-exclusão" quando o sistema não é propriamente redundante na acessibilidade[17]?

Reavendo, nesta edição, incorporando conteúdo em inglês escrito, por força de deveres de participação, cooperação e colaboração internacional[18] que muito nos orgulha, procuramos revisitar temas como cibersegurança em contexto marítimo, dados pessoais e dados não pessoais, monitorização de trabalhadores em contexto laboral, a regulação jurídica do ciberespaço - mutação do paradigma à luz do acórdão James Elliot, *Phishing*, redes sociais e manipulação da opinião pública, o problema da mobilidade em contexto organizacional, e, os desafios da cibersegurança forense de *smartphones* no continente africano. Os temas são oportunos. São, igualmente, desafiantes. São, finalmente, abertos a colaboração múltipla, participada.

Resta-me agradecer a todos quantos contribuíram para mais uma edição da Revista, pelo esforço, pela disponibilidade, pela obra, endereçando a todos, em nome do Centro de Investigação Jurídica do Ciberespaço – CIJIC – da Faculdade de Direito da Universidade de Lisboa, um justíssimo: - Muito Obrigado.

Cyberlaw by CIJIC, ***Direito: a pensar tecnologicamente*.**

Boas leituras.

Lisboa, FDUL, 29 de Março de 2020

Nuno Teixeira Castro

17 Por exemplo, «Ministro Siza Vieira admite aulas por canais "estilo youtube" ou TV por cabo.», @ https://observador.pt/2020/03/29/ministro-siza-vieira-admite-aulas-por-canais-estilo-youtube-ou-tv-por-cabo/
Mas, sem acesso internet, ou sem cabo – até porque a cobertura não é de 100%, há, pelo menos, cerca de 20% de famílias sem acesso ao Cabo – como é que as crianças e adolescentes que se encontrem nesta situação se integram? Como é que se combate esta exclusão digital?
18 Um trabalho colaborativo ímpar. @ https://networkofcenters.net/center/cyberlaw-research-centre-university-lisbon-school-law-cijic

CYBERLAW

by CIJIC

DOUTRINA

O FENÓMENO DO PHISHING

ANTÓNIO RAMOS CARVALHO [1]

1 Mestrando em Segurança da Informação e Direito do Ciberespaço no Instituto Superior Técnico da Universidade de Lisboa (IST-UL), em parceria com a Faculdade de Direito e com a Escola Naval; Mestre em Ciências Militares Navais, Especialidade de Marinha; Especialização profissional em Comunicações e Sistemas de Informação.

RESUMO

A sociedade em que vivemos, comumente apelidada de sociedade da informação, tem vindo a oferecer um leque alargado de potencialidades para os estados e para os cidadãos, no qual a internet, os computadores, os telemóveis, os e-mails e os SMS fazem parte indissociável do seu quotidiano.

Porém, a utilização massiva da informática e da internet, se, por um lado, desempenha um papel essencial para o desenvolvimento, por outro, assume-se como plataforma facilitadora da prática de atos ilícitos, contra as pessoas, o património ou a própria estrutura organizativa da sociedade.

Neste âmbito, o fenómeno de *phishing* tem tido um crescimento exponencial ao longo dos últimos anos, e, em consequência das elevadas quantias monetárias que são subtraídas ilegalmente com esta atividade, tem existido uma crescente preocupação no seio da nossa sociedade, com os impactos sociais e económicos resultantes da concretização desta técnica fraudulenta.

O presente artigo tem como objetivo discutir o fenómeno de phishing, efetuando uma análise da problemática decorrente do modus operandi em Portugal, no que concerne ao seu enquadramento jurídico-penal, concretamente no âmbito da Falsidade Informática (art.º 3) e do Acesso Ilegítimo (artº 3) da Lei do Cibercrime, e ainda ao abrigo da Burla Informática e nas Comunicações (art. 221 do Código Penal).

Palavras-Chave: Cibercrime, Ataques Informáticos, Phishing, Correio Eletrónico e Combate ao Cibercrime.

ABSTRACT

Modern society, frequently called as information society, has been providing a huge potential for the states and for the citizens. Nowadays, the internet, the computers, the mobile phones, the emails and the SMS are an essential part of our daily lives. For instance, in 2018 the number of active internet users worldwide ascended to 4.021 billion, about 53% of the world population [1].

However, the massive use of information technology and the internet, if on the one hand plays an essential role for development, on the other, it assumes itself as a facilitating platform for the practice of illicit acts, against people, estate and the own structure of society.

In this context, the phenomenon of phishing has been growing exponentially over the past few years. Due to the high monetary amounts that are illegally subtract from phishing activity, there has been a rising concern within our society, about the social and economic impacts resulting from the use of this fraudulent technique.

In summary, this paper discusses the phishing phenomenon, doing an analysis of the problem arising from the modus operandi in Portugal, with regard to its legal-penal framework. In particular, it will be analyzed under the crime of Computer Falsehood (art. 3) and Illegitimate Access (art. 3) of the Cybercrime Law, and under computers and Communications spoof (art. 221 of the portuguese Penal Code).

Keywords: Cybercrime, Cyber Attacks, Phishing, Email, Cybercrime Law.

1 According to *Digital 2018* reports from *We Are Social* and *HootSuite*, available in: https://hootsuite.com/pages/digital-in-2018 [21-02-2020].

1. INTRODUÇÃO

Ao longo da última metade do século XX, assistiu-se a uma rápida evolução tenológica, permitindo que as sociedades gerassem elevados índices de crescimento económico e social, e desencadeando o desenvolvimento e adoção de novas Tecnologias de Informação e Comunicação (TIC), as quais moldaram a forma como as pessoas vivem e comunicam entre si, sendo atualmente, vitais ao funcionamento das sociedades modernas.

