FRAUDE DIGITAL E PHISHING: DESAFIOS PARA A EFICÁCIA DA LEI PENAL NO ENFRENTAMENTO DOS CRIMES CIBERNÉTICOS

DIGITAL FRAUD AND PHISHING: CHALLENGES TO THE EFFECTIVENESS OF CRIMINAL LAW IN COMBATING CYBERCRIMES

Arilson Divino de Souza 1
Patrick Silva Rodrigues 2
Realina Maria Ferreira 3

Resumo: Este trabalho investiga os desafios da eficácia da norma penal no enfrentamento aos crimes cibernéticos, em especial à fraude digital por meio do Phishing. Hodiernamente, com a crescente concentração de dados pessoais e acessos aos serviços de instituições e empresas por meio da Internet, avançou-se também as práticas criminosas, que utilizam de mensagens, e-mails, links e outros acessos para enganar e furtar os dados dos usuários. Desse modo, é partindo do questionamento de como se apresenta a eficácia da lei penal brasileira para reprimir e punir os crimes cibernéticos, em especial as fraudes digitais, que o presente artigo se faz pertinente. Assim, buscou-se observar a evolução digital no Brasil, compreendendo o alcance da norma brasileira no campo virtual, em especial sobre a fraude digital por meio do Phishing, além de analisar a eficácia punitiva da lei penal no furto de dados pela prática do Phishing. Enfim, notou-se que o direito penal brasileiro ainda não se mostra plenamente eficaz no enfrentamento destes atos criminosos, pois trata-se de condutas recentes, cujas bases da legislação não acompanharam efetivamente o avanço rápido da tecnologia para prever a incidência massiva dos crimes cibernéticos.

Palavras-chave: Direito penal; enfrentamentos; Crimes Cibernéticos; Phishing;

Abstract : This paper investigates the challenges to the effectiveness of criminal law in addressing cybercrimes, particularly digital fraud through phishing. Nowadays, with the growing concentration of personal data and access to institutional and corporate services via the Internet, criminal practices have also evolved, using messages, emails, links, and other means to deceive and steal users' data. Thus, starting from the question of how effective Brazilian criminal law is in repressing and punishing cybercrimes, especially digital fraud, this article becomes relevant. The study seeks to examine the digital evolution in Brazil, understanding the reach of Brazilian law in the virtual sphere, particularly regarding digital fraud through phishing, and to analyze the punitive effectiveness of criminal law in cases of data theft committed via phishing. Ultimately, it is observed that Brazilian criminal law still does not prove to be fully effective in confronting such criminal acts, as these are recent behaviors and the legal framework has not effectively kept pace with the rapid advancement of technology to anticipate the massive occurrence of cybercrimes.

Keywords: Criminal Law; Approaches; Cybercrimes; Phishing.

1 - Graduando em Direito pela Universidade do Estado de Minas Gerais. Lattes: http://lattes.cnpq.br/4678370647067661, ORCID: 0009-0006-4923-0052. E-mail: patricksilvargs@gmail.com

2 - Graduando em Direito pela Universidade do Estado de Minas Gerais. Lattes: http://lattes.cnpq.br/3924592967807096. Email: arilson.1595049@discente.uemg.br.

3 - Professora na Universidade do Estado de Minas Gerais. Lattes: http://lattes.cnpq.br/0524391606666482. ORCID: 0524-3916-0666-6482. Email: realinaferreira@unifimes.edu.br

Introdução

Prima Facie, torna-se incontestável que a sociedade hodierna está passando por um acelerado avanço tecnológico. Por vezes, o acesso à internet encontra caminhos diversos, dos quais não há o pleno alcance da fiscalização estatal. Desse modo, o conceito de liberdade se estende mais nos ambientes digitais, visto que o controle é notadamente precário, haja vista que o direito não consegue acompanhar o frenético avanço proporcionado pelas novas tecnologias (PINHEIRO, 2009). É nesse contexto de evolução, que as práticas criminosas encontram meios para se desenvolver e evoluir, surgindo os chamados Crimes Cibernéticos. Estes, por sua vez, pode-se entender como crimes praticados por meio de computadores ou contra eles, de maneira que a conduta delituosa se consuma, em grande parte, pela rede de internet (SCHMI-DT, 2014 apud CASTRO, 2003).

Destarte, no bojo dessa nova modalidade de crimes em desenvolvimento, nascem espécies de condutas antijurídicas e culpáveis, como exemplo a Fraude Digital. Ao fazermos um recorte mais profundo na temática, observa-se, ainda, que tal modalidade ainda é gênero, do qual uma gama de meios torna-se espécie da prática delituosa. É nesse cenário que entra o *Phishing*, uma conduta fraudulenta, a qual criminosos buscam obter dados e informações de várias pessoas, por meio do envio de links, mensagens, e-mails ou outros meios de comunicação digital, se passando por entidades financeiras, empresas e entre outras modalidades, sendo extensos os meios para tal fim.

Nesse diapasão, diante de uma espécie de transcendência dos crimes já existentes, ou seja, uma elevação para outros ambientes, como é o caso da fraude digital por meio do *Phishing*, que nasce a preocupação do direito penal alcançar tais condutas criminosas, com fito a não deixar impunes os sujeitos que utilizam de um ambiente do qual as normas ainda não produzem uma eficácia de punição.

Assim sendo, ao partir da questão de quais são os desafios para o alcance e eficácia da lei penal brasileira para enfrentar os ditos crimes cibernéticos, com foco especial à fraude digital por meio do *Phishing*, este trabalho terá como fim analisar o contexto de evolução deste crime, coletando dados teóricos, de maneira a observar a evolução digital no Brasil e compreender o alcance da norma brasileira no campo virtual, discutindo sobre a fraude digital por meio do "Phishing", além de analisar a eficácia punitiva da lei penal no furto de dados pela prática do "Phishing".

