Revista da Faculdade de DIREITO da Universidade Federal de Uberlândia

Entre o ciberespaço e o Direito: A in(existência) legal do crime de *Phishing* em Angola

Between cyberspace and the law: The legal (non)recognition of Phishing as a crime in Angola

António Maria Dala do Nascimento[1]

Resumo: O artigo em tela tem como objeto de estudo o enquadramento jurídico-penal do *Phishing* no ordenamento criminal angolano, analisando as formas pelas quais essa prática pode ser sancionada, mesmo na ausência de uma tipificação penal autónoma. A pesquisa busca responder à questão: de que forma o ordenamento jurídico-penal angolano pode enquadrar e sancionar as condutas típicas do *Phishing*, mesmo na ausência de uma tipificação penal específica?. O principal objetivo consiste em identificar os tipos legais existentes que abrangem comportamentos associados a esse fenómeno e propor um modelo penal específico para o seu tratamento. Este estudo adoptou uma metodologia qualitativa, de natureza exploratória e descritiva, baseada na análise bibliográfica. Os resultados indicam que o *Phishing* pode ser enquadrado em crimes como falsidade informática, burla nas comunicações, acesso ilegítimo e dano em dados informáticos, previstos no Código Penal Angolano. Concluiu-se que, embora existam mecanismos normativos suficientes para punir tais condutas, é necessária a criação de um tipo penal autónomo de *Phishing*, definido como a prática fraudulenta de obtenção de dados pessoais, bancários ou sensíveis mediante manipulação digital e engenharia social.
Palavras-Chave: *Phishing*. Código Penal Angolano. Crimes Informáticos. Enquadramento Jurídico-Penal. Política Criminal.

Abstract: This article examines the criminal-legal framework of *Phishing* within Angolan criminal law, exploring how such conduct can be punished even without an autonomous legal definition. The study seeks to answer how Angolan criminal law can classify and sanction typical *Phishing* behaviors in the absence of a specific provision. Its main goal is to identify existing legal norms that already encompass this phenomenon and to propose a specific criminal model for its regulation. A qualitative, exploratory, and descriptive methodology was adopted, grounded in bibliographic analysis. Findings reveal that *Phishing* may be subsumed

[1] Professor Mestre em Criminologia e Investigação Criminal do Instituto Superior Politécnico de Ciências e Tecnologias (INSUTEC) e do Instituto Superior de Ciências Policiais e Criminais "Genereal – Osvaldo de Jesus Serra Van-Dúnem" (ISCPC). E-mail: liriomiguel.lm@gmail.com. Orcid: https://orcid.org/0009-0001-6458-9526. CV Lattes: http://lattes.cnpq.br/3656286357534267.

DOI: http://dx.doi.org/10.14393/RFADIR-52.1.2024.80545.3-28

under offenses such as computer forgery, communication fraud, unlawful access, and data damage, all covered by the Angolan Penal Code. Although current legislation offers sufficient mechanisms to punish these acts, the research highlights the need for an autonomous criminal provision on *Phishing*, defined as the fraudulent acquisition of personal, financial, or sensitive data through digital manipulation and social engineering.
Keywords: *Phishing*. Angolan Penal Code. Cybercrimes. Criminal-Legal Framework. Criminal Policy.

1. Introdução

A expansão da *Internet* em Angola nas últimas décadas tornou-se um fenómeno expressivo que desempenha um papel substancial no desenvolvimento do país. Este avanço tecnológico actua como um verdadeiro catalisador para a transformação e modernização de vários sectores, impactando positivamente a sociedade angolana no âmbito social, económico e jurídico, permitindo o compartilhamento rápido de conhecimento, a comunicação eficiente, o acesso a recursos educacionais e oportunidades de emprego.

Contudo, esta massiva conectividade também introduz novos desafios, expondo os indivíduos a práticas criminosas no ambiente digital, entre as quais se destacam os ataques de *Phishing*, uma modalidade de engenharia social[2] que visa enganar as vítimas a comprometerem a sua segurança pessoal e a fornecer informações sensíveis. Assim, como no espaço físico, também no ciberespaço, as interações humanas são orientadas por interesses individuais, frequentemente resultando em conflitos e comportamentos ilícitos.

Dados do Serviço de Investigação Criminal angolano (SIC) revelam que, anualmente, os crimes informáticos em Angola causam prejuízos estimados em cerca de 600 milhões de kwanzas. Apenas em 2022, foram formalizadas 1.209 denúncias relacionadas a cibercrimes, o que representa

[2] A Engenharia Social refere-se a práticas de persuasão e engano utilizadas por indivíduos mal-intencionados para manipular outras pessoas a comprometerem a sua segurança pessoal, com a finalidade de obterem informações pessoais.

um aumento de 6% em comparação com o ano anterior. De acordo com Dembinsky (apud SEBASTIÃO, 2022), gestor de dados da *Check Point Software*[3], as tentativas de ataques por *Phishing e Ransomware*[4] em Angola tiveram um aumento de 58% entre 2020 e 2021, tendo como alvos principais, as aplicações bancárias em telemóveis. Em fevereiro de 2021, por exemplo, os sistemas do Ministério das Finanças em Angola foram comprometidos por um ataque informático, durante o qual, contas de *e-mail* e pastas compartilhadas foram invadidas por sujeitos desconhecidos.

No campo jurídico-penal angolano, verifica-se que o *Phishing*, enquanto técnica de ataque informático, não constitui, de forma autónoma, um tipo penal (crime) específico previsto na legislação vigente. Ainda assim, mesmo sem previsão expressa, o *Phishing* pode, em determinadas circunstâncias, ser enquadrado em tipos penais já existentes, ou seja, este ataque cibernético pode servir como meio executivo para a consumação de outros crimes previstos na legislação. Essa constatação conduz ao seguinte *problema* central deste artigo: de que forma o ordenamento jurídico-penal angolano pode enquadrar e sancionar as condutas típicas do *Phishing*, mesmo na ausência de uma tipificação penal específica?

Dessa forma o artigo tem como objetivo geral**:** analisar o enquadramento jurídico-penal do *Phishing* à luz da legislação criminal angolana. Especificamente, procura-se: (i) identificar os tipos legais que podem abranger condutas associadas ao *Phishing*; (ii) interpretar os elementos objetivos e subjetivos desses crimes à luz das práticas comuns de ataque *Phishing*; (iii) contribuir para o debate jurídico-criminológico sobre a necessidade de uma tipificação autónoma do crime de *Phishing* em Angola.

[3] A *Check Point Software* é uma empresa internacional especializada em segurança cibernética. Fundada em 1993. É conhecida por fornecer soluções de segurança para proteger redes e dispositivos móveis contra ameaças cibernéticas

[4] Sequestro de dados com pedido de resgate.

Do ponto de vista metodológico, a investigação assenta em uma abordagem qualitativa, de natureza exploratória e descritiva, fundamentada em pesquisa bibliográfica. O método científico utilizado é o indutivo, partindo da análise de práticas e características típicas do crime de *Phishing* para inferir o seu possível enquadramento legal à luz do ordenamento jurídico-penal angolano.