Esta nova sociedade, comumente apelidada sociedade da informação, tem vindo a oferecer um leque alargado de potencialidades para os estados e para os cidadãos, no qual a internet[1], os computadores, os telemóveis, os e-mails e os SMS fazem parte indissociável do quotidiano.

Porém, a utilização massiva da informática[2] e da internet, se, por um lado, desempenha um papel essencial para o desenvolvimento, por outro, assume-se como plataforma facilitadora da prática de atos ilícitos, contra as pessoas, o património ou a própria estrutura organizativa da sociedade. É neste contexto que Venâncio (2011, p. 15) refere que "as especificidades da criminalidade informática colocam-se, não só na transferência de comportamentos ilícitos para o ambiente digital, como na tipificação de novos crimes com elementos caracterizadores de natureza digital".

1 A origem da internet remonta ao período da presidência de *Eisenhower* nos Estados Unidos da América (EUA), durante a Guerra Fria. Após o lançamento pelos soviéticos do satélite espacial Sputnik, o presidente criou a agência ARPA (*Advanced Research Projects Agency)*, em 1957, com o objetivo de juntar um conjunto de cientistas de renome e competência comprovada, para incrementar a tecnologia espacial. A amplitude de matérias coberta pela ARPA levou à criação de vários departamentos especializados. Na área da informática nasceu o IPTO (*Information Processing Techniques Office*). Neste âmbito, um conjunto coincidente de descobertas desencadeou as fundações da futura internet (Belfiore, 2010).

2 Segundo José Ascensão (2001, p. 203), a informática é "um instrumento automático de elaboração e comunicação de dados".

Deste modo, a criminalidade informática[3] é uma realidade incontornável da nossa sociedade, em constante mutação e evolução, tendo neste âmbito Garcia Marques e Lourenço Martins classificado este conceito como sendo "todo o ato em que o computador serve de meio para atingir um objetivo criminoso ou em que o computador é o alvo desse ato ou em que o computador é objeto do crime" (Marques, 2006, p. 641).

De facto, nos dias de hoje verifica-se um crescimento exponencial das burlas informáticas e as fraudes financeiras à escala internacional. Estima-se que em 2017, mais de 978 milhões de adultos, em 20 países, foram vítimas de cibercrime[4]. Esta tendência verificou-se também em Portugal. De acordo com o Relatório Anual da Segurança Interna (RASI, 2017)[5], o crime de acesso ilegítimo aumentou 13%, a sabotagem informática 32% e a falsidade informática 41%.

Simultaneamente, acompanhando esta evolução, a técnica fraudulenta, denominada por *Phishing*[6], tem tido um crescimento exponencial ao longo dos últimos anos[7], a qual consiste numa forma de furto de identidade *on-line*, que poderá resultar na perda de dados pessoais, particularmente de dados de acesso às contas bancárias, tendo como consequência a subtração de património monetário das vítimas destes crime. Com efeito, o *phishing* assume-se como uma ameaça bastante séria a todos os utilizadores da internet[8], e, por conseguinte, gera uma preocupação constante nas entidades de investigação e nos setores económicos, sobretudo dos utilizadores dos serviços de *homebanking*.

---

3 Em virtude de ser um crime praticado através da internet, existem várias terminologias para designar este tipo de criminalidade, tais como: criminalidade informática, cibercriminalidade, cibercrime, entre outras. Apesar das disposições legais previstas para a criminalidade informática, não existe um conceito expressamente consagrado na lei e uniformemente sedimentado na doutrina e jurisprudência (Marques, 2006).

4 De acordo com Norton (2018); *2017 Norton Cyber Security Insights Report. Global Results*. Disponível em: https://us.norton.com/cyber-security-insights-2017 [06-02-2019].

5 Vd. in Relatório Anual de Segurança Interna de 2017, disponível em: https://www.parlamento.pt/Paginas/2018/abril/EntradaRelSegurancaInterna.aspx [06-02-2019].

6 Este termo, segundo Francisco Luís (Luís, 2011) provém da palavra inglesa *fishing*, fazendo alusão à tentativa de que as vítimas "mordam o anzol" e "caiam" no esquema. Para este efeito, existe a ilusão de que o isco é genuíno. De facto, um atacante terá que criar um "isco" credível e convencer o utilizador a mordê-lo. A nomenclatura *phishing* surgiu em 1996, aquando a sua menção teve lugar num *newsgroup* denominado como *alt.onlineservice. america-online*.

7 Segundo Nelson Amador (2012), da totalidade dos casos de cibercrime identificados em Portugal, 75 % são referentes ao *phishing*. Seguem-se, por ordem, os casos de acesso ilegítimo, dano informático, pornografia de crianças, *software* ilegal e sabotagem.

8 Por exemplo, de acordo com o Special Eurobarometer 423 – Cyber Security Report, aproximadamente 28% dos utilizadores da Internet na União Europeia (UE) não se sentem confiantes para utilizar os serviços de *homebanking* ou para efetuar compras através da internet.

Neste contexto, o presente artigo tem como finalidade definir *phishing* e efetuar uma análise da problemática decorrente do *modus operandi* em Portugal, sobretudo no que respeita ao seu enquadramento jurídico-penal. Para esse efeito, na primeira parte do artigo, serão elencadas algumas das principais causas que estiveram na origem desta atividade criminosa e definido *phishing* ao abrigo da jurisprudência portuguesa. Posteriormente, na segunda parte do artigo, será analisado e caracterizado, resumidamente, o *Modus Operandi* do *phishing* em Portugal, efetuando-se, ainda, um breve enquadramento jurídico-penal da atividade de *phishing*, no âmbito da Falsidade Informática (art.º 3) e do Acesso Ilegítimo (artº 3) da Lei do Cibercrime, e ainda ao abrigo da Burla Informática e nas Comunicações (art. 221 do CP)[9].