Assim, caminha-se para um aprofundamento na temática, reunindo as informações necessária à formação de um texto que pretende esmiuçar tais condutas e verificar em que ponto encontra-se a eficácia da norma penal para aplicar as devidas punições.

Compreende-se, pois, que é necessária uma fonte como esta, para que as pessoas se auto conscientizem dos riscos que as redes oferecem, vez que a sociedade se torna cada vez mais dependente das tecnologias e, em contrapartida, cada vez mais vulnerável aos crimes cibernéticos, tendo em vista que criminosos se espreitam nas vias ocultas das redes, procurando as vítimas virtuais para coletar dados e materiais, com a finalidade de obter, muitas vezes, vantagens econômicas.

A evolução digital no Brasil

Conforme preceitua Patrícia Peck Pinheiro, renomada doutrinadora na esfera do direito digital, no fim dos anos 1950 a internet ainda se encontrava em um estágio embrionário de desenvolvimento, desse modo, a concentração de dados pessoais e informações de risco estavam concentradas em papeis apensos nas empresas, bancos ou entidades públicas. Portanto, o acesso era mais restrito, além de mais dificultoso, haja vista a necessidade de apresentar-se presencialmente caso tivesse o interesse de acessar esses bancos de dados. Assim, exigir-se-ia do indivíduo uma apresentação formal, a fim de averiguar o interesse naquele ato.

Nesse diapasão, conforme apresentado pela doutrinadora, ao longo das décadas seguintes, o projeto que antes era embrionário foi tomando forma, ao passo que a internet

foi se desenvolvendo no país e no mundo. Desse modo, aqueles dados registrados em papeis foram migrando para os sistemas inteligentes, chamado de banco de dados digital. Não foi preciso ir muito além, encontramo-nos na segunda década deste século, e a gama de sistemas informatizados é assustadoramente alta, ou seja, o avanço tecnológico tornou-se tão rápido, que há 10 anos muitas das coisas que usamos hoje, que parecem nativas, não existiam (CARLINI, 2022).

Nesse sentido, observa-se que foi criado um novo espaço na realidade, não sendo este materialmente palpável, porém, acessível de maneira rápida e fácil. Trata-se dos ambientes virtuais, os quais interligam uma vasta rede de comunicações em tempo real, integrando o mundo em um único e concentrado ponto de navegação digital. É nesse contexto que vale dar destaque à seguinte passagem:

> A sociedade humana vive em constante mudança: mudamos da pedra talhada ao papel, da pena com tinta ao tipógrafo, do código Morse à localização por Global Positioning System (GPS), da carta ao e-mail, do telegrama à videoconferência. Se a velocidade com que as informações circulam hoje cresce cada vez mais, a velocidade com que os meios pelos quais essa informação circula e evolui também é espantosa. [PINHEIRO, 2022, pág.47]

Destarte, com o avanço mencionado e a celeridade em processar informações, a migração de atendimentos outrora realizados em papeis e arquivos físicos para o ambiente virtual foi necessário. Como bem pontuou a doutrinadora no pequeno recorte supracitado, a velocidade das informações cresce cada vez mais, e os meios por onde circulam estão em constante transformação. Assim, os bancos de dados pessoais, vinculados a instituições financeiras, empresas com sites digitais e até mesmo ambientes virtuais do governo para atendimento ao público estão cada dia mais robustos.

Isto posto, é notório que o acesso às redes está mais fervoroso, dada a praticidade e celeridade em resolver os problemas do dia a dia do cidadão e das empresas. Dados do Instituto Brasileiro de Geografia e Estatística – IBGE, destacou em uma pesquisa de 2018, que sete a cada dez brasileiros estão conectados à *Internet*. Não muito distante, um estudo divulgado pelas empresas We are Social e Hootsuite em 2019, ressaltou que 66% da população brasileira está ativa nas redes sociais.

Portanto, nota-se que há uma grande concentração de atividades desenvolvidas nesse novo ambiente que ganha, ao passar dos dias, mais espaço entre as pessoas e as empresas, alcançando até mesmo os serviços fornecidos pelos governos. Desse modo, tal avanço torna-se fulcral para o desenvolvimento social e organização do país, visto que traz aos cidadãos a praticidade que outrora não havia, tornando mais célere e menos burocrático algumas ações da vida civil.

Todavia, ainda que não seja visto no plano material, por tratar-se de um ambiente virtual, observa-se que as relações jurídicas estão presentes de maneira extremamente visível, com tendência a crescer mais a cada ano, seja em questão de compras, negociações em instituições financeiras, armazenamento de dados, entre outras infinitas práticas da vida jurídica. Assim, torna-se necessário que o sistema jurídico intervenha nessas ações tal qual intervém no mundo material, pois ainda está presente as condutas humanas. Portanto, aí também deve estar o direito.

Desse modo, pertinente faz-se observar como é a incidência Jurídica no campo virtual, tendo em vista o expressivo avanço da tecnologia no contexto brasileiro atual.

O alcance jurídico no campo virtual

Não se pode olvidar que o mundo digital já é parte integrante da sociedade atual, nele as relações jurídicas estão em constante movimentação. Desse modo, é fundamental que o sistema legislativo esteja atento para as demandas provenientes desse meio, haja vista a

necessidade de tutela dos direitos nesse ambiente.

