DA CRIMINALIZAÇÃO DAS FRAUDES INFORMÁTICAS ANTES E DEPOIS DA ADESÃO DO BRASIL À *CONVENÇÃO DE BUDAPESTE SOBRE O CRIME CIBERNÉTICO*, UM BREVE ENSAIO DE BALANÇO CRÍTICO DESDE UMA PERSPECTIVA PORTUGUESA[1-2]

On the criminalization of computer-related frauds before and after the Accession of Brazil to the Budapest Convention on Cybercrime, a short essay of critical balance from a Portuguese perspective

Manuel David Masseno[3]

---

1 Por opção de princípio, há 3 anos, passei apenas a referir estudos que estejam em Acesso Aberto, ainda que apenas em repositórios; por outro lado, neste estudo, restringirei ainda mais o universo das referências a Autores portugueses, pois o objetivo principal do texto consiste em abrir novas veredas para as pesquisas dos Juristas brasileiros, deixando para um momento posterior o diálogo indispensável com a Doutrina brasileira, quando esta começar a se debruçar especificamente sobre a problemática, ainda que com um par de exceções. Porém, é indispensável ter presente que, em termos gerais, a Doutrina portuguesa na matéria em análise tem por referências fundamentais o disposto no *Código Penal*, de 15 de março de1995 <https://diariodarepublica.pt/dr/legislacao-consolidada/decreto-lei/1995-34437675> e na *Convenção do Conselho da Europa sobre o Cibercrime / Convenção* [do Conselho da Europa] *sobre o Crime Cibernético*, sobretudo desde quando esta foi aprovada e ratificada em simultâneo com a aprovação da nova *Lei do Cibercrime*, a Lei n.º 109/2009, de 15 de setembro <https://diariodarepublica.pt/dr/legislacao-consolidada/lei/2009-128879174>, o que requer uma especial prudência crítica no sentido de evitar transposições intersistemáticas apressadas. Adicionalmente, como a Fonte de referência é a *Convenção de Budapeste*, salvo na medida do estritamente necessário, não serão enfrentadas as questões resultante da Diretiva (UE) 2019/713 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, relativa ao combate à fraude e à contrafação de meios de pagamento que não em numerário e que substitui a Decisão-Quadro 2001/413/JAI do Conselho <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32019L0713>, sobre a qual, ainda que com a tónica na Lei n.º 79/2021, de 24 de novembro, que a transpôs para o Ordenamento português <https://diariodarepublica.pt/dr/detalhe/lei/79-2021-174824631>, temos o estudo de D.R. NUNES (2019b), assim como a minha muito recente intervenção, M.D. MASSENO (2025). Cumpre ainda acrescentar que, sendo o texto da minha inteira responsabilidade, em especial agradeço as leituras, assim como e sobretudo, os reparos de ordem técnico-jurídica dos Colegas Pedro Miguel Freitas, Pedro Dias Venâncio e Sylvia Chaves da Silva Ramos.

2 Este artigo é uma pré-publicação do texto destinado uma obra coletiva a propósito dos 30 anos da Internet Comercial no Brasil, com coordenação do Ministro do Superior Tribunal de Justiça Paulo Dias de Moura Ribeiro *et al*., em coerência com a opção de princípio enunciada na nota anterior.

3 Em Portugal, é Professor Adjunto e Encarregado da Proteção de Dados do Instituto Politécnico de Beja, onde também integra as Coordenações do Laboratório UbiNET – Segurança Informática e Cibercrime e do MESI – Mestrado em Engenharia de

RESUMO

Sendo uma das principais consequências da sua adesão tardia à *Convenção do Conselho da Europa sobre o Crime Cibernético*, (a *Convenção de Budapeste*, de 2001), em 2023, o Brasil está vinculado a adequar o Direito Penal Material anterior, não tendo sequer iniciado qualquer processo legislativo com o objetivo de cumprir essas obrigações internacionais. Sobretudo seguindo os métodos jurídicos comparativo e dogmático, este artigo está centrado nos objetivos e funções da "Fraude informática" no marco da *Convenção*, incluindo o cúmulo com outros crimes, como o "Acesso ilegal", a "Violação de dados" e a "Interferência em sistema". Seguidamente, a pesquisa avança com uma análise transversal de cada um dos crimes com, pelo menos, um objetivo similar no atual Direito brasileiro, também atendendo aos potenciais cúmulos. Terminando com algumas considerações sobre as soluções mais viáveis para superar as disparidades identificada.

Palavras-chave: Brasil. Convenção sobre o Crime Cibernético. Fraudes informáticas

ABSTRACT

As one of the main consequences of its late accession to the Convention of the Council of Europe on Cybercrime (the Budapest Convention, of 2001), in 2023, Brazil is meant to adequate the previous Substantive Criminal Law, not having even opened any legislative procedure in order to comply with those international obligations. Mostly following the Legal Comparative and Dogmatic Methods, the paper focuses on the scopes and role of "Computer-related fraud" within framework of the Convention, including the cumulation with other crimes, such as "Illegal access", "Data interference" and "System interference". Subsequently, the research proceeds with a transversal analysis of each of the crimes with an, at least, similar scope in the current Brazilian Law, also regarding the potential cumulations. Concluding with a few considerations on the most feasible solutions in order to address the identified disparities.

Keywords: *Brazil. Computer-related fraud. Convention on Cybercrime*

SUMÁRIO

Segurança Informática, sendo Investigador [*i.e.*, Pesquisador] Colaborador do CEGUAb – Centro de Estudos Globais da Universidade Aberta e Membro Convidado do CDPC – Centro de estudos e análise da privacidade e proteção de dados da Universidade Europeia, ambas de Lisboa. Desde há mais de uma década, leciona sobre matérias de Direito Penal da Informática no MESI do IPBeja, assim como no Mestrado em Direito e Informática da Escola de Direito da Universidade do Minho e, mais recentemente, também na Pós-Graduação em Direito e Tecnologia da Faculdade de Direito da Universidade Católica Portuguesa – Porto. Para contacto: <masseno@ipbeja.pt>.