9 Face à "economia" do presente artigo, não será efetuado o enquadramento jurídico-penal da atividade de *phishing* ao abrigo das seguintes normas: contrafação, imitação e uso ilegal de marca (art. 323º do DL nº 36/2003, de 5 de Março - Código da Propriedade Industrial); dano relativo a programas ou outros dados informáticos (art. 4º LC); branqueamento (art. 368º-A CP); associação criminosa (art. 299º do CP); apropriação ilegítima em caso de acessão ou de coisa achada (art.º 209º CP); O "furto de identidade" (uso de e-mail e designações bancárias) e o princípio da legalidade.

2. PHISHING

> *"Envio aos internautas de mensagens de correio eletrónico, com a aparência de terem origem em organizações financeiras credíveis, mas com ligações para falsos sítios Web que replicam os originais, e nos quais são feitos pedidos de atualização de dados privados dos clientes"* (CNCS, 2020).

Este novo fenómeno criminal resulta do termo em inglês "*fishing*" e consiste numa das técnicas informáticas que viabiliza o cometimento de burlas informáticas, visando especificamente, tal como o próprio termo deixa antever, "pescar" informação pessoal e confidencial dos utilizadores da internet. Acresce que, geralmente, este tipo de informação obtida ilegalmente, na maioria dos casos, sem que o utilizador se aperceba, é de natureza financeira / bancária, e visa ser utilizada posteriormente, para benefício dos criminosos informáticos, com o consequente prejuízo para as vítimas (Azevedo, 2016).

De um modo mais detalhado, segundo o Supremo Tribunal de Justiça[10], o *phishing* pressupõe:

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

10 Cfr. Acórdão no processo 6479/09.8 TBBRG.G1.S1. Supremo Tribunal de Justiça. [Em linha]. Lisboa (18-12-2013). Disponível em: http://www.dgsi.pt/jstj.nsf [22-02-2020].

Geralmente, o processo mais comum utilizado para a captura da informação concretiza-se, inicialmente, com o envio em massa de mensagens de correio eletrónico de conteúdo fraudulento (SPAM[11]), sob a capa de instituições ou empresas oficiais, podendo, inclusive, conter logotipos e imagens dessas organizações[12]. Com efeito, nesta primeira fase, o criminoso informático tem como objetivo ludibriar o utilizador, levando-o a acreditar que está a receber um *e-mail* cujo remetente é um organismo de natureza público-privado (instituições bancárias, seguradoras, entidades governamentais, entre outros (Verdelho, Phishing e outras formas de defraudação nas redes de comunicação, 2009)).

Simultaneamente, conforme elucida P. Verdelho (2009), o *e-mail* recebido pela vítima poderá incluir uma ligação para uma página web, que, após ser clicada, irá redirecionar o utilizador para essa página falsa, a qual é uma reprodução aproximada do site oficial que os criminosos informáticos pretenderam recriar. Nesta página falsa será solicitado ao utilizador a atualização, validação ou confirmação dos seus dados pessoais, com o pretexto de evitar algum tipo de quebra de segurança. Deste modo, os criminosos informáticos conseguirão obter os dados confidenciais da vítima, a partir dos quais, por exemplo, poderão aceder à sua conta bancária, e, por conseguinte, realizar transferências de montantes de dinheiro sem o consentimento da vítima.

Por outro lado, outra técnica considerada ainda mais sofisticada e perigosa, e que tem sido desenvolvida em simultâneo com o *phishing*, denomina-se por *pharming*, a qual importa sucintamente descrever e elucidar o seu significado, dado que, em diversas ocasiões, é confundida com o *phishing*. Neste caso concreto, o já citado acórdão do STJ de 18 de dezembro de 2013[13], clarifica o seu significado, referindo que esta modalidade de fraude *online* consiste em:

---

11 Segundo G. Marques e L. Martins (2006, p. 655) *Spam* consiste no "envio maciço de mensagens de correio eletrónico não solicitadas, em quantidades que podem não apenas causar incómodo como chegar ao ponto de bloquear o sistema de receção por saturação".

12 Por norma, as mensagens são enviadas para milhares de endereços de e-mail que foram previamente recolhidos na internet, por diversas formas. Neste âmbito, um aspeto importante que importa elucidar consiste no facto de, geralmente o envio dos e-mails ser através de computadores que se encontram sob o controle dos criminosos, e incluem principalmente, servidores web com fragilidades de segurança e em alguns casos computadores pessoais infetados com vírus (p ex. cavalos de troia) criados intencionalmente para permitir o envio de e-mails em massa (spam). Esta rede de computadores infetados por *softwares* maliciosos, controlada remotamente por criminosos, denomina-se por *Botnet* (AVAST, 2019).

13 Cfr. Acórdão no processo 6479/09.8 TBBRG.G1.S1. Supremo Tribunal de Justiça. [Em linha]. Lisboa (18-12-2013). Disponível em: http://www.dgsi.pt/jstj.nsf [22-02-2020].

> "*suplantar o sistema de resolução dos nomes de domínio para conduzir o usuário a uma pagina Web falsa, clonada da página real, baseando-se o processo, sumariamente, em alterar o IP*[14] *numérico de uma direção no próprio navegador, através de programas que captam os códigos de pulsação do teclado (os ditos keyloggers*[15]*), o que pode ser feito através da difusão de vírus via spam, o que leva o usuário a pensar que está a aceder a um determinado site – por exemplo o do seu banco – e está a entrar no IP de uma página Web falsa, sendo que ao indicar as suas chaves de acesso, estas serão depois utilizadas pelos crackers*[16]*, para acederem à verdadeira página da instituição bancária e aí poderem efetuar as operações que entenderem, destinando-se ambas as técnicas (phishing e pharming) à obtenção fraudulenta de fundos*".