A prática de *Phishing* pode ser instrumentalizada para o preenchimento dos elementos objetivos e subjetivo s de diversos crimes tipificados na legislação penal angolana, dependendo das circunstâncias concretas do caso e da intenção do agente. Esta interpretação permite que o ordenamento jurídico-penal de Angola, ainda que de forma indirecta, alcance e sancione as condutas fraudulentas praticadas por meio de ataques *Phishing*, reforçando assim, a eficácia legal na proteção dos bens jurídicos e na adaptação às novas formas de criminalidade cibernética.

2. *Phishing*

2.1. Conceito de *Phishing*

Na contemporaneidade, os criminosos adotam novas metodologias para expandir a execução de delitos antes perpetrados sem a utilização das tecnologias de informação e comunicação. Os crimes cibernéticos, assim, emergem como uma preocupação inegável, englobando uma diversidade de ações que têm sido objeto de tentativas de categorização e, consequentemente, de tipificação no âmbito da legislação jurídico-penal. Nesse contexto, destaca-se a necessidade de focar no principal objeto deste artigo: o *Phishing*. Este procedimento tem-se destacado como uma das principais formas de ataques perpetrados na *Internet*. Originado em ataques de engenharia social, etimologicamente, o termo *Phishing* deriva da palavra em inglês *fishing*,

proveniente da prática da pesca, em que pescadores (o *phisher*[5], utiliza mensagens de engenharia social para obter informações da vítima) utilizam iscas para atrair peixes. Portanto, o termo resulta de uma analogia com a pesca, em que há a necessidade de o usuário na *Internet* morder a isca, e para esse acto, há uma ilusão de que a mesma é autêntica (ALABDAN, 2020).

Khonji *et al.* (2013) elucidam que a modificação do *f* para *ph* na palavra *fishing* ocorreu devido ao primeiro tipo de ataque de *Phishing* ter sido realizado por telemóvel. Em 2006, a sua definição foi incorporada no *Oxford English Dictionary* como a ação fraudulenta de encaminhar e-mails falsos, simulando serem provenientes de empresas confiáveis, com o propósito de persuadir pessoas a fornecer informações pessoais, como senhas e números de cartões de crédito, pela Internet[6].

Nesta mesma linha de ideias, Pinheiro (2020, p. 16), em sua obra Segurança Digital: Proteção de Dados, oferece uma abordagem conceptual esclarecedora acerca do conceito de *Phishing*, destacando que:

> o Phishing pode ser entendido como pescaria ou golpe de pescaria, apresentando-se como uma encenação por meio da qual o utilizador é atraído ou enganado para que, cogitando ser um conteúdo autêntico, aceda um link falso, uma página web ou abra algum arquivo para haver furto de dados ou o respetivo acesso dos mesmos. É um tipo de engenharia social.

De outro modo, na visão de Milletary e Center (2005), o *Phishing* é concebido como uma estratégia astuciosa que emprega meios digitais, como mensagens, imitando o estilo de comunicação de agentes, entidades, empresas e *websites* de confiança, objetivando a obtenção de informações pessoais da vítima. É, portanto, uma forma de engenharia social que busca induzir as vítimas a tomar medidas urgentes, muitas vezes sob a falsa necessidade de validar a conta pessoal ou permitir o acesso do *phisher*.

---

[5] *Phisher* é o termo técnico utilizado para descrever uma pessoa ou entidade envolvida na prática dos ataques de *Phishing*.

[6] Traduzido pelo autor, do inglês original: *the fraudulent pratice of sending e-mails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers, online*.

Apesar disso, embora se observe uma convergência entre os autores ao considerarem o *Phishing* como uma forma de engenharia social, pode-se constatar, a existência de divergências nas ênfases dadas à encenação ilusória, à imitação de entidades confiáveis e à sofisticação técnica. A metáfora da pesca utilizada por Pinheiro (2020) ilustra claramente o carácter atractivo e enganoso do *Phishing*. Enquanto, Milletary e Center (2005) ressaltam a astúcia na imitação, evidenciando a sofisticação técnica do ataque. Essas perspectivas enriquecem a compreensão do *Phishing*, abrangindo desde a sua origem como uma ameaça direccionada a usuários comuns até a sua evolução para ataques mais sofisticados com o intuito de obter informações estratégicas em níveis mais elevados da sociedade e da esfera corporativa.

Observa-se então que, nos últimos anos, a esfera académica tem-se envolvido em debates acerca da evolução conceptual dos ataques de *Phishing*. Se inicialmente essa categoria de abordagem era caracterizada como uma maneira fraudulenta de conduzir usuários da *Internet*, por meio de páginas da *web*, a fornecer informações pessoais, Hong (2012) introduz uma perspectiva mais abrangente ao afirmar que os ataques de *Phishing*, numa primeira fase, têm como alvos usuários comuns da *Internet*, visando o roubo de identidade e informações de cartões. Em todo caso, posteriormente, expandiram-se para abrangir também alvos de elevado *status social*, com o intuito de obter propriedade intelectual, segredos empresariais e informações confidenciais relacionadas à segurança nacional de um determinado Estado.

Por último, Lastdrager (2014), alinhado com a doutrina científica, argumenta que o conceito de *Phishing* deve incorporar outros elementos essências, como informação, alvo, escalabilidade e engano. Em decorrência disto, ele conceitua o *Phishing* como a "ação escalonável de engano em que a representação é utilizada para colher informações de um alvo" (LASTDRAGER, 2014, p. 8). Na perspectiva desse autor, trata-se de um conceito abstracto que amplia o escopo das práticas, possibilitando a

identificação de diversos crimes cibernéticos que podem ser preenchidos por meio desses ataques, conforme se poderá verificar nas secções seguintes.

3. *Phishing* à luz do Direito penal angolano: Entre a ausência de tipificação autónoma e o enquadramento em tipos legais existentes

3.1. Falsidade informática (artigo 442º do código penal angolano)[7]

Uma das técnicas de iniciação para o ataque *Phishing* consiste na criação ou falsificação de páginas *Web*, ou *websites* que replicam, de forma quase idêntica, a aparência e as funcionalidades de instituições específicas. Esta técnica tem o propósito de induzir a vítima potencial, associada a uma determinada instituição, a acessar a página falsa, sob a falsa suposição de que se trata do *website* legítimo da instituição.

O crime de Falsidade Informática reveste-se de natureza pública, o que significa que não é necessária a apresentação de uma queixa-crime para o início do procedimento criminal, sendo suficiente a simples comunicação dos fatos. O bem jurídico protegido por este crime é a segurança e a fiabilidade de documentos, bem como a proteção contra enganos nas relações jurídicas no ambiente informático.

---

[7] Código Penal Angolano, artigo 442º - Falsidade Informática:
1. Quem, com intenção de enganar ou prejudicar, introduzir, alterar, eliminar ou suprimir dados em sistema de informação ou, em geral, interferir no tratamento desses dados, por forma a dar origem a dados falsos que possam ser considerados verdadeiros e utilizados como meio de prova, é punido com pena de prisão até 2 anos ou com a de multa até 240 dias.
2. Quando as ações descritas no número anterior incidirem sobre os dados registados ou incorporados em cartão bancário de pagamento ou qualquer outro dispositivo que permita o acesso a sistema ou meio de pagamento, a sistema de comunicações eletrónicos ou a serviço de acesso condicionado, a pena é de 2 a 5 anos de prisão.
3. As penas estabelecidas nos n.ºs 1 e 2 são aplicáveis a quem, não sendo o autor dos crimes descritos nesses números, utilizar, com a intenção de causar prejuízo a outrem ou de obter beneficio para si ou para terceiro, respetivamente, os dados falsos referidos no n.º1 ou o cartão ou dispositivo em que se encontrarem registados ou incorporados os dados obtidos com fatos descritos no n.º2.
4. Se o autor dos fatos descritos nos números anteriores for funcionário público no exercício das suas funções, a sua pena é de, 6 meses a 3 anos ou multa de 60 a 360 dias, no caso do n.º1; e 4 a 10 anos, no caso dos n.ºs 2 e 3.