1 UM PONTO DE PARTIDA, AS IMPLICAÇÕES DA ADESÃO DO BRASIL À *CONVENÇÃO DE BUDAPESTE* NO SEU DIREITO PENAL MATERIAL.

Recentemente, embora mais de duas décadas após a respectiva conclusão, **o Brasil aderiu à *Convenção do Conselho da Europa sobre o Crime Cibernético***, adotada em Budapeste, a 23 de novembro de 2001[4/5], comumente designada como *Convenção de Budapeste*, a qual continua sendo a referência mor no quadro do Direito Penal Internacional da Informática[6].

---

4 Sobre a *Convenção*, em termos gerais, embora sobretudo centrada nas suas previsíveis consequências para as Fontes legislativas portuguesas, dispomos das páginas introdutórias de P. VERDELHO (2003, *passim*), assim como e sobretudo as reflexões de F.P. CARVALHO, O. MORALES G. & M. ÁLVAREZ F. (2018, 48-54), além dos meus breves apontamentos atualizados, MASSENO (2023a).

5 O que ocorreu na sequência de um processo longo, formalmente desencadeado com a sinalização diplomática da sua disponibilidade para ser convidado a aderir à *Convenção*, em julho de 2019, com o convite a ser efetivado em dezembro de esse ano, embora a Presidência da República apenas tenha enviado para o Congresso a proposta de ratificação legislativa com a Mensagem nº 412, de 22 de julho de 2020, com a adesão a ser aprovada por meio do Decreto Legislativo nº 37, de 16 de dezembro de 2021, e a promulgação ocorrer através do Decreto nº 11.491, de 12 abril de 2023 <https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Decreto/D11491.htm>. Embora de no Decreto constar que "a República Federativa do Brasil firmou a Convenção sobre o Crime Cibernético, em Budapeste, em 23 de novembro de 2001", essa indicação apenas pode resultar de um *lapsus calami*, pois do texto resulta também que "Governo brasileiro [apenas] depositou, junto ao Secretário-Geral do Conselho da Europa, em 30 de novembro de 2022, o instrumento de ratificação à Convenção", não sendo um dos subscritores iniciais. Para um balanço do processo de Adesão à *Convenção* e das implicações para o Ordenamento Penal brasileiro, por todos, incluindo múltiplas referências, remeto para os estudos de C. M SOUZA & H. L. BARBOZA (2022) e I. D. CORRÊA & J.A. MONTEIRO Neto (2023), além dos meus breves apontamentos, M.D. MASSENO (2021b) e (2023c).

6 Embora, não possa ser omitido que, a respetiva Assembleia Geral aprovou, por aclamação, a 24 de dezembro de 2024, a *Convenção das Nações Unidas contra Crimes Cibernéticos - Fortalecimento da cooperação internacional para o combate a certos crimes cometidos por meio de sistemas de tecnologia da informação e comunicação e para o compartilhamento de provas eletrônicas de crimes graves*. Esta Convenção resultou de uma iniciativa da Federação Russa, a qual contou com o apoio da Bielorrússia, do Camboja, da Coreia do Norte, do Irã, de Myanmar, da Nicarágua e da Venezuela, além dos da China e da Índia, tendo a Assembleia Geral da ONU adotado a Resolução 73/187, de 17 de dezembro de 2018, relativa ao «combate à utilização das tecnologias da informação e da comunicação para fins criminosos», enquanto a 27 de dezembro de 2019, foi a vez

Como de esta Adesão resulta a necessidade de "adotar medidas legislativas e outras providências necessárias", adequando o correspondente Direito Penal Material[7], procurei estruturar algumas reflexões explicativas e críticas, sobretudo com o objetivo de contribuir para o debate que deve anteceder a criminalização de novas condutas ou a modificação do enquadramento das já antes penalizadas, tendo por referência a "Fraude informática" (Artigo 8.º da *Convenção*).

2 O TIPO "FRAUDE INFORMÁTICA" NA *CONVENÇÃO*

Para um melhor entendimento quanto ao âmbito da questão, atendendo ao explicitado na "Minuta do Relatório Explicativo" apensa à *Convenção*, a qual iremos acompanhando de perto, temos que a tipificação da "Fraude informática" foi concebida de modo a abranger um espectro muito amplo de práticas maliciosas contra o património, desde que no âmbito dos sistemas informáticos. Assim, textualmente:

> A revolução tecnológica veio multiplicar as possibilidades de cometer infracções de carácter económico, tais como as fraudes, das quais citamos as fraudes verificadas com os cartões de crédito. Os activos representados ou administrados por sistemas informáticos (fundos

da Resolução 74/247, a qual instituiu um comité de peritos intergovernamental aberto (o «Comité ad hoc») encarregado de elaborar uma convenção internacional, com o objetivo de ser alcançado um acordo até 2024. O que ocorreu no dia 8 de agosto, depois de debates muito acesos e participados devido aos potenciais riscos para os Direitos Humanos suscetíveis de resultarem da ênfase colocada na proteção da Soberania e dos interesses dos Estados, assim como das vicissitudes decorrentes da invasão da Ucrânia pela Federação Russa coincidindo com o início dos trabalhos e interrompendo-os por alguns meses. Por outro lado, embora os Estados Unidos da América e a União Europeia, incluindo os atuais Estados-membros e os candidatos à adesão, tenham levantado as objeções manifestadas durante os trabalhos, não se sabe se e quanto será depositado o quadragésimo instrumento de ratificação, entrando a *Convenção* em vigor para as Partes que o tenham feito. O texto da *Convenção*, nas línguas oficiais da ONU, incluindo informações preambulares sobre os correspondentes atos preparatórios, está disponível, neste endereço: https://docs.un.org/A/79/460.

7 Como, aliás, procurei mostrar, em termos gerais, na minha muito recente Aula Aberta para a WB Educação, M.D. MASSENO (2023c) e, mais especificamente, a propósito da qualificação criminal dos ataques de *ransomware*, M.D. MASSENO (2023d).