Por conseguinte, o *pharming* consiste igualmente na difusão via *spam*, mas desta feita de ficheiros ocultos, os quais de forma encoberta instalam *software* malicioso[17] nos computadores ou sistemas informáticos das vítimas. Deste modo, o utilizador do computador não tem margem para desconfiar de algum indício suspeito, ao contrário do que sucede no *phishing*, onde existe a receção de um e-mail. A partir desse momento, o utilizador acredita que está a aceder a uma página escolhida por si, mas está, na verdade, a aceder ao IP de uma outra página web, controlada pelo criminoso informático (Guimarães, 2013).

O *phishing*, tal como a maioria dos comportamentos maliciosos que ocorrem na web, é uma atividade de dimensão transnacional, que surgiu

14 O IP é a sigla de *Internet Protocol*, o qual é o endereço específico de um equipamento na internet, e estabelece como os pacotes de dados vão da origem ao destino (Marques, 2006).
15 *Keylogger* é um programa de computador do tipo *spyware* cuja finalidade é registar tudo o que é digitado, quase sempre a fim de capturar senhas, números de cartão de crédito (AVAST, 2019).
16 De acordo José Matos (2009, p. 97), *cracker* é "alguém que "quebra" códigos de segurança em sistemas pessoais ou em redes, ou obtém ilicitamente códigos de licença de programas".
17 Também denominado por *Malware*, são programas informáticos destinados a perturbar, alterar ou destruir todos ou parte dos módulos indispensáveis ao bom funcionamento de um sistema informático. São exemplos, os vírus, os vermes, os cavalos de Troia, entre outros (APDSI, 2019).

inicialmente ligada à obtenção de dados de cartões de crédito, mas que atualmente tem como principal alvo os serviços de *homebanking*[18] (Barreira, 2015).

Neste sentido, concordando com Venâncio (2011, p. 15), consta-se que as "práticas e capacidades da informática, e em particular da internet, potenciam a internacionalização da criminalidade", tornando assim, mais difícil a reconstituição do percurso das informações entre o emissor e o recetor, e por conseguinte permitindo a dissimulação de atos e agentes criminosos.

18 Também denominado como banco internético (do inglês *Internet banking*), *e-banking*, banco online ou "banca eletrónica", é um serviço concedido pelas instituições bancárias aos seus clientes, permitindo-lhes executar uma série de operações bancárias, por telefone ou online, relativamente às contas dos quais sejam titulares Ac. STJ de 18/12/2013, Proc. 6479/09.8TBBRG.G1.S1 (Ana Paula Boularot) in http://www.dgsi.pt [22-02-2020].

3. TIPOS LEGAIS DE CRIME ASSOCIADOS AO PHISHING

Relativamente ao enquadramento legal do *phishing*, conforme refere Pedro Verdelho (2009), este não é claro, salientando que a maioria das jurisdições apenas pune várias parcelas desta forma de atuar, não qualificando autonomamente esta atividade complexa enquanto crime. Não obstante, o mesmo autor (2009) acrescenta que numa primeira análise, terá que se ter em linha de conta que subjacente ao *phishing* estará sempre a elaboração e emissão de mensagens de correio eletrónico de conteúdo enganoso, com indicação falsa do remetente (SPAM). Assim, ao considerar-se que uma mensagem de correio eletrónico se trata de um documento enquadrável, tal como defende Pedro Verdelho (2009, p. 414), no artigo 255.º, alínea a) do CP, "esta parcela do *phishing* poderá ser enquadrada sem dificuldades na previsão do crime de falsificação, previsto e punido pelo artigo 256.º, n.º1 do Código Penal".

Por seu turno, no que concerne à criação de uma página *Web* falsa, em tudo idêntica à página institucional de uma organização bancária, já se afigura como uma construção jurídico-penal bastante mais complexa (Verdelho, 2009). Neste sentido, abordar-se-á, em seguida, de uma forma sucinta, se este *modus operandi* do *phishing* poderá, ou não, ser individualmente enquadrado nos seguintes tipos legais de crime: Falsidade informática (Art.º 3 da LC), Acesso ilegítimo (Art. 6º LC) e Burla informática e nas comunicações (art.º 221 CP).

3.1 Falsidade informática (Art. 3º da LC[19])

No que concerne à falsidade informática, verifica-se que, conforme enuncia Pedro Verdelho (2015, p. 257), este é um crime complexo, o qual em termos genéricos "pretende transpor para o ambiente digital a proteção conferida aos mesmos interesses da falsificação do mundo real, prevista no código penal" (arts. 255º ss). Não obstante, conforme elucida José Ascensão (2001, p. 222), verifica-se que se trata de um tipo novo e não apenas um tipo qualificado em relação ao art. 256º CP. Logo o art. 3º/1 exclui a

19 Lei n.º 109/2009 de 15/9, Disponível em: http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1137&tabela=leis [22-02-2019].

aplicação do art. 256º CP. No mesmo sentido, não se pode recorrer ao art. 256º como tipo geral que regeria os aspetos não especificamente regulados pelo atual art. 3º LC.

O bem jurídico que se pretende proteger no crime de falsidade informática, segundo a jurisprudência do AC do TRL, de 9 de janeiro de 2007[20], é a segurança nas relações jurídicas, e, no âmbito da temática tratada, respeitará concretamente à segurança nas transações bancárias. Por conseguinte, trata-se de um crime informático em sentido estrito, porque os atos de falsificação incidem sobre os dados informáticos ou o tratamento de dados por um sistema informático. (Brito, Falsidade Informática (art. 3º LCib), 2017).