Segundo a professora Moniz (2004, p. 269), "sempre que um documento falsificado seja inserido no tráfego informático, configura-se um caso de falsidade informática." Ademais, a autora sustenta que, conforme o disposto no n.º 1 do crime de Falsidade Informática, é imprescindível que "os dados ou programas possam ser_utilizados como meio de_prova, de modo que a sua visualização produza os mesmos efeitos que um documento falsificado" (MONIZ, 2004, p. 270).

Em essência, o resultado obtido é análogo ao da Falsificação de Documento[8], sendo que a Falsidade Informática constitui uma extensão do tipo clássico de falsificação, adaptada às especificidades do ambiente informático. Consoante as concepções doutrinárias do célebre professor da Faculdade de Direito da Universidade Agostinho Neto de Angola, Rodrigues (2016), sobre esta temática, explica que a falsificação de documentos consiste, em primeiro lugar, na elaboração de um documento inteiramente falso, mas também inclui a alteração de um documento verdadeiro, a utilização abusiva da assinatura de outra pessoa disposta no respetivo suporte documental para elaborar documento falso e, ainda, a falsidade intelectual.

Fazendo a apreciação sob a perspectiva informática, pode-se afirmar que não se protege um novo bem jurídico, nem um bem jurídico especificamente ligado ao ambiente informático. O objetivo do legislador foi salvaguardar a segurança e a fiabilidade dos documentos, bem como a proteção contra enganos nas relações jurídicas, ou a veracidade na reconstituição das relações jurídicas, de forma exatamente idêntica aos interesses protegidos pelo direito penal clássico (falsificação de documento),

[8] Código Penal Angolano, artigo 251º - Falsificação de documento:
1. É punido com pena de prisão até 2 anos ou com multa até 240 dias quem, com o propósito de causar prejuízo a alguém ou de obter, para si ou para outrem, um benefício:
a) Elaborar documento falso, imitando verdadeiro;
b) Falsificar ou alterar documento verdadeiro;
c) Utilizar abusivamente a assinatura de outra pessoa para elaborar documento falso;
d) Fizer constar falsamente num documento, fatos juridicamente relevantes ou nele omitir fatos juridicamente relevantes que no documento deviam constar.

porém, no caso em concreto, por via da incriminação de condutas que envolvam a falsificação de programas ou dados informáticos. Deste modo, tal como descrevem Castanheira e Andrade (2009), a única especificidade deste tipo de crime reside no *modus operandi*, que se destaca pela execução via meios informáticos. Os elementos objetivos do crime de Falsidade Informática decorrem de circunstâncias como introduzir, alterar, eliminar ou suprimir dados em sistemas de informação ou, em geral, interferir no tratamento desses dados, por forma a dar origem a dados falsos (não genuínos), enquanto o elemento subjetivo é caracterizado pela intenção de enganar ou prejudicar para que possam ser considerados verdadeiros.

Pode-se concluir então que os perpetradores do crime, ao criarem e manterem um *site* idêntico ao legítimo, preenchem a conduta descrita no n.º 1 do artigo 442º. Isso ocorre porque, com intenção de enganar ou prejudicar, eles interferem no tratamento desses dados, por forma a dar origem a dados falsos. O n.º 2 do artigo 442º agrava a responsabilidade dos agentes quando as ações descritas no nº. 1 incidirem sobre *os* dados registados ou incorporados em cartão bancário de pagamento ou qualquer outro dispositivo que permita o acesso a sistema ou meio de pagamento, a sistema de comunicações eletrónicas ou a serviço de acesso condicionado. Esse agravamento aplica-se claramente a muitas das aplicações bancárias móveis, que atuam como plataformas de comunicação entre a instituição e o cliente.

Consequentemente, é inegável que a criação de uma página falsa para a execução de um ataque de *Phishing* reflete a intenção do agente criminoso de, posteriormente, utilizar os dados obtidos, mediante o erro ou engano induzido ao utilizador, para acessar sua conta e causar-lhe prejuízo. Assim, conforme a descrição do n.º 2, o simples acto de criar o referido *site*, aliado à intenção dos agentes de provocarem engano ou prejudicar nas relações juridicas relativas a sistema ou meio de pagamento, a sistema de comunicações eletrónicas ou a serviço de acesso condicionado, fazendo o utilizador acreditar que está no domínio legítimo da sua instituição, constitui

uma conduta capaz de preencher integralmente os elementos objetivos previstos no tipo penal de Falsidade Informática, conforme estabelecido no artigo 442º do Código Penal Angolano.

3.2. Furto de identidade (o caso do uso de *e-mails*)

A crescente utilização da *Internet*, impulsionada por um número gradativo de utilizadores de origens diversas, tem expandido significativamente a quantidade de informação disponível *online*, tornando-a acessível a qualquer pessoa. Diante desse aspecto, e considerando a relevância dos dados pessoais, é inevitável que a exploração indevida dessa informação se torne atractiva para indivíduos com menos escrúpulos, resultando num aumento substancial dos furtos de identidade na *Internet*. Assim, a utilização de referências, nomes e denominações falsos por agentes criminosos constitui um dos métodos empregados para induzir as vítimas a acreditar na legitimidade das solicitações recebidas, criando a falsa percepção de que interagem com uma pessoa ou entidade de boa-fé, com o intuito de fomentar a convicção de que a solicitação apresentada é legítima.

Estudos apresentados em 2009, durante o Congresso Internacional *World Wide Web*, realizado em Madrid, a 18 de Abril, demonstraram a relativa facilidade com que se podem conduzir ataques nas redes sociais *Facebook* e *LinkedIn*. Esses estudos indicaram que as redes sociais assumem uma importância crescente tanto nos contactos locais quanto globais, suscitando discussões sobre a legitimidade da prática de empregadores consultarem o perfil de candidatos para obter informações adicionais sobre a sua personalidade. Ainda segundo esta mesma pesquisa, conduzida por Balzarotti *et al.* (2009), evidenciou-se ser extremamente simples lançar ataques automatizados de furto de identidade contra as principais redes sociais, permitindo o acesso a um vasto volume de informações pessoais.