> eletrónicos, dinheiro de depósitos) tornam-se alvos de manipulações da mesma maneira que as tradicionais formas de propriedade. Estes crimes consistem principalmente na manipulação da entrada no sistema, em que são introduzidos dados incorretos, ou em manipulações em programas e outras interferências no tratamento de dados. [Consequentemente,] **O objetivo deste artigo é o de penalizar toda e qualquer manipulação indevida durante o tratamento de dados, cuja intenção seja a de efectuar uma transferência indevida de propriedade** [, *rectius* de património, sendo o negrito meu][8].

Portanto, pode ser tido por assente que o preceito foi pensado e redigido com uma grande abertura, de modo a abranger as novas realidades sociais e tecnológicas suscetíveis de alcançarem os resultados indesejados, embora sempre de natureza essencialmente patrimonial. O que permite também enquadrar ações pouco relevantes à época, sobretudo por razões de ordem tecnológica, incluindo os ataques de *ransomware*[9]. Consequentemente, na *Convenção* o tipo ficou previsto nos seguintes termos:

> Artigo 8 - **Fraude informática** [negrito meu]
>
> Cada Parte adotará medidas legislativas e outras providências necessárias para tipificar como crime, em sua legislação interna, a conduta de quem causar, de forma dolosa e não autorizada, prejuízo patrimonial a outrem por meio de:

---

[8] Como consta do Ponto 36 da *Minuta*, a qual está também acessível em língua portuguesa, embora seguindo a norma europeia anterior ao *Acordo Ortográfico* de 1990 <https://rm.coe.int/16802fa429>. Do mesmo modo e ainda mais claramente, estes objetivos constam do Ponto II.2.a do *Relatório* do Comité Europeu de Problemas Criminais do Conselho da Europa, apenso à *Recomendação n.º R (89) 9*, de 13 de setembro de 1989, a qual teve uma importância fundamental nos trabalhos preparatórios da *Convenção*, como é assumido tanto na *Minuta de qua* quanto no *Preâmbulo* da própria *Convenção*. A *Recomendação* está disponível em inglês, designadamente pela Organização dos Estados Americanos: https://www.oas.org/juridico/english/89-9&final%20Report.pdf.

[9] Como já defendemos, inclusive com alguma profundidade argumentativa, M.D. MASSENO (2023d). Sobre o *modus operandi* destas, M.D. MASSENO & E. WENDT (2017), assim como, mais extensamente, D.R. NUNES (2019a).

a. qualquer inserção, alteração, apagamento ou supressão de dados de computador;

b. qualquer interferência no funcionamento de um computador ou de um sistema de computadores, realizada com a intenção fraudulenta de obter, para si ou para outrem, vantagem econômica ilícita.[10]-[11]

---

[10] Esta redação segue, de perto, a constante do *Relatório* apenso à *Recomendação n.º R (89) 9*, de 13 de setembro de 1989, em cujos termos a "Computer related fraud" [aliás, a primeira das condutas a serem criminalizadas] consiste em: "The input, alteration, erasure or suppression of computer data or computer programs, or other interference with the course of data processing, that influences the result of data processing thereby causing economic or possessory loss of property of another person with the intent of procuring an unlawful economic gain for oneself or for another person (alternative draft: with the intent to unlawfully deprive that person of his property)". A *Recomendação* do Comité de Ministros, incluindo o *Relatório*, por esta recebido, estão disponíveis em inglês, designadamente pela Organização dos Estados Americanos: https://www.oas.org/juridico/english/89-9&final%20Report.pdf. Ainda a este propósito, é de sublinhar que o Brasil optou por se afastar da terminologia e da estrutura frásica das Versões já publicadas em língua portuguesa, designadamente, da "oficiosa" do próprio Conselho da Europa <https://rm.coe.int/16802fa428>, assim como das oficiais de Portugal, constante da Resolução da Assembleia da República n.º 88/2009, em 10 de Julho de 2009 <https://diariodarepublica.pt/dr/detalhe/resolucao-assembleia-republica/88-2009-489698>, e de Cabo Verde, conforme à Resolução [da Assembleia Nacional] n.º 116/VIII/2014, de 19 de novembro <https://kiosk.incv.cv/V/2014/11/19/1.1.70.1929/p2107>, tendo ido diretamente à versão oficial em inglês <https://rm.coe.int/1680081561>, embora sem a seguir exatamente, inclusive ao traduzir "*Convention on Cybercrime*" por "Convenção sobre o Crime Cibernético". Ora, esta "liberdade legística" poderá ter consequências, como veremos em seguida, as quais deverão ser evitadas aquando da aprovação da lei, ou leis, de adequação do Ordenamento penal brasileiro à Convenção, sobretudo tendo em vista o conteúdo e o alcance *Princípio da tipicidade penal*, previsto no inciso XXXIX do Artigo 5º da *Constituição Federal* de 1988. A este propósito, é de salientar que as versões oficiais da *Convenção*, em inglês e francês, assim como todas as oficiosas, podem ser consultadas na correspondente página do Conselho da Europa: https://www.coe.int/en/web/conventions/-/council-of-europe-convention-on-cybercrime-ets-no-185-translations.

[11] Efetivamente, esta conceptualização corresponde ao estado dos debates a propósito de estas questões, designadamente quanto à inserção do § 263a "Computerbetrug" [Fraude informática] no *Strafgesetzbuch* (StGB) [*Código Penal*, alemão] através da "Zweites Gesetz zur Bekämpfung der Wirtschaftskriminalität" [a Segunda Lei para Combater a Criminalidade Económica], de 15 de maio de 1986, a qual dispõe, quanto ao nosso objeto de estudo, que "1) Wer in der Absicht, sich oder einem Dritten einen rechtswidrigen Vermögensvorteil zu verschaffen, das Vermögen eines anderen dadurch beschädigt, daß er das Ergebnis eines Datenverarbeitungsvorgangs durch unrichtige Gestaltung des Programms, durch Verwendung unrichtiger oder unvollständiger Daten, durch unbefugte Verwendung von Daten oder sonst durch unbefugte

Aliás, é patente como o texto da *Convenção* contém uma noção muito ampla de "fraude", *rectius* de "objetivo fraudulento", a propósito dos dolos específicos facultativos dos tipos correspondentes ao "Acesso ilegal" (Artigo 2), à "Interceptação ilícita" (Artigo 3)[12] e à "Falsificação informá-