Os elementos objetivos do crime de falsidade informática, conforme refere Pedro Verdelho (2010, p. 506), consistem em "introduzir, modificar, apagar ou suprimir dados informáticos ou por qualquer outra forma interferir num tratamento informático de dados, produzindo dados ou documentos não genuínos".

Como referido anteriormente, o primeiro passo levado a cabo pelos grupos criminosos, que se dedicam à captura de elementos bancários dos utilizadores dos serviços de *homebanking*, assenta na criação de páginas Web falsas, correspondente a um *site* na internet e supostamente pertencente a um banco ou entidade emissora de cartões de crédito.

Segundo Paulo Teixeira (2013), os agentes do crime, ao criarem e manterem o *site* idêntico ao do banco, preenchem a conduta prevista no nº 1 do art. 3º da Lei 109/2009, pois "*com intenção de provocarem engano nas relações jurídicas, interferem num tratamento informático de dados, produzindo dados ou documentos não genuínos, com a intenção de que estes sejam considerados ou utilizados para finalidades juridicamente relevantes como se o fossem"*. Por sua vez, o nº 2 agrava a responsabilidade dos agentes quando *"as ações descritas incidirem sobre os dados registados ou incorporados em cartão bancário de pagamento ou em qualquer outro dispositivo que permita o acesso*

20 Cfr. AC TRL 5940/2006-5, [Em linha]. Lisboa (09-01-2007). Disponível em: http://www.dgsi.pt/jstj.nsf [22-02-2020].

a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado", como claramente se constituirá o sistema de *homebanking*, enquanto plataforma de comunicação entre a instituição de crédito e o respetivo cliente.

Por outro lado, importa referir que alguns autores defendem que estes atos são meramente preparatórios de outros tipos legais de crime[21], e por conseguinte não puníveis. Neste caso, destaca-se a posição defendida por Pedro Verdelho (2009, p. 414), ao mencionar que:

> "*mais complexa é a criação de uma página web falsa, correspondente a um site Internet suposta e enganosamente construído como pertencendo legitimamente a um banco ou uma entidade emissora de cartões de crédito. Discute-se o enquadramento de uma página web no conceito de documento constante da alínea a) do artigo 255º do artigo 4º da Lei da Criminalidade Informática (Lei nº 109/91, de 17 de Agosto), que prevê a falsidade informática*".

Não obstante, Paulo Teixeira (2013) defende que o simples facto de o *site* estar criado e existir a possibilidade de um utilizador vir a aceder a este domínio falso, acreditando que está na página do seu banco, preenche os elementos objetivos necessários para que o autor incorra na prática do crime de falsidade informática. Neste sentido, o mesmo autor (2013), acrescenta que os agentes do crime incorrem na prática dos crimes de falsidade informática e burla informática e nas comunicações[22], dado que os respetivos tipos protegem interesses diferentes, não existindo consunção, nem um eventual concurso aparente. Neste sentido, Paulo Teixeira (2013, p. 23), conclui que "é cometido um crime

21 Defendem estes autores a ideia de que as mensagens por si só constituem um mero "furto de identidade" (da pessoa coletiva que é a instituição bancária) e portanto não punível em termos da legislação penal nacional, na medida em que por si só não são adequadas à produção do prejuízo patrimonial. Neste sentido, concordando com Paulo Teixeira (2013, p. 22), discorda-se desta posição, dado que o bem jurídico protegido é "a segurança das relações jurídicas e não o património, bem jurídico que virá a ser de facto afetado, mas numa fase ulterior e não neste momento".

22 Segundo Paulo Teixeira (2013), existe um concurso real heterogéneo entre o crime de falsidade informática e o crime burla informática e nas comunicações, não existindo uma relação de sobreposição ou intersecção entre os dois tipos.

de falsidade informática na forma continuada, nos termos dos art. 30º, nº2 e art. 79º do CP".

3.2 Acesso Ilegítimo (Art. 6º LC)

O conceito de Acesso Ilegítimo, conforme clarifica Pedro Venâncio (2011), respeita principalmente às infrações relativas às ameaças à segurança (confidencialidade, integridade e disponibilidade) dos sistemas informáticos. Por conseguinte, o bem jurídico protegido é a segurança do sistema informático.

No que concerne à conduta típica do acesso ilegítimo, esta assenta no facto de se aceder, por qualquer modo, a um sistema informático, sem a permissão legal ou sem autorização do proprietário, nos termos do n.º 1 do Art.º 6 da LC, bem como no facto de o agente "ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas, um conjunto executável de instruções, um código ou outros dados informáticos destinados a produzir as ações não autorizadas" (nos termos do n.º 2, do Art. 6º da LC). Deste modo, conforme refere a jurisprudência do Ac. do TRG de 17 de novembro de 2008[23], trata-se de "um crime de perigo abstrato e constitui uma barreira para evitar a prática de outros ilícitos de maior gravidade". Com efeito, o crime fica consumado com o acesso não autorizado nos termos da al. a), do nº 4, do Art. 6º, a tomada de conhecimento de um segredo comercial ou industrial, ou de dados confidenciais protegidos por lei, configura circunstância agravante do crime de acesso ilegítimo.