Para compreender com precisão o conceito de identidade, é necessário recorrer ao ordenamento jurídico angolano, especificamente à Lei Fundamental. A Constituição Da República De Angola consagra, no artigo 32.º, o direito à identidade, à privacidade e à intimidade. No contexto do presente estudo, a ênfase recai sobre o direito à identidade, que a Constituição Da República De Angola assegura como o conjunto de elementos que identifica cada pessoa como individuo, singular, abrangendo também o direito ao bom nome e reputação, à imagem, à palavra e à reserva da intimidade da vida privada e familiar. No Código Civil Angolano, no Título II (Das Relações Jurídicas), Subtítulo I (Das Pessoas), Capítulo I (Pessoas Singulares), Secção I (Personalidade e Capacidade Jurídica), o artigo 72.º, n.º 1, sob a epígrafe Direito ao Nome, estabelece que toda a pessoa tem direito a usar o seu nome completo ou abreviado,e a opor-se a que outrem o use ilicitamente para sua identificação ou outros fins. O nome, portanto, é reconhecido como um direito da personalidade, sendo este conceito intrinsecamente relacionado aos indivíduos enquanto pessoas físicas. No âmbito da proteção da privacidade do indivíduo, o ordenamento jurídico angolano prevê também a existência de um diploma legal que consagra a proteção dos dados pessoais. Trata-se da Lei n.º 22/11, de 17 de Junho (Lei da Proteção de Dados Pessoais), que na alínea b) do artigo 5.º, sob a epígrafe Definições, conceitua dados pessoais como qualquer informação, seja qual for a sua natureza ou suporte, incluindo imagem e som, relativa a uma pessoa singular identificada ou identificável (titular dos dados), acrescentando ainda que é considerada identificável a pessoa que possa ser identificada directa ou indirectamente, designadamente por referência a um numero de identificação ou à combinação de elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social.

Daqui se concluirá, que a identidade constitui uma referência singular a um indivíduo considerado fisicamente. De toda a maneira, o fato de essa questão estar relacionada ao cidadão enquanto pessoa física e individual

suscita um desafio significativo quando transposta para o mundo digital. Como exemplo, considere-se o caso de um endereço de *e-mail* em nome de alguém que possa ser associado ou identificado como um indivíduo específico e reconhecido na comunidade ou no meio social. Surge então a dúvida se um *e-mail* dessa natureza se enquadra ou não na categoria de dado pessoal legalmente protegido. Este tipo de referência é frequentemente utilizada em endereços de *e-mail* criados intencionalmente por autores de ataques de *Phishing*, visando atrair as vítimas a abrir *e-mails* e acessar determinados domínios.

Neste âmbito, a questão em análise consiste em determinar se a utilização de endereços de *e-mail* falsos constitui, por si só, um elemento suficiente para ser qualificado como um ilícito de natureza criminal. No entendimento do pesquisador deste estudo, observa-se uma lacuna legislativa evidente nesse domínio, uma vez que a lei angolana não prevê, nem sanciona, a criação e utilização de um endereço de *e-mail* que se faça passar por outrem.

Concretamente, não existe uma norma específica que caracterize ou inclua a criação de um *e-mail* falso como uma conduta criminosa. Em outras palavras, qualquer pessoa pode, se assim o desejar, utilizar o seu nome ou qualquer outro para criar uma conta em diversos serviços de *e-mail*, sem que isso implique, de imediato, uma infração penal. De toda a forma, este acto encontra um limite, particularmente no que diz respeito à forma como o utilizador pode empregar a identidade associada ao *e-mail*. O artigo 274.º do Código Penal Angolano, sob a epígrafe Assunção ou Atribuição de Falsa Identidade[9], estabelece que aquele que assumir a identidade de terceira pessoa e acrescenta com o propósito de obter beneficio, para si ou para outrem, ou de causar prejuízo, será responsabilizado criminalmente. Logo, sempre que

[9] Código Penal Angolano, artigo 274º - Assunção ou Atribuição de Falsa Identidade:
Aquele que assumir a identidade de terceira pessoa ou atribuir a terceira pessoa falsa identidade com o propósito de obter benefício, para si ou para outrem, ou de causar prejuízo a alguém é punido com pena de prisão até 2 anos ou co a de multa até 240 dias.

um indivíduo utilizar uma conta de *e-mail* para se fazer passar por outra pessoa física, para obter vantagens ou causar prejuízos a terceiros, tal conduta será considerada crime, configurando-se, em geral, como um acto de assunção de falsa identidade. Este enquadramento legal assegura que, apesar da ausência de regulamentação específica sobre a criação de *e-mails* falsos, o uso fraudulento desses meios para furtar a identidade de outrem e prejudicar terceiros, como no caso dos ataques de *Phishing*, são passíveis de sanção penal, reforçando a proteção da identidade no âmbito digital.

3.3. Acesso ilegítimo a sistema de informação e devassa de sistema de informação (artigo 438º do código penal angolano)[10]

Após o envio em massa de *e-mails*, a vítima, ao abrir a mensagem destinada a si, acaba por comprometer o seu dispositivo ou computador, resultando em uma possível infecção.

[10] Código Penal Angolano, *artigo* 438º - Acesso ilegítimo a sistema de informação e devassa de sistema de informação:
1. Quem, sem autorização, aceder à totalidade ou à parte de um sistema de informação, de que não for titular, é punido com pena de prisão até 2 anos ou com a de multa até 240 dias.
2. Se o acesso for conseguido através da violação das regras de segurança ou se tiver sido efetuado a um serviço protegido, a pena é de 2 a 8 anos de prisão.
3. A mesma pena é aplicável sempre que, no caso descrito no n.º1, o agente:
a) Tomar conhecimento de segredo comercial ou industrial ou de dados confidenciais protegidos por lei;
b) Obtiver beneficio ou vantagem patrimonial de valor elevado, conforme este é definido na alínea b) do artigo 391.º
4. É punido com pena do n. 1º quem, sem estar devidamente autorizado:
a) Proceder ao tratamento informático de dados ou informações individualmente identificáveis;
b) Transmitir a terceiros, para fins diferentes dos autorizados, dados ou informações informaticamente tratados;
c) Criar, manter ou utilizar ficheiro informático de dados pessoalmente identificáveis relativos a convicções políticas, religiosas ou filosóficas, a filiação partidária ou sindical ou à vida provada de outrem.
5. A tentativa é sempre punível.
6. Para efeitos do n. 2º, serviço protegido significa qualquer serviço de radiodifusão ou da sociedade da informação, desde que prestado mediante remuneração e com acesso condicionado, conforme este é descrito na alínea c) do artigo 250 º.

O termo acesso ilegítimo refere-se, primordialmente, à infração que ameaça a segurança dos sistemas informáticos, abrangendo aspectos como a confidencialidade, integridade e disponibilidade (VENÂNCIO, 2011).

De acordo com Rodrigues (2011, p. 163 – 164), este tipo legal visa proteger a "esfera formal da privacidade e do segredo ou a integridade do sistema informático lesado", fundamentando-se numa nova concepção de inviolabilidade do domicílio informático, seja em termos restritos, seja numa perspectiva mais ampla, pretendendo a tutela do uso legítimo dos meios informáticos pelos seus titulares. Ainda segundo o autor, o Acesso Ilegítimo configura "um crime informático-digital próprio (ou puro), que acarreta riscos para os fluxos informacionais, comunicacionais e informático-digitais" (RODRIGUES, 2011, p. 171).

Conforme mencionado por Martins e Marques (2006), o Conselho da Europa considera este crime como uma das infrações informáticas mais emblemáticas, comummente conhecida como espionagem informática ou furto de informação. A intenção do legislador é salvaguardar ou proteger o bem jurídico denominado domicílio informático, comparável à introdução em casa alheia (no sentido de invasão de domicílio físico).