Einwirkung auf den Ablauf beeinflußt, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.". Por sua vez, a *Recomendação* esteve na base da *Primeira Geração* de Leis europeias sobre a matéria, como ocorreu em Itália com a inclusão do art. 640 ter "Frode informática" no *Codice Penale*, pela "Legge 23 dicembre 1993 n. 547", pela qual "Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalita' su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a se' o ad altri un ingiusto profitto con altrui danno, e' punito con la reclusione da sei mesi a tre anni e con la multa da lire centomila a due milioni.", em Espanha, com a previsão pela qual "También se consideran reos de estafa los que, con ánimo de lucro, y valiéndose de alguna manipulación informática o artificio semejante consigan la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero." (Artigo 248.2) do *Código Penal*, aprovado pela *Ley Orgánica 10/1995*, de 23 de novembro. Alguns meses antes, em Portugal, aproveitando a reforma profundada do *Código Penal*, operada pelo Decreto-Lei n.º 48/95, de 15 de março, ao inserir o Art.º 221.º "Burla informática", "1 - Quem, com intenção de obter para si ou para terceiro enriquecimento ilegítimo, causar a outra pessoa prejuízo patrimonial, interferindo no resultado de tratamento de dados ou mediante estruturação incorrecta de programa informático, utilização incorrecta ou incompleta de dados, utilização de dados sem autorização ou intervenção por qualquer outro modo não autorizada no processamento, é punido com pena de prisão até 3 anos ou com pena de multa.", cuja Comissão Revisora pretendeu seguir o antes referido modelo alemão, como resulta das respectivas *Actas*, embora em termos não propriamente felizes. A propósito da "Burla informática" no Direito português, ainda que uma desvalorização da *Convenção de Budapeste*, têm interesse as reflexões de C.G. PEDRA (2019, 15-19), assim como de C. RODRIGUES (2019, 44-45), D.S. PALMA (2019, 77-82 e 84-86) e de P.L.R. MOTA (2019, 171-173), assim como as minhas, aliás muito recentes, M.D. MASSENO (2025), as quais incluem também alusões uma evolução jurisprudencial no sentido de alargar a consideração às Fontes internacionais. Acrescente-se ainda a mesma estrutura foi seguida relativamente à "Fraude relacionada com sistemas de informação" na Diretiva (UE) 2019/713, de 17 de abril de 2019, relativa ao combate à fraude e à contrafação de meios de pagamento que não em numerário, conforme à qual "Os Estados-Membros devem tomar as medidas necessárias para assegurar que sejam puníveis como infrações penais os atos de transferir ou fazer transferir dinheiro, valor monetário ou moedas virtuais que causem desse modo um prejuízo patrimonial ilícito para outrem, a fim de obter benefícios ilícitos para si próprio ou para terceiro, quando esses atos sejam praticados com dolo através de: a) Obstrução ou interferência no funcionamento de um sistema de informação, sem direito a tal; b) Introdução, alteração, eliminação, transmissão ou supressão de dados informáticos, sem direito a tal." (Artigo 6.º), sobre esta, remeto para os desenvolvimentos transversais de D.R. NUNES (2019b) e também para as minhas referências breves, MASSENO (2025).

[12] "Cada Parte adotará medidas legislativas e outras providências necessárias para tipificar como crime em sua legislação interna a interceptação ilegal e intencional, realizada por meios técnicos, de transmissões não-públicas de dados de computador para um sistema informatizado, a partir dele ou dentro dele, inclusive das emissões

tica" (Artigo 7). Sendo a mesma, essencialmente, empregue para assinalar um desvalor relativo à intenção de alguém obter vantagens patrimoniais por meios ilícitos e dolosos.

a) Passando a uma análise da **configuração típica** da "Fraude informática", no que se refere ao seu **elemento objetivo**, estão presentes, enquanto **objetos** necessários e alternativos **da ação** ou os "dados de computador", a serem entendidos como "qualquer representação de fatos, informações ou conceitos numa forma adequada para o processamento num sistema de computador que inclua um programa capaz de fazer o sistema realizar uma tarefa;" (Artigo 1 b.); ou o "sistema de computador" [o qual] designa qualquer aparelho ou um conjunto de aparelhos interconectados ou relacionados entre si que asseguram, isoladamente ou em conjunto, pela execução de um programa, o processamento eletrônico de dados;" (Artigo 1 a.).

Para tanto e seguindo sempre o enunciado na *Convenção*, é necessário entender que, nesta, o "programa" ficou abrangido pela noção de "dados de computador". Ao passo que, por "aparelho" deve ser considerado não apenas um esquipamento físico (*hardware*), mas também os programas de computador que permitem o seu funcionamento (*software*), como resulta explicitamente do texto, a propósito da criminalização específica dos atos preparatórios, ao incluir o "programa de computador" na noção de "aparelho" (Artigo 6º parágrafo 1, letra a i))[13]-[14].

---

eletromagnéticas oriundas de um sistema informatizado que contenham esses dados de computador. Qualquer Parte pode exigir para a tipificação do crime o seu cometimento com **objetivo fraudulento** ou que seja praticado contra um sistema de computador que esteja conectado a outro sistema de computador."

[13] Neste ponto, é indispensável ter ainda em atenção que, como resulta explicitamente do Ponto 22 da *Minuta*, "Foi considerado pelos autores do projeto que, ao abrigo da presente Convenção, as Partes não ficariam obrigadas a copiar textualmente, para as suas legislações nacionais, os quatro conceitos definidos no Artigo 1º, desde que tais conceitos se encontrem abrangidos nas referidas legislações de uma forma coerente com os princípios da *Convenção* e proporcionem uma estrutura equivalente para a sua implementação.". Ora, no Ponto 22, a propósito do "sistema de computador" consta que este "é um equipamento composto por *hardware* e *software* desenvolvidos para o tratamento automático de dados digitais [enquanto] a expressão "tratamento de dados" significa que os dados no sistema informático são operados através da execução de um programa de computador.".