Relativamente ao tipo subjetivo, constata-se que foi eliminada a exigência do elemento subjetivo especial da ilicitude vertida no Art. 7.º da LCI[24], "intenção de alcançar, para si ou para outrem, um benefício ou vantagem ilegítimos", facto que deixa claro que o crime consiste apenas no acesso doloso[25] não autorizado a um sistema

23 Cfr. Acórdão no processo 2233/07 Tribunal da Relação de Guimarães. [Em linha]. Lisboa (17-11-2008). Disponível em: http://www.dgsi.pt/jstj.nsf [22-02-2020].
24 Lei n.º 109/91, de 17/8, disponível em: http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=151&tabela=lei_velhas&nversao=1&so_miolo= [22-02-2020].
25 Em qualquer das modalidades de dolo previstas no Art. 14º do CP, Lei n.º 48/95, de 15/5 disponível em http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=109&tabela=leis [22-02-2020].

informático, independentemente do móbil do agente ou o meio por ele utilizado (Brito, 2017).

Neste contexto, perante o *modus operandi* das ações de *phishing*, verifica-se que os agentes do crime agindo dolosamente, adotam uma conduta suscetível de se enquadrar no previsto nºs 1 e nº 2 do art. 6º da LC, uma vez que, podem aceder ao sistema informático da vítima, sem a sua permissão e sem o seu conhecimento. Além disso, face aos criminosos tomarem conhecimento de dados confidenciais, protegidos por lei, nos termos da al. a), do n.º 4 do art. 6º é agravada a punibilidade do ilícito (Teixeira, 2013).

Face ao exposto, e conforme afirma Pedro Teixeira (2013), encontram-se preenchidos os requisitos dos nºs. 2, e al. a) do nº4 do art. 6º da LC, pelo que, por conseguinte, trata-se de um crime agravado, dispensando a necessidade de queixa-crime para o procedimento criminal[26].

Por fim, quanto ao concurso, embora existam outros autores que possuam posições dissonantes[27], para Pedro Teixeira (2013), existe um concurso efetivo real entre o crime de acesso ilegítimo e o crime de burla informática e nas comunicações. A primeira razão avançada pelo autor (2013), assenta no facto de que o fenómeno de *phishing* não poderá reduzir o efeito ilícito do art.º 6 a um ato de execução da burla informática e nas comunicações além do que os agentes do crime terão acesso a vários dados pessoais da vítima, arquivados no seu computador.

Concomitantemente, Pedro Teixeira (2013, p. 36), ainda enfatiza que: "*com a consunção do art. 6º da LC pelo art. 221º do CP o agente seria apenas punido pela*

26 Neste âmbito importa esclarecer que, conforme menciona Pedro Venâncio (2011), o tipo legal do "Acesso Ilegítimo" se encontrava já contemplado, quer no revogado Art. 7º da LCI, quer no Art. 2º da CCiber., pelo que o procedimento criminal dependerá de queixa, sendo um crime semi-público, exceto nos casos previstos no nsº 2 e 4 do art.º 6 da LC, conforme já mencionado.

27 Neste âmbito, por exemplo Pinto de Albuquerque defende que "há uma relação de concurso aparente (consunção) entre o crime de burla informática e os crimes de falsidade informática, dano relativo a dados ou programas informáticos, sabotagem informática, acesso ilegítimo e a interceção ilegítima, sendo estes factos prévios não puníveis" (Albuquerque, 2010, p. 691)

prática de um ilícito, o que a nosso ver não iria ter em linha de conta a prática pelo mesmo, num momento anterior, de outro tipo de crime autónomo".

3.3 Burla Informática e nas comunicações (art. 221ºCP)

Neste crime o bem jurídico protegido é, conforme elucida Almeida Costa (1999), o património numa aceção jurídico-económica, ou seja, como o conjunto de utilidades económicas detidas pelo sujeito e cujo exercício ou fruição a ordem jurídica não desaprova[28].

De igual modo, conforme refere Almeida Costa (1999), a burla informática constitui um crime de execução vinculada, dado que se restringe à exigência de que a lesão do património se produza através da utilização de meios informáticos, e que não se reconduza ao *modus operandi* da burla do art. 217 CP. Do mesmo modo, Teresa Quintela de Brito (2017) elucida que o crime de burla informática, além de ser um crime de execução vinculada, também poderá ser classificado como um crime de dano/lesão do bem jurídico, por a sua consumação depender da provocação de um prejuízo patrimonial (diminuição do ativo/aumento do passivo), bem como um crime material/de resultado, uma vez que a sua consumação depende de um evento espácio-temporalmente destacado da ação, que consiste na saída dos bens ou valores da esfera de disponibilidade da vítima.

No que diz respeito às ações desenvolvidas pelos agentes do crime para a condução da atividade de *phishing,* estas visam sobretudo a tentativa de captura das credenciais bancárias do serviço de *homebanking* da vítima. Para tal, a vítima irá aceder, sem tomar conhecimento desse facto, a uma página Web falsa, que tenta reproduzir o mais fielmente possível o sítio original do seu banco, induzindo-a a introduzir os seus dados bancários. Com efeito, os criminosos na posse destes elementos irão aceder à conta bancária da vítima, lesando o seu património (Teixeira, 2013).

28 Segundo, Almeida Costa (1999), incluem-se no património os direitos subjetivos patrimoniais (de carácter real ou obrigacional), os lucros cessantes e demais expectativas legítimas de obtenção de vantagens económicas.

Decorrente deste modo *modus operandi*, conforme menciona Rita Santos (2005), infere-se que esta atividade se diferencia da burla clássica, pela ausência do momento intersubjetivo que a caracteriza, ou seja, existe burla informática nos casos em que o prejuízo patrimonial decorre diretamente da operação informática, totalmente automatizada em que a intervenção humana não corresponde a um controlo efetivo e crítico do resultado do tratamento informático de dados. É neste sentido que Almeida Costa (1999, p. 330), concomitantemente afirma que:

> "*a burla informática concretiza-se num atentado directo ao património, i. e., num processo executivo que não contempla, de permeio, a intervenção de outra pessoa e cuja única peculiaridade reside no facto de a ofensa ao bem jurídico se observar através da utilização de meios informáticos*".