Os elementos objetivos que caracterizam o crime de Acesso Ilegítimo assentam na "ausência de permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou parte dele, e de qualquer modo aceder a um sistema informático", bem como o fato de o agente ilegalmente transmitir dados informáticos destinados a produzir ações não autorizadas (VENÂNCIO, 2011, p. 60). Nos termos do n.º 2, o elemento objetivo também se fundamenta na violação de regras de segurança, o que acarreta um agravamento da pena, situando-se entre 2 a 8 anos de prisão. Já o n.º 3 estabelece que a mesma pena será aplicável se, através do acesso, o agente tiver tomado conhecimento de segredo comercial ou industrial ou de dados confidenciais, protegidos por lei, ou de se o benefício ou a vantagem

patrimonial obtidos forem de valor elevado. O acesso ilegítimo possui como elemento subjetivo a mera intenção do agente em aceder ilegitimamente a um sistema, desrespeitando os direitos de quem detém a sua titularidade.

No caso do ataque de *Phishing*, os perpetradores, agindo dolosamente, adoptam uma conduta suceptivel de se enquadrar nos nos n.ºs 1 e 2 do artigo 438.º, uma vez que passam a conseguir acessar o sistema informático da vítima sem o seu conhecimento e à sua revelia, com o propósito bem definido de capturar elementos de segurança, informações ou dados pessoais da vítima. Outro aspecto relevante a destacar é que, no caso de ataques de *Phishing* que envolvem a utilização de um *Trojan*[11], a vítima pode ser redireccionada para um *website* alternativo, visualmente idêntico ao da instituição desejada, onde, por meio de erro ou engano, as suas credenciais bancárias são capturadas, podendo o próprio programa utilizado no ataque, ter a capacidade de recolher esses dados automaticamente (*keylogger*[12]), fatos estes que permitem ao vitimário obter acesso a dados confidenciais protegidos por lei, o que pode levar à sua punição conforme a alínea a) do n.º 3 do artigo 438.º. Por último, diante do exposto, verifica-se que, nos termos dos n.ºs 1 e 2 e a alínea a) do n.º 3 do referido artigo 438.º, os fatos ilícitos descritos possuem natureza pública, não sendo necessária a apresentação de queixa por parte da vítima para a instauração do procedimento criminal correspondente. Além disso, a tentativa de praticar tais actos também são puníveis, conforme estipulado no n.º 5 do artigo em análise.

[11] Na ciência da computação um *trojan* ou cavalo de troia é um tipo de *software* malicioso que engana os usuários quanto à sua verdadeira intenção, camuflando-se como um programa normal.

[12] Um *keylogger* é um tipo de *software* ou *hardware* que regista todas as teclas digitadas em um teclado, geralmente sem o conhecimento do usuário. Ele é usado por cibercriminosos para capturar informações confidenciais, como senhas e dados, à medida que a vítima as digita em seu dispositivo.

3.4. Dano em dados informáticos (artigo 440º do código penal angolano)[13]

O crime de dano informático era um tipo penal até então desconhecido no ordenamento jurídico angolano. Mesmo sendo assim, os *bens* incorporados em suportes informáticos são igualmente entidades que, à semelhança de outros bens, requerem e demandam, na actualidade, a devida tutela penal.

Para o autor, está evidente que o bem jurídico tutelado no crime em questão assemelha-se à propriedade protegida pelo crime de dano[14] previsto no artigo 410.º do Código Penal Angolano. O tipo clássico dano salvaguarda a propriedade contra lesões intencionais que afectam directamente a integridade ou o estado da coisa, ou seja, proporciona proteção aos bens corpóreos contra danos causados intencionalmente (VERDELHO *et al.*, 2003).

Ora, os programas e os dados informáticos, apesar de não possuírem uma materialidade análoga às coisas que existem de forma autónoma em

[13] Código Penal Angolano, artigo 440º - Dano em dados informáticos:
1. Quem, com intenção de causar prejuízo a terceiro ou de obter beneficio para si ou para terceiro, alterar, deteriorar, inutilizar, apagar, suprimir, ou destruir, no todo ou em parte, ou de qualquer forma, tornar não acessíveis dados alheios, conforme os define a alínea d) do artigo 250.º ou lhes afetar a capacidade de uso, é punido com as penas previstas nos artigos 392º e 393.º em razão do valor do prejuízo causado.
2. A mesma pena é aplicável a quem, com intenção de causar prejuízo a terceiro ou de obter beneficio para si ou para terceiro, destruir, total ou parcialmente, inutilizar, apagar, alterar, danificar, embaraçar, impedir, interromper, perturbar gravemente o funcionamento ou afetar a capacidade de uso de um sistema de informação, conforme é definido na alínea e) do artigo 250.º
3. As penas estabelecidas nos n.ºs 1 e 2 são aplicáveis a quem, não sendo o autor dos crimes descritos nesses números, utilizar, com a intenção de causar prejuízo a outrem ou de obter beneficio para si ou para terceiro, respetivamente, os dados falsos referidos no n.º1 ou o cartão ou dispositivo em que se encontrem registados ou incorporados os dados obtidos com os fatos descritos no n.º2.
4. Se o autor dos fatos descritos nos números anteriores for funcionário público no exercício das suas funções, a pena é de:
a) Prisão de 6 meses a 3 anos de multa de 60 a 360 dias, no caso do n.º1;
b) 4 a 10 anos, no caso dos n.ºs 2 e 3.

[14] Código Penal Angolano, artigo 410º - Dano:
1. Quem causar dano relevante a coisa alheia, destruindo-a, danificando-a, desfigurando-a ou inutilizando-a, é punido com as penas estabelecidas para o crime de furto no artigo 392.º, atendendo ao valor do prejuízo causado pelo dano.

relação ao seu suporte, não deixam de ser considerados *coisas* protegidas. São entidades imateriais, porém apreensíveis empiricamente, expostas à ação humana e susceptíveis de serem objeto de direitos de propriedade, bem como de serem destruídas ou danificadas por diversos meios, como vírus, e, por conseguinte, podem ser abrangidas pelo crime de dano. Assim, no contexto do crime de dano em dados informáticos, o bem jurídico protegido é o funcionamento adequado, ou o uso correcto, de dados ou programas informáticos. A especificidade deste tipo de crime reside no fato de que não se ataca a substância física de um objeto, mas sim as informações contidas em determinados dados ou programas. Contudo, as formas de agressão são análogas, pois também aqui se pune o acto de destruir, danificar ou tornar inutilizável o bem alheio. Portanto, o legislador visou proteger de maneira especial os danos causados a dados e programas informáticos (CASTANHEIRA & ANDRADE, 2009).

Os elementos objetivos tipificadores do crime de Dano Informático, assentam, por um lado na não permissão legal do titular do direito do sistema ou de parte dele e por outro em alterar, deteriorar, inutilizar, apagar, suprimir, ou destruir, no todo ou em parte, ou de qualquer forma, tornar não acessíveis dados alheios, ou lhes afectar a capacidade de uso, enquanto, o elemento subjetivo neste tipo de crime traduz-se na intenção de causar prejuízo a terceiro ou de obter beneficio para si ou para terceiro.