[14] O que, *obiter dictum*, permite também melhor entender o objeto da ação prevista e punida no crime de "Invasão de dispositivo informático", tal como costa do *caput*

Por sua vez, no que se refere à caracterização do **conteúdo** da **ação típica**, são dois os elementos de natureza objetiva, em alternativa e de forma relativamente vinculada. Os quais consistem em "qualquer inserção, alteração, apagamento ou supressão de dados de computador" ou em "qualquer interferência no funcionamento de um computador ou de um sistema de computadores", incluindo o próprio *hardware*.

O que obriga, preliminarmente, à análise de dois outros tipos previstos na *Convenção*, a "Violação de dados" (Artigo 4º) e a "Interferência em sistema" (Artigo 5º), cujos objetos e conteúdos das respectivas ações coincidem com os da "Fraude informática"[15].

Assim, no que se refere à "Violação de dados"[16], resulta que:

> 1. Cada Parte adotará medidas legislativas e outras providências necessárias para tipificar como crimes, em sua legislação interna, a danificação, a eliminação, a deterioração, a alteração ou a supressão dolosas e não autorizadas de dados de computador.
>
> 2. Qualquer Parte pode reservar-se o direito de exigir que da conduta descrita no parágrafo 1 resulte sério dano para a vítima.

Sendo que, a este preciso propósito, a própria *Minuta* esclarece ainda:

---

do Art. 154-A do *Código Penal* brasileiro, [introduzido pela Lei nº 12.737, de 30 de novembro de 2012, a qual "dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências" (a, dita, *Lei Carolina Dieckmann*)], isto é, o mesmo não se restringe a dispositivos físicos em si mesmo considerados, isto é, ao *hardware*, podendo incluir os virtuais, sempre que diferenciados, como procurei mostrar, em diálogo com a Doutrina brasileira, em M.D. MASSENO (2018).

15 Como sublinhou e analisou, inclusive detalhadamente, P.D. VENÂNCIO (2013).

16 Manifestamente, esta terminologia não é feliz por coincidir com a usualmente usada, também no Brasil, para referir os incidentes de segurança conduzindo a violações de segurança de dados pessoais, os "vazamentos de dados", conforme ao Artigo 48 da Lei n. 13.709, de 14 de agosto de 2018, a *Lei Geral de Proteção de Dados Pessoais*, sobre estas questões, por todos, *vide* M.D. MASSENO, G.M. MARTINS & J.L. FALEIROS Jr. (2020). Aliás, neste caso, a versão brasileira não apenas se afasta da "oficiosa", a qual prefere a designação "Interferência nos dados", como da portuguesa e cabo-verdiana, "Dano provocado nos dados", sendo esta também objeto de críticas ao indiciar um mimetismo excessivo com o crime de "Dano", como também das oficiais "Data interference" e "Atteinte à l'intégrité des données".

> A introdução de códigos dolosos, tais como vírus e rotinas tais como os chamados "cavalos de Tróia", encontra-se pois abrangida por este parágrafo da mesma maneira que a modificação dos dados resultante deste acto. (Ponto 61)[17]

Por sua vez, no que se refere à "Interferência em sistemas", resulta que:

> Cada Parte adotará medidas legislativas semelhantes e outras providências necessárias para tipificar como crime, em sua legislação interna, qualquer grave obstrução ou impedimento, dolosos e não autorizados, do funcionamento de um sistema de computador por meio da inserção, transmissão, danificação, apagamento, deterioração, alteração ou supressão de dados de computador.

Assim, sempre seguindo a *Minuta*, se na "Violação de dados" "[…] os interesses jurídicos protegidos são a integridade e o adequado funcionamento ou a correcta utilização dos dados ou programas informáticos armazenados." (Ponto 60); na "Interferência em sistemas", o mesmo "reside no interesse de operadores e utilizadores de sistemas informáticos e de telecomunicações em que os mesmos apresentem um funcionamento adequado." (Ponto 65).

Nestas bases, embora a consumação de cada um de estes crimes seja suscetível de afetar o património das vítimas, o mesmo não surge em primeira linha. Aliás, sobretudo no que se refere à "Interferência em sistemas", poderão estar em causa interesses sociais gerais, muito para além dos enunciados na *Minuta*. Sendo certo estarmos perante dois crimes de resultado e de dano, pois a sua consumação pressupõe a lesão do bem jurídico tutelado.

---

[17] O que, no Direito brasileiro vigente, apenas ocorre, pelo menos explicitamente, no contexto da "Invasão de dispositivo informático", ao ser também criminalizada a ação de "instalar vulnerabilidades para obter vantagem ilícita", embora apenas para caraterizar um dolo específico, na parte final do *caput* do preceito, tal como resultou da Lei nº 14.155, de 27 de maio de 2021, a ser analisada mais à frente; assim como, da forma qualificada consistente no "controle remoto não autorizado do dispositivo invadido", prevista no § 3º, também *in fine*, do mesmo enunciado legislativo.

Do mesmo modo, no respeitante ao elemento subjetivo de ambos os tipos, não é exigida qualquer intenção de natureza patrimonial, quer em prejuízo da vítima, quer em proveito próprio ou de terceiro.

Porém, o acréscimo da dimensão patrimonial aponta para estarmos perante um concurso apenas aparente, com a "Fraude informática" a consumir a "Violação de dados" ou a "Interferência em sistema". O que ainda será mais claro relativamente a outras condutas enquadráveis na previsão típica, como as transferências bancárias ilícitas[18].

Em contrapartida, teremos um concurso material quando os efeitos ultrapassarem o poder de disposição patrimonial da vítima. Como ocorre no caso de ataques de *ransomware* afetando infraestruturas críticas ou serviços de interesse social[19].