É nesse cenário que verificamos a dificuldade da incidência normativa em um espaço tão recente, cujas bases não puderam ainda ser amplamente tutelada pelo direito, portanto, acertadas são as palavras da professora Patrícia:

> O grande desafio do Direito é enfrentar essa contradição entre globalização e individualização, que é a grande característica de nossa era — uma era de transição, em que convivem conceitos aparentemente tão díspares. Na nova ordem mundial, não é possível receitar um mesmo remédio para toda a economia. No caso brasileiro, esse desafio é ampliado por vivermos em uma sociedade que, durante tanto tempo, esteve sob regimes autoritários e, em sua cultura jurídica, guarda ainda muitos resquícios desse autoritarismo. Para enfrentar uma realidade tão difusa e complexa, é imprescindível que os profissionais do Direito revejam sua forma de atuação, aplicando os princípios fundamentais e desenvolvendo novas soluções para atender às demandas futuras. [PINHEIRO, 2022, pág.47]

Destarte, não há como iniciar tal contexto sem falar de um marco importante para a regulamentação digital no Brasil. Trata-se do Marco Civil da Internet, a Lei nº 12.965 de 23 de abril de 2014, a qual exerceu um impacto significativo na aplicação do direito no espaço virtual. Referente ao tema em tela, verifica-se que a lei concedeu uma seção específica para o tratamento dos dados disponíveis em redes da internet. Nessa vertente, a seção II da referida lei trata sobre a proteção aos registros, aos dados pessoais e às comunicações privadas, seguida da seção III, a qual dispõe sobre as Responsabilidades por Danos Decorrentes de Conteúdo Gerado por Terceiros.

Assim, nota-se que o direito vem, timidamente, abordando a temática do campo virtual, tentando regular suas estruturas e possibilitar uma tutela dos direitos e deveres nessa seara. A Lei supracitada é uma das mais importantes no atual ordenamento jurídico, no quesito sobre incidência jurídica no campo digital, porém, outros marcos também foram importantes para dispor sobre regulamentações na esfera digital, ainda que não estruturem uma totalidade de medidas eficazes.

Cita-se, nesse momento, o próprio Código de Processo Civil, que menciona sobre normas para o desenvolvimento de processos judiciais eletrônicos, bem como a Lei Geral de Proteção de Dados, lei nº 13.709/2018, tendo por objetivo proteger os direitos fundamentais de liberdade e privacidade, incidindo no campo digital com grande importância, frente ao crescente aumento nos crimes cibernéticos envolvendo dados pessoais na internet.

Noutra vertente, a Lei nº 12.737/2012, conhecida como lei Carolina Dieckmann, estabeleceu os princípios, garantias e deveres para o uso da internet no âmbito nacional. O texto da referida norma incluiu no Código Penal brasileiro alterações significativas para tipificar, pela primeira vez, crimes virtuais com natureza de delitos informáticos, tendo como condutas tipificadas criminalmente, por exemplo, a invasão de dispositivos eletrônicos com finalidade de obter, adulterar ou destruir dados ou informações contra a vontade do proprietário o aparelho atingido ou o usuário das redes de informática.

Nessa seara, é fundamental analisar como o direito penal é abordado no plano virtual, com fulcro a observar como é a tipificação de crimes cibernéticos, bem como os desafios para a norma penal garantir a tutela do bem jurídico atingido e a repressão das condutas criminosas que se espalham exponencialmente no país.

O direito penal digital e seus desafios na área virtual

O direito digital enfrenta o desafio de lidar com as dificuldades de obtenção de provas, impostas pela complexidade da tecnologia. Trata-se de situações inovadoras, marcadas por

fatos de difícil acesso e entendimento, que frequentemente resultam em repercussões negativas para os usuários. Entre esses problemas, destacam-se *Phishing* de Boletos, quando envolve uma tentativa de enganar a vítima por e-mail, para pagamento de boletos falsos, fraudes e falsificações. A tecnologia tem a capacidade de criar fatos aparentemente reais, confundindo internautas que dependem dela para finalidades pessoais ou profissionais, levando-os a cair em golpes perpetrados por infratores que, devido ao avanço tecnológico, são difíceis de identificar.

Diante desse cenário, o direito digital busca punir os infratores, mas enfrenta a lentidão na aprovação de normas, que muitas vezes não acompanham a velocidade das inovações tecnológicas. Essa realidade exige que os advogados sejam ágeis na interpretação e aplicação das leis, assegurando a proteção dos direitos dos usuários e a garantia da privacidade, através da utilização expostas na LEI Nº 14.155/2021 (Artigo. 154-A do Código Penal.)

O artigo 154-A do Código Penal brasileiro define o crime de invasão de dispositivo informático, que consiste em: *Invadir um computador ou dispositivo semelhante de outra pessoa, alterar ou apagar informações, aceder a dados privados, instalar vulnerabilidades para obter vantagem ilícita.*

A pena para este crime é de reclusão de 1 a 4 anos e multa. A pena pode ser aumentada de 1/3 a 2/3 se a invasão resultar em prejuízo económico. Se a invasão resultar na obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, a pena é de reclusão de 2 a 5 anos e multa.