Mudando para a questão do *Phishing*, particularmente ao processo de contaminação dos computadores e dispositivos móveis das vítimas, realizado pelos agentes criminosos e abordando a questão de forma técnica, observa-se que a grande maioria dos ataques se concentra em programas de navegação *web*. Estes navegadores são amplamente utilizados pelos usuários para acessar a *Internet*, incluindo *website* de instituições e redes sociais onde inserem suas credenciais de acesso (*username* e *password*). Os agentes do *Phishing* enganam as vítimas para que revelem informações confidenciais, como senhas ou dados bancários, mediante *e-mails* fraudulentos ou *websites*

falsos. Após obter essas informações, os criminosos podem utilizá-las para acessar sistemas informáticos sem autorização. Esse acesso permite-lhes alterar, deteriorar, inutilizar, apagar, suprimir, ou destruir dados importantes, configurando-se assim o crime de dano em dados informáticos. Por exemplo, após um ataque de *Phishing* bem-sucedido, o *phisher* pode usar as credenciais obtidas para ingressar na rede da vítima e implantar *malware* que corrompe ou apaga arquivos, ou mesmo manipular dados para desviar recursos financeiros. Dessa forma, o *Phishing* não apenas compromete a segurança dos dados, mas também facilita a execução de crimes mais graves, como o dano directo a esses dados.

3.5. burla informática e nas comunicações (artigo 443º do código penal angolano)[15]

A *burla*[16], em sua acepção clássica, exige do agente uma conduta extremamente específica, que se manifesta através de um meio enganoso, o qual constitui a causa efectiva do erro em que se encontra a vítima. Contudo, na burla informática, não se exige a presença de um artifício fraudulento, nem tampouco a participação activa da vítima no processo de execução do crime.

[15] Código Penal Angolano, artigo 443º - Burla informática e nas comunicações:
É punido com as penas estabelecidas para o crime de furto qualificado no n.º 3 do artigo 393.º, atendendo ao valor do prejuízo material causado, quem, com o propósito de obter para si ou para terceiros vantagem patrimonial pelas formas descritas, causar a outrem prejuízos de natureza patrimonial:
a) Interferir no resultado do tratamento de dados conforme definido na alínea d) do artigo 250.º, mediante estruturação incorreta de programas de computador, utilização incorreta e ou incompleta de dados, utilização de dados sem autorização ou mediante intervenção, por qualquer outro modo não autorizado, no processamento;
b) Usar programas, dispositivos ou outros meios que, separada ou conjuntamente, se destinem a diminuir, alterar ou impedir, no todo ou em parte, o normal funcionamento ou exploração do serviço de telecomunicações.

[16] Código Penal Angolano, artigo 417º - Burla:
Quem, usando de qualquer meio astucioso ou enganoso, induzir ou mantiver outrem em erro ou engano e, com o propósito de obter para si ou para terceiro um enriquecimento ilícito, a levar a praticar atos que lhe causem ou causem a terceira pessoa prejuízo patrimonial é punido com as penas estabelecidas para o crime de furto no artigo 392.º, atendendo ao valor do prejuízo patrimonial causado.

Exige-se apenas a intenção de causar um prejuízo patrimonial, utilizando-se, para tal, de um meio informático, ou, mais precisamente, interferindo em um sistema de tratamento de dados.

Concernente aos elementos objetivos da burla informática, em termos do seu resultado, conforme elucidado por Monteiro (2012), estes consistem em causar a outrem prejuízo de natureza patrimonial, concretizando-se através da interferência no resultado do tratamento de dados, mediante estruturação incorrecta de programas de computador, utilização incorrecta e ou incompleta de dados, utilização de dados sem autorização ou mediante intervenção, por qualquer outro modo não autorizado, no processamento. Por oposição, o elemento subjetivo manifesta-se com o propósito de obter para si ou para terceiros vantagem patrimonial, o que implica que o agente da infração tenha plena consciência de que a sua conduta é contrária à lei no que tange aos resultados que produz. Assim, a criminalização da burla informática tem como finalidade não apenas a proteção do património, mas também a salvaguarda da fiabilidade dos dados (por exemplo, transferências eletrónicas de fundos) e a sua proteção.

Clarifica-se que a burla informática configura um crime cuja execução se limita à exigência de que a lesão patrimonial ocorra exclusivamente por meio da utilização de sistemas informáticos, pois, o legislador determinou que tal infração só pode ser cometida através dos meios previstos na norma incriminadora (meios informáticos). Conforme descreve Costa (1999, p. 330), "a burla informática concretiza-se num atentado ao património, num processo executivo que não contempla, de permeio, a intervenção de outra pessoa e cuja única peculiaridade reside no fato de a ofensa ao bem jurídico se observar através da utilização de meios informáticos". Essa característica distingue-a da burla clássica, que, conforme salientado no artigo 417º do Código Penal Angolano, pode ser cometida por recurso a qualquer (meio) erro ou engano quanto aos fatos que o agente astuciosamente induziu.

Entretanto, para se explicar a posição adoptada pelo autor do presente artigo, especialmente em relação ao fenómeno do *Phishing*, que constitui o foco central deste estudo, proceder-se-á uma pequena análise comparativa entre a Burla prevista no artigo 417º e a Burla informática e nas comunicações prevista no artigo 443º ambas do Código Penal Angolano.

Na denominada burla clássica, o recurso a um instrumento informático configura-se como um meio astucioso utilizado pelo agente do crime para induzir a vítima em erro ou engano quanto aos fatos, levando-a a adoptar uma conduta que resulte em prejuízo patrimonial. A título de exemplo, pode-se mencionar um anúncio publicado na *Internet* para a venda de um artigo, como um computador, em que a vítima realiza a compra por transferência bancária, ou outro meio, mas recebe em seu domicílio apenas uma caixa de cartão contendo objetos com peso semelhante ao do artigo pretendido. Embora o ambiente informático seja o meio através do qual as comunicações e transações foram realizadas, tal situação é passível de se enquadrar no âmbito de proteção da burla clássica, e não da burla informática.

A burla informática a que se pretende referir neste artigo, sob a lógica dos ataques de *Phishing*, desenvolve-se através dos seguintes passos: a) envio de mensagens enganosas, com o propósito de induzir a vítima a abrir um *e-mail* ou SMS e proceder ao descarregamento ou execução de um programa malicioso; b) instalação desse programa no computador da vítima, o qual modificará o navegador, redirecionando-a para um *site* fraudulento; c) Utilização de dados de acesso (*username* e *password*) sem autorização para entrar na conta da vítima, seja em aplicativos bancários ou outros; d) Realização de transferências bancárias para contas de destino previamente determinadas pelo agente criminoso.

As ações acima descritas permitem que os agentes do crime preencham os elementos objetivos do tipo penal em questão, uma vez que interferem no resultado do tratamento de dados, mediante (1) estruturação incorrecta de

programas de computador, (2) utilização incorrecta e ou incompleta de dados, (3) utilização de dados sem autorização ou mediante intervenção, por qualquer outro modo não autorizado, no processamento. Assim, a estruturação do programa informático é considerada incorrecta quando diverge da finalidade para a qual foi projetado, gerando novas instruções e resultados objetivamente contrários ao propósito original desse programa. No caso em análise, a estruturação incorrecta ocorre por meio da manipulação do *browser*.