Cumpre ainda acrescentar que a consumpção não se deve considerar como implicando excluir a criminalização dos atos preparatórios relativos ao "Uso indevido de aparelhagem" (Artigo 6.º) na "Fraude informática", como resultaria de uma leitura apressada do preceito[20]:

---

18 Sobre o *modus operandi* de estas, C.F. BARREIRA (2015), embora desde uma perspectiva diferente da aqui seguida.

19 Como defendi, na perspetiva da própria *Convenção*, M.D. MASSENO (2023d), e também já concluíra, para os Direitos português e brasileiro, em M.D. MASSENO & E. WENDT (2017), o mesmo sendo defendido por D.R. NUNES (2019a), este apenas para o Ordenamento português. Aliás, assim ocorre com as formas qualificadas previstas no *Código Penal* português, para a "Sabotagem informática" se "A perturbação causada atingir de forma grave ou duradoura um sistema informático que apoie uma actividade destinada a assegurar funções sociais críticas, nomeadamente as cadeias de abastecimento, a saúde, a segurança e o bem-estar económico das pessoas, ou o funcionamento regular dos serviços públicos." (Artigo 5.º n.º 5 a)) ou na Diretiva 2013/40/UE, relativa a ataques contra os sistemas de informação, sempre que a "Interferência ilegal no sistema" (Artigo 4.º) (Artigo 5.º), sempre as infrações "Sejam cometidas contra um sistema de informação que constitua uma infraestrutura crítica." (Artigo 9.º n.º 4 c))

20 E também resulta, explicitamente, do previsto no Artigo 7.º ("Instrumentos utilizados para cometer infrações") da Diretiva (UE) 2019/713, conforme al qual, "Os Estados-Membros devem tomar as medidas necessárias para assegurar que sejam puníveis como infrações penais a produção, a aquisição para si próprio ou para terceiro, incluindo a importação, a exportação, a venda, o transporte, a distribuição ou a disponibilização de um dispositivo ou de um instrumento, de dados informáticos ou de outros meios principalmente concebidos ou especificamente adaptados para cometer uma das infrações previstas no artigo 4.o, alíneas a) e b), no artigo 5.º ["Infrações relacionadas

1. . Cada Parte adotará medidas legislativas e outras providências necessárias para tipificar como crimes, em sua legislação interna, as seguintes condutas, quando dolosas e não autorizadas:

a. a produção, venda, aquisição para uso, importação, distribuição ou a disponibilização por qualquer meio de: i. aparelho, incluindo um programa de computador, desenvolvido ou adaptado principalmente para o cometimento de quaisquer dos crimes estabelecidos de acordo com os artigos de 2 a 5; ii. uma senha de computador, código de acesso, ou dados similares por meio dos quais se possa acessar um sistema de computador ou qualquer parte dele, com a intenção de usá-lo para a prática de quaisquer dos crimes previstos nos artigos de 2 a 5; e b. a posse de qualquer dos instrumentos referidos nos parágrafos a.i ou ii, com a intenção de usá-los para a prática de quaisquer dos crimes previstos nos artigos de 2 a 5. Qualquer Parte pode exigir, por lei, a posse de um número mínimo de tais instrumentos, para que a responsabilidade criminal se materialize.

2. Este Artigo não deve ser interpretado para estabelecer responsabilidade criminal quando a produção, venda, aquisição para uso, importação, distribuição ou disponibilização por qualquer meio ou a posse referidos no parágrafo 1 deste Artigo não se destine à prática de qualquer dos crimes tipificados de acordo com os artigos 2 a 5 desta Convenção, como para, por exemplo, a realização de testes autorizados ou a proteção de um sistema de computador.

3. Cada Parte pode reservar-se o direito de não aplicar o parágrafo 1 deste Artigo, desde que a reserva não se refira à venda, distribuição ou a disponibilização por qualquer meio, dos itens ou instrumentos referidos no parágrafo 1 a.ii deste Artigo.

---

com a utilização fraudulenta de instrumentos de pagamento não corpóreos que não em numerário"] , alíneas a) e b), **ou no artigo 6.º** ["**Fraude relacionada com sistemas de informação**"], pelo menos quando esses atos forem praticados com a intenção de que esses meios sejam utilizados.". O que o Legislador português não cumpriu, no que se refere ao segundo preceito, ao transpor a Diretiva através da Lei n.º 79/2021, de 24 de novembro, mesmo tendo alterado a redação do Artigo 221.º n.º 1 ("Burla informática e nas comunicações") do *Código Penal*, o que terá também escapado a D.R. NUNES (2022, 19-23), apesar de este se ter detido na análise do conteúdo e do alcance desta criminalização autónoma de atos preparatórios.

Adicionalmente, poderá também caber um concurso material com o crime de "Acesso ilegal" (Artigo 2), em cujos termos,

> Cada Parte adotará medidas legislativas e outras providências necessárias para tipificar como crime, em sua legislação interna, o acesso doloso e não autorizado à totalidade de um sistema de computador ou a parte dele. Qualquer Parte pode exigir para a tipificação do crime o seu cometimento mediante a violação de medidas de segurança; com o fim de obter dados de computador ou com outro objetivo fraudulento; ou contra um sistema de computador que esteja conectado a outro sistema de computador. [21]

Neste caso, quanto ao bem jurídico protegido, ainda segundo a *Minuta*, está em causa "A necessidade de protecção reflecte os interesses de organizações e indivíduos em gerir, operar e controlar os seus sistemas de forma livre e tranquila." (Ponto 44)

Por outras palavras, é essencialmente procurada a segurança dos sistemas de computadores, de modo a manter a confiança dos particulares e das empresas, assim como a dos mercados e da sociedade em geral, nas respectivas segurança, confidencialidade e integridade, incluindo os dados presentes nos mesmos. Além de antecipar ou até complementar a tutela, quando não é viável imputar probatoriamente as ações previstas na "Fraude informática" nos casos concretos.

Em extrema síntese, o "Acesso ilegal" será um crime de perigo abstrato, não relevando qualquer dano ou dolo específico, designadamente de índole patrimonial.