Com efeito, tal característica diferencia-o da burla comum, que, como sobressai do art. 217º do CP, pode ser cometida por recurso a qualquer erro ou engano quanto aos factos que o agente astuciosamente provocou[29] (Brito, 2017). Perante estes factos, Pedro Teixeira (2013) refere que o crime de burla informática é um tipo de crime não negligente e necessariamente doloso, em que, a "*intenção*" exigida não é compatível com o dolo eventual (art. 14º do CP). Acresce que, e de acordo com o mesmo autor (2013), outro aspeto, que diferencia a burla informática da burla tradicional, assenta no facto de a consumação do prejuízo patrimonial se verificar como uma consequência adequada da conduta do agente em que não se pode desprezar a intervenção da vítima, sobressaindo desta distinção, a relação de exclusão[30] entre o crime de burla e o crime de burla informática, dados os diferentes modos de execução.

---

29 Concretamente, este facto distingue-a da burla do art. 217 CP, dado que, nesta, a atuação ardilosa do agente tem de produzir um erro ou engano sobre a vítima, que a leva a praticar um ato de diminuição patrimonial (própria ou alheia), existindo, conforme elucida Teresa Quintela de Brito (2017, p. 3), "um duplo nexo de imputação objectiva (do engano da vítima à acção do agente; da diminuição patrimonial à indução em erro da vítima) ".

30 Neste caso concreto, Teresa Quintela de Brito (2017, p. 4), denomina-a por relação de alternatividade ou de exclusividade típica, dado que, conforme a mesma clarifica "as situações enquadráveis, no art. 221º nunca realizam o tipo de burla do art. 217º".

Outro aspeto que importa clarificar prende-se com o facto dos agentes do crime terem de aceder à conta bancária da vítima, sem o seu consentimento, para posteriormente concretizarem o levantamento das verbas disponíveis. Este acesso não autorizado, *a priori*, enquadra-se nos elementos objetivos da prática de um crime de acesso ilegítimo, dado que o agente do crime age, "sem permissão legal ou sem para tal estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, de qualquer modo acede a um sistema informático" (nº1, art. 6 LC). Sendo agravado em virtude de "através do acesso, o agente tiver tomado conhecimento de segredo comercial ou industrial ou de dados confidenciais, protegidos por lei " (al. a), nº4, art. 6 LC). Não obstante, apesar do crime de acesso ilegítimo se constituir como um meio para a realização do crime de burla informática, não constitui o elemento essencial deste crime. Assim, o acesso não autorizado à conta bancária da vítima será consumado pelo crime do qual é o meio de execução (Teixeira, 2013). Por conseguinte, conforme elucida Rita Santos (2005), neste caso em que a prática deste ilícito pressupõe, em regra, o acesso ilegítimo a um sistema ou rede informáticos ou a interceção não autorizada de comunicações eletrónicas, verifica-se que existe uma relação de consunção pura, sendo que, as incriminações previstas no art. 6º LC são absorvidas pela consagrada no art. 221º, nº1 do CP.

4. CONCLUSÕES

Numa primeira análise, verifica-se claramente que em virtude do crescimento exponencial do número de casos de *phishing* registados em Portugal nos últimos anos, e consequentemente, das elevadas quantias monetárias que são subtraídas ilegalmente com esta atividade, existe uma crescente preocupação no seio da nossa sociedade, com os impactos sociais e económicos resultantes da concretização desta técnica fraudulenta.

No que concerne ao *modus operandi* do *phishing*, constatou-se que esta se inicia com o envio da remessa maciça de mensagens de correio eletrónico (spam), que incluem uma ligação para uma página na web falsa. Nesta primeira fase, o pirata informático visa enganar a vítima, fazendo-a acreditar que está a receber um *e-mail* cujo remetente é a sua entidade bancária. Em seguida, a vítima clica na hiperligação referida na mensagem de correio eletrónico, deparando-se com uma página semelhante ao *site* oficial do seu banco, onde lhe será solicitada a identificação através da introdução do nome de utilizador e palavras-passes referentes à sua conta bancária, ou de outras informações confidenciais como o número de conta, número de contribuinte ou outros dados pessoais. Deste modo, os piratas informáticos passam a conhecer os códigos secretos relativos às contas bancárias da vítima, permitindo-lhes o acesso a estas e a realização de transferências de montantes sem conhecimento, nem consentimento do titular da conta (Verdelho, 2009).

Relativamente ao enquadramento legal do *phishing*, notou-se que, conforme menciona Pedro Verdelho (2009), este não é claro, constatando-se que a maioria das jurisdições apenas pune várias parcelas desta forma de atuar, não qualificando autonomamente esta atividade complexa enquanto crime. Não obstante, o mesmo autor (2009) acrescenta que, numa primeira análise, terá que se ter em linha de conta que subjacente ao *phishing* estará sempre a elaboração e emissão de mensagens de correio eletrónico de conteúdo enganoso, com indicação falsa do remetente (SPAM). Assim, ao considerar-se que uma mensagem de correio eletrónico se trata de um documento enquadrável, tal como defende Pedro Verdelho (2009, p. 414), no artigo 255.º, alínea a)

do CP, "esta parcela do *phishing* poderá ser enquadrada sem dificuldades na previsão do crime de falsificação, previsto e punido pelo artigo 256.º, n.º1 do Código Penal".