Dessa forma, a vítima poderá ser direccionada a um *site mascarado* que imita o original, induzindo-a, por meio de erro, a inserir todos os seus dados em campos especificamente criados para esse fim. De posse desses dados e com a capacidade de manipulá-los, os criminosos acessarão a conta do lesado, preenchendo assim os elementos objetivos do tipo penal de burla informática e nas comunicações.

3.6. Branqueamento de capitais (artigo 82º da Lei n.º 5/20 – Lei de Prevenção e Combate ao Branqueamento de Capitais, do Financiamento do Terrorismo e da Proliferação de Armas de Destruição em Massa)[17]

[17] Lei n.º 5/20 – Lei de Prevenção e Combate ao Branqueamento de Capitais, do Financiamento do Terrorismo e da Proliferação de Armas de Destruição em Massa, Artigo 82.º - Branqueamento de capitais:
1. Comete o crime de branqueamento de capitais e é punido com pena de prisão até 2 (dois) a 8 (oito) anos, quem:
a) Converter, transferir, auxiliar ou facilitar alguma operação de conversão ou transferência de vantagens obtidas por si ou por terceiro, com o fim de dissimular a sua origem ilícita ou de evitar que o autor ou participante da infração seja criminalmente perseguido ou submetido a uma ação criminal;
b) Ocultar ou dissimular a verdadeira natureza, origem, localização, disposição, movimentação ou titularidade de bens ou dos direitos relativos a esses bens, tendo conhecimento que esses bens ou direitos são provenientes da prática, sob qualquer forma de comparticipação das infrações previstas no n.º 4 do presente artigo;
c) Adquirir, possuir ou utilizar bens ou dos direitos relativos bens, tendo aquele que os adquire, possui ou utiliza, conhecimento deque no momento da sua receção, esses bens são provenientes da prática sob qualquer forma de comparticipação das infrações previstas no n.º4 do presente artigo, são punidos com a mesma pena.

A problemática da ocultação dos proventos decorrentes de actividades delituosas suscitou, desde os primórdios, uma preocupação tanto por parte dos agentes envolvidos em práticas criminosas quanto das entidades responsáveis pela concepção e implementação de mecanismos de combate à criminalidade em suas múltiplas facetas. O branqueamento de capitais configura-se como um fenómeno de relevância jurídico-penal relativamente recente em Angola, ainda que os autores de ilícitos penais tenham, desde sempre, envidado esforços no sentido de conferir uma aparência de legalidade aos recursos provenientes das suas actividades criminosas.

De forma pragmática, o branqueamento de capitais consiste num processo pelo qual se visa ocultar a origem ou proveniência ilícita de determinados bens, obtidos como vantagens de actividades criminosas, para posteriormente introduzi-los no mercado lícito. Trata-se de um crime cujas condutas típicas não causam uma lesão definitiva e irreversível ao bem jurídico, mas sim colocam em risco a concretização da justiça, especialmente no que concerne à apreensão e perda dos benefícios resultantes do crime (SÁ PEREIRA & LAFAYETTE, 2006).

O tipo objetivo do crime de branqueamento de capitais encontra-se previsto no n.º 1, alínea a), do artigo 82.º da Lei n.º 5/20, que estabelece que quem converter, transferir, auxiliar ou facilitar alguma operação de conversão ou transferência de vantagens obtidas por si ou por terceiro, com o fim de dissimular a sua origem ilícita ou de evitar que o autor ou participante da infração seja criminalmente perseguido ou submetido a uma ação criminal, é punido com pena de prisão de 2 a 8 anos. A alínea b) do mesmo número sanciona aquele ocultar ou dissimular, não propriamente as vantagens, mas sim, por um lado, a verdadeira natureza, origem, localização, disposição, movimentação ou titulariedade de bens, ou, por outro ângulo, direitos relativos a esses bens. É evidente, portanto, a preocupação do legislador em estender a proteção jurídica a todo e qualquer auxílio ou colaboração, indo além das ações do próprio beneficiário/agente das vantagens ilícitas.

A relação entre o branqueamento de capitais e o *Phishing* revela uma interdependência na execução desses crimes, onde os ataques de *Phishing* representam um papel definidor na facilitação das etapas subsequentes do branqueamento de capitais. Por exemplo, o ataque de *Phishing* na modalidade de burla informática, permite aos criminosos, por meio de técnicas sofisticadas, obter dados sensíveis das vítimas, como credenciais de acesso a contas bancárias, utilizadas para realizar transferências não autorizadas de valores. Esses montantes, uma vez transferidos para contas controladas pelos agentes do crime, torna-se o produto material de ilícitos, que posteriormente passam pelos processos de conversão, transferência, ocultação e dissimulação, característicos do branqueamento de capitais.

Por último, o branqueamento de capitais, conforme definido no artigo 82.º da Lei n.º 5/20, depende da existência de um crime antecedente, listado nos crimes de catálogo mencionados no n.º 1 do mesmo artigo, sendo, portanto, um crime derivado e de conexão. Isso significa que, sem a prática de um ilícito anterior (os crimes aos quais utilizam os ataques *Phishing*) que gera os fundos ilícitos, o branqueamento de capitais não poderia ocorrer. Dessa forma, o *Phishing* não apenas viabiliza o prejuízo patrimonial das vítimas, mas também serve como o meio pelo qual os criminosos obtêm os recursos necessários para serem branqueados, completando assim o ciclo criminoso que abrange desde a obtenção fraudulenta de fundos até a sua integração na economia formal de maneira aparentemente legítima.

4. Conclusão

O presente artigo partiu do problema central de saber como o ordenamento jurídico-penal angolano pode enquadrar e sancionar as condutas típicas do *Phishing*, tendo em conta que o referido crime não possui, até o momento, uma tipificação penal autónoma no sistema jurídico-penal angolano. A análise empreendida demonstrou que, embora inexistente como

figura típica expressa, o fenómeno do *Phishing* encontra correspondência material em diversos tipos legais já previstos no Código Penal Angolano, revelando a capacidade adaptativa e interpretativa do direito penal face às novas formas de criminalidade informática.

Ao longo do trabalho, verificou-se que as condutas associadas ao *Phishing*, possíveis de ser enquadradas à luz do código penal angolano, tais como a falsidade informática (artigo 442º), o acesso ilegítimo a sistema informático (artigo 438º), o dano em dados informáticos (artigo 440º), a assunção ou atribuição de falsa identidade (artigo 274º) e, de modo especial, a burla informática e nas comunicações (artigo. 443.º), abrangem comportamentos equivalentes aos praticados nos esquemas fraudulentos de *Phishing*. Tais dispositivos legais, embora concebidos para uma realidade tecnológica distinta, permitem uma resposta penal adequada às ofensas informáticas que afetam bens jurídicos como a integridade patrimonial, a privacidade digital e a confiança nas comunicações eletrónicas.

Do ponto de vista jurídico-material, constata-se que a ausência de uma tipificação específica para o *Phishing* não implica um vazio normativo absoluto, mas antes um desafio hermenêutico que convoca a doutrina e a jurisprudência a reconhecer a natureza híbrida e multifacetada desse fenómeno, situado entre a fraude tradicional e o cibercrime moderno. Assim, o ordenamento angolano revela-se capaz de responder penalmente a condutas lesivas praticadas em ambiente digital, desde que interpretado em conformidade com os princípios de legalidade, proporcionalidade e tutela efetiva dos bens jurídicos.