---

[21] A propósito deste tipo, analisando as mudanças a resultarem da Convenção para *a Lei da Criminalidade Informática* então vigente em Portugal, a Lei n.º 109/91, de 17 de agosto <https://diariodarepublica.pt/dr/detalhe/lei/109-1991-674438>, têm muito interesse as considerações de R. BRAVO (2003), enquanto eu me ocupei da respectiva comparação com o previsto na Diretiva 2013/40/UE, do Parlamento Europeu e do Conselho, de 12 de agosto de 2013, relativa *a ataques contra os sistemas de informação* e que substitui a Decisão-Quadro 2005/222/JAI do Conselho <https://eur-lex.europa.eu/eli/dir/2013/40/oj?locale=pt> e com a *Lei Carolina Dieckmann*, M.D. MASSENO (2018); sobretudo para o enquadramento das Fontes anteriormente aplicáveis em Portugal, ainda têm interesse as considerações gerais de P.S. DIAS (2006).

Consequentemente, tratar-se-á de um concurso real se o acesso for obtido diretamente por meios técnicos diretos (*Hacking*), sendo ideal sempre que a "Fraude" se processe através de uma "injeção" de código malicioso, assim como nos casos de a "inserção, alteração, apagamento ou supressão de dados de computador" ou a "interferência no funcionamento de um computador ou de um sistema de computador" ser operada por quem estiver autorizado a aceder ao sistema, mas não a operar as referidas ações, com os efeitos e as finalidades de natureza patrimonial previstas pela *fattispecie*. O mesmo valendo para as condutas dirigidas à produção de mensagens falsas, criadas com o objetivo de induzirem as vítimas a ativarem programas, a facultarem os correspondentes códigos de acesso aos sistemas informáticos, como ocorre com o *Phishing* ou com o *Pharming*, ou ainda a procederem elas próprias a tais inserções de dados.

Ainda a propósito de concursos[22], será viável um concurso material com a "Falsificação informática" (Artigo 7), com a qual coincidem também os objetos e os conteúdos das ações, embora restritamente aos dados, nos seguintes termos:

> Cada Parte adotará medidas legislativas e outras providências necessárias para tipificar como crimes, em sua legislação interna, a inserção, alteração, apagamento ou supressão, dolosos e não autorizados, de dados de computador, de que resultem dados inautênticos, com o fim de que sejam tidos como legais, ou tenham esse efeito, como se autênticos fossem, independentemente de os dados serem ou não diretamente legíveis e inteligíveis. Qualquer Parte pode exigir, para a tipificação do crime, o seu cometimento com intenção de defraudar ou com outro objetivo fraudulento.[23]

---

[22] Sobre estas questões, tem um particular interesse o estudo, no contexto da *Convenção de Budapeste*, de P.D. VENÂNCIO (2013, 99-105), assim como, no âmbito do Direito português, embora desde perspetivas várias, mas quase sempre tendo por referência subjacente a *Convenção*, de D.R. NUNES (2017, 41-48), assim como os contributos sintéticos, tendo por referência o crime de "Burla informática", de C.G. PEDRA (2019, 25-29), de C. RODRIGUES (2019, 54-60), de D.S. PALMA (2019, 86-89), de P.L.R. MOTA (2019, 178-180) e, ainda, de D.R. NUNES (2019b, 28-29 e 34).

[23] Sobre a configuração de este tipo, também com referências à *Convenção*, embora essencialmente centrado nas Fontes portuguesas, é de indicar o estudo de D.R. NUNES (2017).

Porém, diferem quanto a não terem de ser dados alheios e o resultado consistir na obtenção de "dados inautênticos, com o fim de que sejam tidos como legais, ou tenham esse efeito, como se autênticos fossem". O que configura um crime de perigo, ao não ser exigida a efetivação do dano.

Adicionalmente, a *Minuta* assume que, "Neste caso, o interesse jurídico protegido será o da segurança e da credibilidade dos dados eletrónicos que poderão ter consequências ao nível das relações jurídicas." (Ponto 81, *in fine*).

> O que extravasa também o âmbito patrimonial, alcançando o interesse geral relativo à segurança jurídica e a fiabilidade das transações eletrónicas, mesmo sem incidência económica.

Em síntese, a "Fraude informática" configura-se como um crime de dano, a ser consumado com o prejuízo patrimonial efetivo da vítima, para tal não bastando à "inserção, alteração, apagamento ou supressão de dados de computador" ou a "interferência no funcionamento de um computador ou de um sistema de computadores". Embora destas ações, em si mesmo consideradas, possam também resultar danos de natureza patrimonial. Ainda a este propósito, cabe acentuar que a "vantagem económica ilícita" integra apenas o elemento subjetivo do tipo, a ser abordado em seguida.

b) passando ao **elemento subjetivo do tipo**, resulta ser exigido um dolo genérico correspondente a "causar, de forma dolosa e não autorizada, prejuízo patrimonial a outrem"; ao qual acresce o específico que subjaz à "intenção fraudulenta de obter, para si ou para outrem, vantagem económica ilícita".

Ainda no que se refere ao alcance do dolo específico indicado, apesar de uma interpretação apenas enunciativa do texto publicado no *Diário Oficial da União* apontar para o inverso, é indispensável acrescentar que o mesmo releva para as duas condutas típicas e não apenas em caso de "interferência no funcionamento de um computador ou de um sistema de computadores". Como nos mostra uma leitura comparativa entre as

versões oficiais e vinculantes, em inglês[24] e em francês[25], assim como as outras versões em língua portuguesa, a "oficiosa" do próprio Conselho da Europa[26] e as correspondentes às aprovações para ratificação de Portugal e de Cabo Verde[27], as quais coincidem, *verbatim*.

d) Por último, quanto ao **bem jurídico penalmente protegido**, a própria redação do preceito aponta, de um modo inequívoco, para o património da vítima. Aliás, no mesmo sentido, como antecipado, da *Minuta* consta, explicitamente, que o "objetivo deste artigo é o de penalizar toda e qualquer manipulação indevida durante o tratamento de dados, cuja intenção seja a de efectuar uma transferência indevida de propriedade." (Ponto 36).

O que deverá ser entendido para além de uma consideração estática dos bens em propriedade, incluindo também todas as situações jurídicas de natureza patrimonial. Sobretudo, porque nunca devemos esque-

---

[24] "Article 8 – **Computer-related fraud**
Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:
a any input, alteration, deletion or suppression of computer data, b any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person".