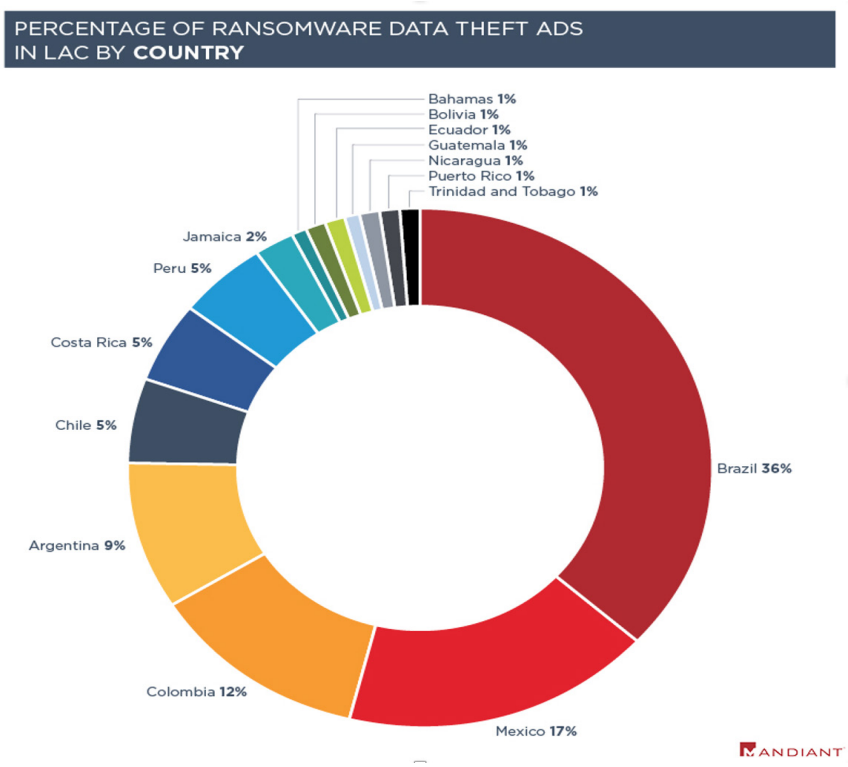
O artigo 154-A também prevê que quem produzir, oferecer, distribuir, vender ou difundir um dispositivo ou programa de computador com o intuito de permitir a prática da invasão incorre na mesma pena.

Pode-se também fundamentar na necessidade de garantir a segurança dos usuários contra ataques de hackers, que violam a privacidade ao obter dados pessoais de internautas. Esses ataques frequentemente resultam em indução ao pagamento de boletos fraudulentos ou direcionamento para sites falsos, criados para se passarem por páginas legítimas de empresas. Esses sites falsificados reproduzem as características e solicitações de informações das páginas originais, enganando os usuários. A fraude geralmente só é descoberta quando as mercadorias não chegam ou os pagamentos realizados não são efetivados.

Como se pode observar, o direito penal digital enfrenta grandes desafios, sendo crescente a necessidade de endurecimento das leis e ampliação das penas de reclusão para crimes cibernéticos e virtuais de forma inibir o crime. Essa rigidez se justifica pelos alarmantes dados sobre o aumento dessas práticas ilícitas.

Durante a pandemia de Covid-19, por exemplo, os crimes cibernéticos cresceram de acordo com dados levantados pela ferramenta de coleta e análise de segurança cibernética - *Fortinet Threat Intelligence Insider Latin America* - mais de 2,6 bilhões de atos virtuais criminosos foram registrados no Brasil nos primeiros seis meses do ano de 2020, ou seja o Brasil respondeu por 36% das 20 bilhões de tentativas de ataques cibernéticos, de janeiro a setembro de 2020, em toda a América Latina e Caribe. Isso equivale a 6,8 bilhões de tentativas de ataques cibernéticos.

Imagem 1. RANKING MUNDIAL DE RANSOMWARE



Fonte: https://cloud.google.com/blog/topics/threat-intelligence/top-cyber-threats-to-latin-america-and-the-caribbean/

Com base nisso, observa-se que o isolamento social contribuiu para a intensificação desses

crimes, já que as pessoas passaram mais tempo conectadas, realizando transações online. O advento do PIX, que facilitou operações financeiras, também tornou as transações mais ágeis, mas abriu brechas para criminosos digitais. Diariamente, pessoas são submetidas a golpes por organizações criminosas digitais que montam estruturas complexas e difíceis de rastrear.

A crescente tendência tecnológica da sociedade, evidenciada durante o período de isolamento social na pandemia e pelo surgimento de ferramentas como o PIX e o DDA (Débito Direto Autorizado) para pagamento de boletos bancários, abriram brechas que resultou em um aumento significativo nos crimes digitais, com os golpes *phishing* de boletos, *ransomware* e fraudes em transações financeiras que revelam a sofisticação das estratégias de criminosos cibernéticos. Estes delitos exploram a tecnologia e invadem a privacidade, roubando dados e extorquindo vítimas, causando danos financeiros e emocionais.

Além disso, a atuação das autoridades enfrenta desafios devido à complexidade em reunir provas e identificar os infratores. A estatística demonstra a gravidade e a escala desses problemas, que ainda se deparam com limitações na legislação atual. Isso indica que são necessárias medidas mais rígidas para acompanhar o rápido avanço tecnológico e inibir as condutas criminosas.

É fundamental investir em soluções, incluindo o endurecimento das penas para crimes digitais, a especialização das forças de segurança e do judiciário, além do fortalecimento de estratégias preventivas. Somente por meio de uma abordagem mais precisa será possível proteger os cidadãos e garantir a privacidade e confiança na tecnologia, sendo implantadas já nos desafios que começam no registro das ocorrências.

Em muitos casos, as autoridades enfrentam dificuldades para reunir provas ou identificar os infratores, o que impede a instauração de inquéritos policiais. Além disso, as estratégias cada vez mais sofisticadas dos criminosos reforçam esta urgência de uma legislação

penal mais rígida, capaz de acompanhar a evolução tecnológica e proteger os cidadãos contra crimes digitais, talvez alteração do artigo 155, § 4º-B, do Código Penal, ainda não seja suficiente para inibição da conduta, sendo que a pena para o furto mediante fraude cometido por meio de dispositivo eletrônico é de reclusão de 4 a 8 anos, além de multa, que antes era reclusão de 2 anos para forma de inibir as fraudes foram alterados para reclusão de 4 anos.

A pena pode ser aumentada em 1/3 a 2/3 se o crime for praticado por meio de um servidor localizado fora do país. Se o crime for cometido contra um idoso ou vulnerável, a pena pode ser aumentada de 1/3 ao dobro. O furto qualificado pode ocorrer em diversas situações, como: destruição ou rompimento de obstáculo, Abuso de confiança, Fraude, Escalada, Destreza, Emprego de chave falsa e Concurso de duas ou mais pessoas.