Por sua vez, no que concerne à criação de uma página *Web* falsa, em tudo idêntica à página institucional da instituição bancária, já se afigura como uma construção jurídico-penal bastante mais complexa (Verdelho, 2009). Perante este facto, analisou-se de uma forma sucinta, este *modus operandi* do *phishing* ao abrigo dos seguintes tipos legais de crime: Falsidade informática (Art.º 3 da LC), Acesso ilegítimo (Art. 6º LC) e Burla informática e nas comunicações (art.º 221 CP).

Decorrente desta análise, verifica-se que a dificuldade de abordagem do fenómeno de *phishing* se encontra, por um lado, refletido na escassez de jurisprudência nesta área no ordenamento jurídico português, e por outro, da necessidade da existência de um conhecimento profundo que engloba, tanto questões de natureza técnica, como de natureza jurídica.

Com efeito, a cibercriminalidade, como é corroborado como Pedro Teixeira (2013, p. 114), é efetivamente um dos

"fenómenos que, provavelmente, veio lançar um dos maiores desafios nas estruturas judiciais e de investigação criminal, desde logo pela relativa impunidade com que cada vez mais é praticada, fruto de uma maior sofisticação das técnicas e tecnologias empregues, bem como pela sua celeridade, assim como pelo seu caráter transnacional e a sua volatilidade".

Neste sentido, para os Estados poderem fazer face aos novos desafios que a cibercriminalidade acarreta, é fundamental desenvolver e fomentar medidas eficazes de prevenção. Estas podem traduzir-se através da implementação de políticas de sensibilização e aumento da cibereducação da sociedade, e pelo desenvolvimento e incremento da formação especializada dos profissionais que trabalhem nesta área, aliada à disponibilização de mais e melhores meios, tanto humanos como materiais.

BIBLIOGRAFIA

Albuquerque, P. P. (2010). *Comentário do Código Penal à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem* (2ª ed. ed.). Lisboa: Universidade Católica Portuguesa.

Amador, N. (2012). *Cibercrime em Portugal: Trajetórias e Perspetivas de Futuro.* Lisboa: Instituto Superior de Ciênciais Policiais e Segurança Interna.

APDSI. (6 de 2019). *Glossário da Sociedade da Informação.* Fonte: APDSI: http://www.apdsi.pt/index.php/portugues/menu-secundario/glossario.html

Ascensão, J. O. (2001). Criminalidade informática. *Direito da Sociedade de Informação, II*, 203-228.

AVAST. (22 de 2 de 2019). *Academia de Ameaças Online*. Fonte: AVAST: https://www.avast.com/pt-br/c-online-threats

Azevedo, A. (2016). *Burlas Informáticas: Modos de Manifestação.* Braga: Universidade do Minho.

Barreira, M. (2015). *HOME BANKING - A REPARTIÇÃO DOS PREJUÍZOS DECORRENTES DE FRAUDE INFORMÁTICA.* Lisboa: Faculdade de Direito da Universidade Nova de Lisboa.

Belfiore, M. (2010). *The Department of Mad Scientists.* Nova Iorque: Harper Perennial.

Brito, T. Q. (2017). Acesso Ilegítmo. *Cibercrime* (pp. 1-6). Lisboa: FDUL.

Brito, T. Q. (2017). Burla informática e nas telecomunicações. *Cibercime - 2016/2017* (pp. 1-9). Lisboa: FDUL.

Brito, T. Q. (2017). Falsidade Informática (art. 3º LCib). *Cibercrime 2016-2017* (pp. 1-12). Lisboa: FDUL.

CNCS. (23 de 2 de 2020). *Glossário*. Fonte: Centro Nacional de Cibersegurança Portugal: https://www.cncs.gov.pt/recursos/glossario/

Costa, A. (1999). *Comentário Conimbricence do CP, Tomo II.* Coimbra: Coimbra Editora.

GNR. (23 de 2 de 2020). *Phishing*. Acesso em 23 de 2 de 2020, disponível em GNR: https://www.gnr.pt/cyberFraudesNet.aspx

Guimarães, M. (2013). A fraude no comércio electrónico: o problema da repartição do risco por pagamentos fraudulentos. In Infracções Económicas e Financeiras. Em *Estudos de Criminologia e de Direito* (pp. 581 - 597). Coimbra : Coimbra Editora.

Luís, F. (2011). Proteger o dinheiro – Home banking, Conselhos aos utilizadores. *Inforbanca*(88), 10-11.

Marques, L. M. (2006). *Direito da Informática* (2ª ed. ed.). Coimbra: Almedina.

Matos, J. (2009). *Dicionário de Informática e Novas tecnologias.* Lisboa: FCA - Editora de Informática, (Ed.), Lidel.

Santos, R. C. (2005). *Tratamento Jurídico-Penal da Transferência de Fundos Monetários Através da Manipulação Ilícita dos Sistemas Informáticos.* Coimbra: Coimbra Editora.

Teixeira, P. G. (2013). *O fenómeno do Phishing - Enquadramento jurídico-penal.* Lisboa: Universidade Autónoma de Lisboa.

Venâncio, P. (2011). *Lei do Cibercrime - Anotada e Comentada* (1.ª Edição ed.). Lisboa: Coimbra Editora.

Verdelho, P. (2009). Phishing e outras formas de defraudação nas redes de comunicação. Em *Direito da Sociedade da Informação (Oliveira Ascensão, coordenação).* (Vol. III, pp. 407-419). Coimbra: Coimbra Editora.

Verdelho, P. (2010). *Anotação à Lei n.º 109/2009, de 15 de setembro.* Lisboa : Universidade Católica Editora.

Verdelho, P. (2015). Em C. J. Santos, *Enciclopédia de Direito e Segurança* (pp. 255-263). Lisboa: Almedina.