Contudo, o estudo evidencia também a necessidade de aperfeiçoamento legislativo, tendo em vista a constante sofisticação dos mecanismos de ataques cibernéticos e a emergência de novas formas de manipulação digital, que escapam às categorias tradicionais do direito penal. Nesse sentido, e enquanto autor deste artigo, apresento uma proposta de criação de um tipo penal autónomo de *Phishing*, cuja redação poderia ser formulada nos

seguintes termos: *Phishing* é a prática fraudulenta de obtenção de dados pessoais, bancários ou informações sensíveis mediante o uso de manipulação digital, engenharia social ou simulação de identidade legítima através de meios eletrónicos, com o intuito de obter vantagem ilícita ou causar prejuízo a outrem.

A consagração expressa desse tipo penal contribuiria significativamente para aumentar a segurança jurídica, reforçar a precisão normativa e elevar a eficácia repressiva no combate à criminalidade informática em Angola, alinhando o ordenamento jurídico-penal angolano com as melhores práticas e padrões internacionais de proteção cibernética.

Em síntese, conclui-se que o direito penal angolano dispõe, atualmente, de instrumentos normativos suficientes para sancionar condutas de *Phishing* por via de interpretação integrativa, mas carece de modernização legislativa para acompanhar a velocidade das transformações tecnológicas e garantir uma tutela penal específica, coerente e preventiva. Este artigo, ao lançar luz sobre essa problemática, não pretende esgotar o debate, mas antes estimular novas reflexões doutrinárias e legislativas sobre o enfrentamento do cibercrime em Angola, especialmente na intersecção entre direito penal, tecnologia e segurança informacional.

Referências

ALABDAN, R. **Phishing attacks survey: Types, vectors, and technical approaches**. *Future Internet*, v. 12, n. 10, p. 1-39, 2020. Disponível em: https://doi.org/10.3390/fi121000168. Acesso em: 12 out. 2025.

ANGOLA. DECRETO-LEI n.º 38/20 da Assembleia Nacional: **Lei que aprova o Código Penal Angolano.** Diário da República: I Série, N.º 179, 2020. Disponível em: https://tribunalsupremo.ao/wp-content/uploads/2023/03/C%C3%B3digo-Penal-e-do-Processo-Penal-Angolanos-2020-DRI-179_11-Novembro-176_230110_151357-1.pdf. Acesso em: 12 set. 2025.

ANGOLA. **Constituição da República de Angola da Assembleia Nacional**. *Diário da República*: I Série, n.º 23, 5 fev. 2010. Disponível em: https://www.tribunalconstitucional.ao/docs/Constituicao_da_Republica_de_Angola.pdf. Acesso em: 12 set. 2025.

ANGOLA. LEI N.º 22/11, da Assembleia Nacional: **Lei da proteção de dados pessoais.** Diário da República: I Série, N.º 114, 2011. Disponível em: https://apd.ao/ao/legislacao/. Acesso em: 21 fev. 2025.

ANGOLA. LEI N.º 5/20 da Assembleia Nacional: **Lei de prevenção e combate ao branqueamento de capitais, do financiamento do terrorismo e da proliferação de**

armas de destruição em massa. Diário da República: I Série, N.º 10, 2020. Disponível em: https://www.paced-paloptl.com/uploads/publicacoes_ficheiros/lei-lei-de-prevencao-e-do-combate-ao-branqueamento-de-capitais-financiamento-do-terrorismo-e-da-proliferacao-de-armas-de-destruicao-massiva.pdf. Acesso em: 12 nov. 2025.

BALZAROTTI, D.; COVA, M.; VIGNA, G. **ClearShot: Eavesdropping on keyboard input from video**. In: *2008 IEEE Symposium on Security and Privacy*, 2008, p. 170–183. IEEE. Disponível em: https://doi.org/10.1109/SP.2008.25. Acesso em: 11 nov. 2025.

CASTANHEIRA, R.; ANDRADE, M. C. **Direito penal hoje: Novos desafios e novas respostas**. Coimbra: Coimbra Editora, 2009.

COSTA, A. M. A. **Comentário conimbricense do Código Penal, Vol. II**. Coimbra: Coimbra Editora, 1999.

HONG, J. **The state of Phishing attacks**. *Communications of the ACM*, v. 55, n. 1, p. 74-81, 2012. Disponível em: https://doi.org/10.1145/2063176.2063197. Acesso em: 10 nov. 2025.

KHONJI, M.; IRAQUI, Y.; JONES, A. **Phishing detection: A literature survey**. *IEEE Communications Surveys & Tutorials*, v. 15, n. 4, p. 2091–2121, 2013. Disponível em: https://doi.org/10.1109/SURV.2013.032213.00009. Acesso em: 12 mai. 2025.

LASTDRAGER, E. E. **Understanding Phishing: A systems approach [Doctoral dissertation, University of Twente]**. University of Twente Research Information, 2014. Disponível em: https://doi.org/10.3990/1.9789036536865. Acesso em: 4 abr. 2025.

MARTINS, A. G.; MARQUES, J. A. G. **Direito da informática**. Almedina, 2006.

MILLETARY, J.; CENTER, C. **Technical trends in Phishing attacks**. *Journal of Criminology*, v. 1, p. 3, 2007. Disponível em: https://www.cisa.gov/sites/files/Phishing_trends.pdf. Acesso em: 14 out. 2025.

MONIZ, H. I. G. **O crime de falsificação de documentos: Da falsificação intelectual e da falsificação em documento**. Coimbra: Coimbra Editora, 2004.

MONTEIRO, C. **Aulas do curso de direito e informática da Universidade do Minho**. Universidade do Minho, 2012.

OXFORD ENGLISH DICTIONARY**. Phishing**. In: *Oxford English Dictionary online*. Oxford University Press. Disponível em: https://www.oed.com. Acesso em: 5 jan. 2025.

PINHEIRO, P. P. **Segurança digital: Proteção de dados**. São Paulo: Saraiva Educação, 2020.

RODRIGUES, B. S**. Da prova penal tomo IV: Da prova eletrónico-digital e da criminalidade-informático-digital**. Rei dos Livros, 2011.

RODRIGUES, O. **Apontamentos de direito penal**. Escolar Editora, 2016.

SÁ PEREIRA, F.; LAFAYETTE, L. **Direito penal econômico: Parte geral e parte especial**. Rio de Janeiro: Lumen Juris, 2006.

SEBASTIÃO, S**. Ataques cibernéticos em Angola crescem 21% ao ano**. *Forbes África Lusófona*, 28 jul. 2022. Disponível em: https://www.forbesafricalusofona.com/ataques-ciberneticos-em-angola-crescem-21/. Acesso em: 17 jun. 2025.

VENÂNCIO, P. D. **Lei do cibercrime anotada e comentada**. Coimbra: Coimbra Editora, 2011.

VERDELHO, P.; BRAVO, R.; ROCHA, M. L**. Leis do cibercrime Vol. I**. Centro Atlântico, 2003.

Artigo recebido em: 26/11/2025.
Aceito para publicação em: 16/12/2025.