Fraude digital por meio de *Phishing*

Fraudes digitais, como o *phishing*, são uma ameaça crescente no ambiente virtual, especialmente pelo uso de e-mails, aparentemente inofensivos. É importante entender que os "atacantes" estão sempre evoluindo suas táticas. Somente a tecnologia não é suficiente para barrar alguns dos ataques mais básicos de *phishing*. Muitas dessas mensagens conseguem contornar as proteções de e-mail e chegam à caixa de entrada como se fossem legítimas.

Hoje, e-mails de *phishing* frequentemente se disfarçam como mensagens enviadas por empresas ou até mesmo por pessoas conhecidas e confiáveis. Por exemplo, um "atacante" pode enviar 20 milhões de mensagens ao mesmo tempo, informando sobre um suposto problema com uma remessa dos Correios. Enquanto muitos destinatários podem ignorar a mensagem por não terem enviado pacotes recentemente, basta que 40 mil pessoas, por exemplo, tenham acabado de despachar encomendas para que o golpe tenha grande eficácia. Isso acontece diariamente, o tempo todo. Estima-se que pelo menos 3,4 bilhões de e-mails de *phishing* sejam enviados em todo o mundo todos os dias, representando metade de todos os ataques de fraude.

Os hackers exploram a curiosidade e o excesso de confiança das pessoas. O excesso de confiança ocorre porque, no geral, acreditamos que somos capazes de diferenciar o que é falso do que é verdadeiro, e muitos pensam que isso não aconteceria consigo. Já a curiosidade pode ser despertada por mensagens que mencionam, por exemplo, uma tentativa de login não autorizado, levando o destinatário a querer descobrir mais detalhes.

Esses fatores humanos tornam os ataques altamente eficazes. Existem também casos mais elaborados, como os de *spear phishing* (ou *phishing* direcionado). Nesses ataques, os fraudadores pesquisam o funcionamento de uma empresa ou instituição para obter informações, como padrões de e-mails e detalhes da estrutura hierárquica. Assim, conseguem identificar responsáveis por pagamentos e bancos utilizados pela organização.

O e-mail continua sendo a principal ferramenta para conduzir negócios online. Um funcionário pode responder centenas de mensagens por semana, o que aumenta a probabilidade de que mensagens maliciosas escapem pelas proteções e sejam tratadas como legítimas, com consequências potencialmente devastadoras para as vítimas e as empresas.

Como estratégias de defesa, a tecnologia atualizada usa os sistemas de "CIBERSEGURANÇA", que é um dos bons antivírus, o qual pode ser usado como meio de proteção de dados, porem essas medidas precisam ser complementadas por uma boa dose de capacidade de não confiar automaticamente em mensagens, ou seja um comportamento preventivo pode fazer toda a diferença.

Por exemplo, ao receber uma mensagem aparentemente legítima dos Correios, evite clicar em links. Em vez disso, entre diretamente em contato com o atendimento ao cliente. Essa recomendação também se aplica a outros casos: antes de clicar em um link para resolver uma multa, baixar um e-book gratuito ou acessar qualquer outro conteúdo, pare e verifique. Certifique-se de que o e-mail veio de um endereço ou organização legítima.

Embora a tecnologia mude rapidamente, o comportamento humano é mais resistente à mudança. Por isso, as estratégias antifraude devem levar em consideração que continuaremos

sendo curiosos e confiantes. Reconhecer nossas vulnerabilidades e entender o que nos leva a ignorar nosso julgamento crítico pode nos ajudar a criar barreiras mais eficazes contra golpes online.

Essa resistência à mudança no comportamento humano também reflete nas dificuldades enfrentadas pelo Judiciário em lidar com crimes virtuais. Algumas jurisprudências destacam os desafios para identificar os criminosos, enquanto mostram que as vítimas, ao tentarem restituir os valores lesados, frequentemente responsabilizam empresas, como instituições financeiras, por falhas de segurança. Um exemplo disso é a jurisprudência do Tribunal de Justiça do Rio de Janeiro, referente à Apelação Cível, que tratou de um caso envolvendo um boleto bancário falso, resultado de uma fraude virtual conhecida como *phishing*, onde a parte autora buscava tanto a devolução dos valores quanto indenização por danos morais.

A fraude ocorreu durante uma suposta compra pela internet, mas não ficou comprovado que a transação foi realizada no site oficial da empresa ré, a B2W Companhia Digital (Americanas.com). O Tribunal destacou a ausência de vínculo entre o boleto gerado e as atividades da empresa, afastando sua responsabilidade pela fraude. Além disso, a instituição financeira envolvida no pagamento foi considerada apenas um intermediário, sem qualquer relação direta com o golpe.

Nesse contexto, o Tribunal reconheceu a ocorrência de fortuito externo, ou seja, um evento imprevisível e inevitável, alheio ao controle das partes rés, o que rompeu o nexo de causalidade necessário para a responsabilização. Como não havia provas de que as rés contribuíram para o prejuízo sofrido pela autora, o Tribunal concluiu pela ausência de responsabilidade objetiva, conforme previsto no Código de Defesa do Consumidor, e entendeu que os danos morais alegados não estavam configurados. Dessa forma, a sentença de improcedência foi mantida, e o recurso da parte autora foi desprovido, isentando as rés de qualquer obrigação de reparação. Vejamos:

> Ementa: APELAÇÃO CÍVEL, AÇÃO INDENIZATÓRIA POR DANOS MATERIAIS E MORAIS. DEMANDA ATRAVÉS DA QUAL A PARTE AUTORA OBJETIVA RESTITUIÇÃO DO VALOR PAGO, BEM COMO A CONDENAÇÃO DAS EMPRESAS RÉS AO PAGAMENTO DE INDENIZAÇÃO POR DANO MORAL. COMPRA REALIZADA PELA INTERNET ATRAVÉS DE BOLETO BANCÁRIO FALSO. FRAUDE VIRTUAL GOLPE CONHECIDO COMO PHISHING, AUSENCIA DE PROVA DE TER O AUTOR EFETUADO A COMPRA NO SITIO ELETRÔNICO DA EMPRESA B82W COMPANHIA DIGITAL IAMERICANAS.COM.) GERAÇÃO DE BOLETO FALSO QUE NÃO POSSUI RELAÇÃO COM SUPOSTO AGIR DA EMPRESA RÉ, POIS AUSENTE QUALQUER PROVA DE QUE A PARTE AUTORA EFETIVAMENTE EFETUOU A COMPRA NO SITE OFICIAL DA PRIMEIRA RECORRENTE, AUSENCIA DE RESPONSABILIDADE DA INSTITUIÇÃO FINANCEIRA, QUE FIGURA APENAS COMO INTERPOSTO DO PAGAMENTO DO BOLETO FALSO. FORTUITO EXTERNO DEMONSTRADO. ROMPIMENTO DO NEXO DE CAUSALIDADE. RESPONSABILIDADE OBJETIVA NÃO RECONHECIDA, DANO MORAL NÃO CONFIGURADO. SENTENÇA DE IMPROCEDENCIA QUE SE MANTEM. PRECEDENTES DESTA CORTE ESTADUAL DE JUSTIÇA. DESPROVIMENTO DO RECURSO. (TJ-RJ-APELAÇÃO: APL XXXXX20208190021 202200151777)

A eficácia punitiva da obtenção ilícita de dados pela prática do Phishing

A obtenção ilícita de dados, especialmente por meio de práticas como o *phishing*, tem se

tornado um dos maiores desafios para a segurança cibernética no Brasil, afetando diretamente a confiança nas instituições financeiras. Nesse cenário, o Governo Federal anunciou uma nova estratégia para enfrentar os crimes cibernéticos, Decreto nº 10.222/2020 - Estratégia Nacional de Segurança Cibernética, Com medidas voltadas à prevenção de fraudes bancárias eletrônicas e golpes digitais. Esse plano pode ser fundamental para reduzir os problemas cibernéticos, especialmente relacionados às instituições financeiras.

Em 23 de março de 2022, foi lançado o Plano Tático de Combate aos Crimes Cibernéticos, um convênio firmado entre a Polícia Federal e a Federação Brasileira de Bancos (Febraban), sob a coordenação do Ministério da Justiça. O plano traça uma série de medidas para reduzir a ocorrência de crimes cibernéticos no ambiente financeiro. Na ocasião do lançamento, a Febraban destacou que suas ações individuais em 2021 conseguiram evitar fraudes que poderiam ultrapassar 4 bilhões de reais, beneficiando diretamente os clientes dos bancos brasileiros.

Uma das iniciativas mais relevantes é a criação de um banco de dados centralizado de ocorrências cibernéticas, acessível às polícias judiciais, como as polícias civis da União e dos estados. Essa centralização promete maior precisão, rapidez e assertividade na resolução de crimes cibernéticos. O plano inclui ainda eixos temáticos, como a prevenção e investigação de ameaças cibernéticas, o gerenciamento de riscos e incidentes, e o aprimoramento das infraestruturas críticas com controles de segurança necessários. Também prevê padronização e integração internacional, o que é essencial para setores como o financeiro.

Na estrutura do plano, prevê espaço para mais pesquisas, desenvolvimento, inovação e educação voltados ao combate à criminalidade cibernética. A integração das bases de informação entre diferentes setores e polícias deverá melhorar os tempos de resposta e a eficiência no combate a essas atividades criminosas.

Outro destaque no campo da segurança cibernética ocorreu em 24 de março de 2022, quando a polícia da Inglaterra prendeu vários membros do grupo Lapsus$, conhecido por ataques a grandes empresas brasileiras e internacionais. Foram detidas sete pessoas, com idades entre 16 e 21 anos, na região de Londres. O suposto líder do grupo, um jovem de 16 anos, utilizava o pseudônimo “White”, possivelmente em referência ao personagem White Rose da série “Mr. Robot”.

O grupo Lapsus$ causou prejuízos significativos a várias organizações, incluindo o Ministério da Saúde do Brasil. A polícia brasileira continua até atualidade investigação a participação de brasileiros nessas atividades, mas as apurações ainda não foram concluídas.

Esses eventos destacam a importância de iniciativas robustas no combate à criminalidade digital, reforçando a segurança da informação como um tema crucial para governos, empresas e indivíduos. Nesse contexto, a crescente sofisticação dos golpes cibernéticos exige atenção redobrada, especialmente de correntistas e usuários de serviços bancários. O Banco do Brasil alinhado a essa necessidade, enfatiza a conscientização sobre as ameaças digitais, oferecendo orientações claras para evitar prejuízos significativos. A segurança digital é uma responsabilidade compartilhada entre as instituições financeiras e seus clientes, e a colaboração de todos é fundamental para enfrentar os desafios da era digital. Agir rapidamente e comunicar o banco pode minimizar os impactos.

Devido aos acontecimentos envolvendo clientes do Banco do Brasil S/A em 25 de dezembro de 2024, relacionados a crimes cibernéticos com saques indevidos nas contas dos correntistas, o Banco emitiu um comunicado alertando sobre os avanços tecnológicos que oferecem vastas facilidades, frequentemente utilizadas por meio de softwares maliciosos.

Uma das estratégias dos golpistas, segundo o alerta do Banco, é simular situações em que se fazem passar por funcionários do banco, como gerentes de conta, utilizando argumentos convincentes para propor soluções que supostamente regularizariam problemas de segurança. O Banco também destaca sinais de tentativas de golpe, como ligações inesperadas, solicitações para instalação de softwares, pressões para agir rapidamente, mensagens com links suspeitos ou até mesmo pedidos de informações pessoais.

Para se proteger contra esses golpes, é recomendado evitar a instalação de softwares a

pedido de ligações inesperadas, sempre solicitar a identificação de quem está ligando, evitar clicar em links suspeitos e não baixar aplicativos de fontes não confiáveis. Caso se torne vítima de um golpe, a orientação é manter a calma, bloquear o número do golpista e excluir qualquer e-mail ou mensagem suspeita. Além disso, é fundamental alterar a senha de todas as contas, comunicar o Banco sobre o ocorrido e registrar um boletim de ocorrência.

Considerações finais

Nesse sentido, todo o arcabouço de informações construídos ao longo do texto, permite que caminhemos a uma conclusão lógica e esperada, ou seja, a evolução acelerada da tecnologia. Não é preciso ir além, para que seja verificado que, a cada dia, os sistemas da informação estão se desenvolvendo, adquirindo sempre uma nova roupagem, a qual leva a um crescimento exponencial da era digital, como bem preceituou Patrícia Peck Pinheiro.

Decorrente de tal fato, também se observa que as condutas delituosas, que a pouco menos de duas décadas estavam concentrada no mundo real, ou seja, nas relações interpessoais, de maneira física, exigindo-se o contato para a consumação de um delito, agora estão fervorosamente migrando para o plano digital. Assim, não se exige mais uma proximidade entre a vítima e o autor, haja vista que as redes sociais e os meios digitais romperam a barreira do contato físico. O fato é que, estando rompida a necessidade de proximidade, o crime digital torna-se um empecilho de difícil controle, vez que aqueles que praticam as condutas delituosas se escondem em mensagens criptografadas ou perfis falsos, os quais dificultam o reconhecimento do indivíduo. A tecnologia evoluiu exponencialmente, conforme nota-se no decorrer do texto.

Em contrapartida, o direito e o sistema normativo brasileiro não possuem a mesma frequência de evolução, tal como apresentou-se a tecnologia. Há um abismo considerável entre o atual estágio da tecnologia e o alcance das normas do direito brasileiro nas redes. Nesse "vale escuro" que se espreitam os criminosos, que utilizam de falhas nos sistemas, bem como do anonimato que as redes, em certa medida, proporcionam, para cometerem fraudes contra aqueles usuários mais vulneráveis.

Em vista disso, em que pese as investidas governamentais para uma tentativa de coibir os ataques digitais, nota-se que se trata de um esforço demasiadamente dispendioso, vez que não há uma eficácia considerável na redução dos crimes cometidos no ambiente virtual. Depreende-se que o atraso normativo é uma questão estrutural, bem como pré-determinada. Com isso, busca-se exprimir que a evolução digital, acompanhada das inovações nas condutas criminosas para aproveitar-se de tal meio, cresce em um nível tão acelerado, que se torna impensável ao direito penal prever todas as possíveis condutas ou espécies de fraudes que serão cometidas, ou criadas.

Além de tal ponto, há ainda a barreira técnica, ou seja, é necessário equipamentos desenvolvidos e equipes capacitadas para interceptar atividades fraudulentas nas redes, pois o maior problema enfrentado pelo sistema jurídico é, de fato, conhecer os autores dos delitos. Desse modo, as investigações policiais estagnam, pois não possuem ferramentas necessárias para chegarem aos autores das fraudes digitais.

Nesse diapasão, conclui-se que a fraude digital em geral e, em especial, aquela praticada por meio do *Phishing*, é um entrave difícil e trabalhoso para se contornar, tendo em vista que, como exposto, aqueles que praticam tal conduta, caminham por um vale complexo de localizá-los, vez que a problemática é extensa. Desse modo, em certa medida, notou-se que a expansão da tecnologia, de maneira imprevisível e exponencial, somada à criatividade e capacidade de adaptação daqueles que agem ao arrepio da lei, para se moldarem na mesma velocidade do crescimento tecnológico, com fito à pratica delituosa, dificultará cada vez mais a incidência das normas penais, as quais não conseguem a mesma desenvoltura para acompanhar a evolução.

É nesse cenário, que se observou a eficácia quase nula das regulamentações penais para dar uma resposta efetiva aos crimes cibernéticos. Em que pese à tímida tratativa das normas penais, no que tange à disposição de crimes digitais, ainda há uma distância bastante considerável entre o direito penal e a realidade virtual alcançada hodiernamente.

Referências

ANDRADE, B. **Crimes Cibernéticos: Como a Legislação Penal está se Adaptando à Nova Realidade Digital - Blog do Direito IDP**. Disponível em: <https://pos.idp.edu.br/idp-learning/direito-penal/crimes-ciberneticos-como-a-legislacao-penal-esta-se-adaptando-a-nova-realidade-digital/>. Acesso em: 15 set. 2025.

ANDRION, Roseli. **História da segurança virtual: A origem do cibercrime**. 2021. Disponível em:https://canaltech.com.br/seguranca/historia-da-seguranca-virtual-a-origem-docibercrime-203073/. Acesso em: 04 de out. de 2025.

BISPO, A. S.; BINTO, E.V.; **CRIMES CIBERNÉTICOS: DA INEFICÁCIA DA LEI CAROLINA DIECKMANN NA PRÁTICA DE CRIMES VIRTUAIS**. Revista Ibero-Americana de Humanidades, Ciências e Educação. São Paulo, v.9.n.11. nov.2023

BUCCI, C. et al. **Possibilidades de Uso de Honeytokens e Engenharia Social na Identificação de Crimes Cibernéticos Baseados em Phishing.** [s.l: s.n.]. Disponível em: . Acesso em: 9 out. 2025.

CASTRO, Carla Rodrigues Araújo de. **Crimes de informática e seus aspectos processuais**. 2.ed. Rio de Janeiro: Lumen Juris, 2003.

CUNHA, V.F.; CORTIZO, V.M.; **CRIMES CIBERNÉTICOS: Implicações Legais, eficácia das leis existentes e necessidade de adaptação do sistema legal a era digital**. Revista Acadêmica Online. V. 10 N 51 (2024): mai/jun, 2024.

DECRETO-LEI No 2.848, DE 7 DE DEZEMBRO DE 1940. Disponível em: . https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm. Acesso em 10 de setembro de 2025

DULLIUS, Aladio Anastácio. **Dos crimes praticados em ambientes virtuais.** 2012. Disponível em: https://conteudojuridico.com.br/consulta/artigos/30441/dos-crimes-praticados-em-ambientes-virtuais . Acesso em: 09 set. 2025.

DULLIUS, Aladio Anastácio. **Governo Federal lança Plano Tático de Combate a Crimes Cibernéticos**. Disponível em: <https://www.gov.br/pt-br/noticias/justica-e-seguranca/2022/03/governo-federal-lanca-plano-tatico-de-combate-a-crimes-ciberneticos>.

JOÃO, O.; CAMPOS, P.; ARAÚJO, D. PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS PRO-REITORIA DE GRADUAÇÃO ESCOLA DE DIREITO, NEGÓCIOS E COMUNICAÇÃO CURSO DE DIREITO NÚCLEO DE PRÁTICA JURÍDICA COORDENAÇÃO ADJUNTA DE TRABALHO DE CURSO ARTIGO CIENTÍFICO ANÁLISE DOS IMPACTOS DOS CRIMES CIBERNÉTICOS NA SOCIEDADE BRASILEIRA: DESAFIOS E PERSPECTIVAS DE COMBATE. [s.l: s.n.]. Disponível em: https://repositorio.pucgoias.edu.br/jspui/bitstream/123456789/7243/1/ARTIGO.%20JO%C3%83O%20PEDRO.pdf. Acesso em: 9 setembro de 2025.

JOÃO, O.; CAMPOS, P.; ARAÚJO, D. **Lei Carolina Dieckmann: 10 anos da lei que protege a privacidade dos brasileiros no ambiente virtual**. Disponível em: <https://www.defensoria.ce.def.br/noticia/lei-carolina-dieckmann-10-anos-da-lei-que-protege-a-privacidade-dos-brasileiros-no-ambiente-virtual/>. Acesso em 27 de setembro de 2025

LOBO, Ana Paula. **Proteção de dados é um direito fundamental do cidadão e cabe à União fiscalizar**. 2022. Disponível em: https://www.convergenciadigital.com.br/Governo/Protecaode-dados-e-um-direito-fundamental-do-cidadao-e-cabe-a-Uniao-fiscalizar-59416.html. Acesso em: 10 out. 2025.

MANDIANT. **Top Cyber Threats to Latin America and the Caribbean | Mandiant**. Disponível em: <https://cloud.google.com/blog/topics/threat-intelligence/top-cyber-threats-to-latin-america-and-the-caribbean/>. Acesso em: 15 set. 2025.

MARTINS, Antônio Eduardo Senna. **Direito Digital: desafios e implicações jurídicas na era digital**. 2023. Disponível em: https://www.jusbrasil.com.br/artigos/direito-digital-desafiose-implicacoes-juridicas-na-era-digital/1973368973. Acesso em: 09 out. 2025.

MONTEIRO, J; SILVA. D. **História da Internet**. 2009. REVISTA OWL (OWL JOURNAL) ISSN: 2965-2634 vol. 1, n. 2, Campina Grande, set. 2023.

Pinheiro, Patricia Peck. **Direito Digital**/Patricia Peck Pinheiro. - 7. ed. - São Paulo: Saraiva Educação. 2021.

PX. Empresa de tecnologia especialista em infraestrutura e segurança da informação. **O mapa dos ataques DDoS no Brasil**. Especialista em segurança cibernética, 2022. Disponível em: https://upx.com/post/mapa-ataques-ddos-brasil/. Acesso em 09 de out. de 2025.

SCHMIDT, Guilherme**. Crimes cibernéticos**. Jusbrasil, 2014. Disponível em: < http://gschmidtadv.jusbrasil.com.br/artigos/149726370/crimes-ciberneticos>. Acesso em: 09 out. 2025.

SILVA JÚNIOR, Reginald Vieira. **Os desafios do direito penal frente aos crimes cibernéticos. 2021**. Disponível em: https://www.nucleodoconhecimento.com.br/lei/crimesciberneticos. Acesso em: 09 de out. de 2024.

SILVA, Maria Laura Cordeiro. **A omissão legislativa na tipificação dos crimes cibernéticos e a sua intensificação com o aumento de usuários na internet em Goiá**s. FACULDADE EVANGÉLICA DE GOIANÉSIA CURSO DE DIREITO, Trabalho de Conclusão de Curso, 2021. Disponível em: http://repositorio.aee.edu.br/handle/aee/18053. Acesso em: 09 de out. de 2025.

SILVA, P. S. D. Direito e crime cibernético:análise da competência. Brasília: Vestnik, 2015.

TEIXEIRA, O.; SANTOS, D.; NUNES, N. **EVOLUÇÃO DOS CRIMES CIBERNÉTICOS NA PANDEMIA**. [s.l: s.n.]. Disponível em: https://repositorio.ufms.br/bitstream/123456789/6041/1/949.pdf. Acesso em 20 de setembro de 2025.

Recebido em 24 de outubro de 2025.
Aceito em 03 de dezembro de 2025.