[25] "Article 8 – **Fraude informatique**
Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait intentionnel et sans droit de causer un préjudice patrimonial à autrui:
a par toute introduction, altération, effacement ou suppression de données informatiques; b par toute forme d'atteinte au fonctionnement d'un système informatique, dans l'intention, frauduleuse ou délictueuse, d'obtenir sans droit un bénéfice économique pour soi-même ou pour autrui.".

[26] "Artigo 8º – **Burla informática**
Cada Parte adoptará as medidas legislativas e outras que se revelem necessária para estabelecer como infracção penal, em conformidade com o seu direito interno, o acto intencional e ilegítimo, que origine a perda de bens a terceiros através:
a) Da introdução, da alteração, da eliminação ou da supressão de dados informáticos;
b) De qualquer intervenção no funcionamento de um sistema informático, com a intenção de obter um benefício económico ilegítimo para si ou para terceiros.".

[27] "Artigo 8.º – **Burla informática**
Cada Parte deverá adoptar as medidas legislativas e outras que se revelem necessárias para classificar como infracção penal nos termos do seu direito interno, quando praticado intencional e ilicitamente, o prejuízo patrimonial causado a outra pessoa por meio de:
a) Qualquer introdução, alteração, apagamento ou supressão de dados informáticos;
b) Qualquer interferência no funcionamento de um sistema informático;
com intenção de obter para si ou para outra pessoa um benefício económico ilegítimo."

cer que os poderes de livre disposição não se confundem com os direitos sobre bens patrimoniais concretos e podem ser determinados por efeito do *dolus* ou do *metus*, para usar as caracterizações romanísticas em sede de *delicta*. O que possibilita até um enquadramento nuclear da "Fraude informática" perante ações complexas como as articuladas nos ataques de *ransomware*, tendo por referência os tipos constantes da *Convenção de Budapeste*. Considerações estas que serão também relevantes para a análise dos presentes tipos penais brasileiros.

Consequentemente, a confiança dos operadores económicos dos mercados na integridade e fiabilidade nos sistemas e redes de computadores é também protegida, ainda que reflexamente.

Por outro lado, a referência a uma ação "não autorizada", pelo próprio titular do sistema ou pela lei, incluindo quem tivesse autorizado acesso ao sistema, embora não para a prática de tais ações, resultando na manipulação dos dados ou do sistema, obriga a considerar o controlo exclusivo destes também no âmbito dos bens jurídicos protegidos pelo crime de "Fraude informática".

Cabe ainda acrescentar que a tentativa, iniciada com o começo das ações mencionadas na previsão típica, será tendencialmente punível[28]. O mesmo não ocorrendo com os atos preparatórios[29], salvo nos casos de concurso material com o "Acesso ilegal", como antes exposto.

3 SEGUIDO POR UM ENSAIO DE ANÁLISE CONTRASTATIVA DOS ATUAIS TIPOS PENAIS BRASILEIROS

Desde a caraterização do tipo *de quo* na *Convenção*, cumpre passar a uma análise sistemática, ainda que apenas de natureza apenas topográ-

---

[28] Nos termos do previsto no Artigo 11 parágrafo 2, embora as Partes possam reservar-se o direito de não o fazer, conforme a parágrafo 3.

[29] Pois o crime correspondente ao "Uso indevido de aparelhagem" (Artigo 6) apenas prevê a obrigatoriedade para as Partes no que se refere aos tipos "Crimes contra a confidencialidade, integridade e disponibilidade de dados e sistemas de computador" e não aos "Crimes informáticos", como ocorre com a "Fraude informática" ou a "Falsificação informática", o mesmo valendo para os "Crimes relacionados ao conteúdo da informação" ou a "Violação de direitos autorais e de direitos correlatos".

fica, das Fontes legislativas brasileiras vigentes[30]. Embora, sem sequer intentar uma sua reconstrução dogmática, o que seria em absoluto despropositado nesta sede.

Para a concretizar, por um lado, serão tidos como coordenadas essenciais os elementos objetivos que integram a sua *fattispecie*, isto é, os "dados de computador" ou o "sistema de computador" enquanto objetos da ação; assim como, pelo outro, as ações típicas consistentes em "qualquer inserção, alteração, apagamento ou supressão de dados de computador" ou "qualquer interferência no funcionamento de um computador ou de um sistema de computadores". Às quais, necessariamente, acresce a consideração do património enquanto bem jurídico penalmente protegido, mesmo se não exclusivamente.

a) Assim, desde as referências antes enunciadas, será de excluir o crime de "Invasão de dispositivo" (Artigo 154-A do *Código Penal*, por várias vezes mencionado), ainda que esta incida sobre um "dispositivo informático". Para o que basta atentar que, na correspondente previsão, o "adulterar ou destruir dados ou informações" não integra o elemento objetivo do tipo, mas antes um dos dolos específicos, em alternativa ao consistente em "obter […] dados ou informações", sendo este um crime de mera conduta que se consuma com o acesso a dispositivo informático de uso alheio […] sem autorização expressa ou tácita do usuário". (*Caput*). Ao passo que o "prejuízo econômico" constitui apenas um fator de qualificação, elevando a moldura da pena "de um sexto a um terço" (§ 2º)[31].

O que não exclui a viabilidade de a "Invasão" poder concorrer, em termos efetivos, com as condutas previstas noutros tipos criminais, sobretudo quando as respectivas ações não exigem o acesso por via técnica aos dados presentes num sistema para se consumarem, sendo de recordar o escrito a propósito do "Acesso ilegal" na *Convenção*.

---

[30] O que já intentei reiteradamente, desde há mais de uma década, essencialmente para fins ilustrativos ou didáticos, sendo esta a última das quais M.D. MASSENO (2023c).

[31] Como procurei mostrar, antes da Lei nº 14.155, de 27 de maio de 2021, a qual será abordada em seguida no referente a outras novidades, embora a nova redação do preceito não infirme o então defendido, M.D. MASSENO (2018).

b) Pelo menos *prima facie*, será distinta a situação do crime relativo à "Inserção de dados falsos em sistema de informações" (Artigo 313-A do *Código Penal*), ao ser prevista e punida a conduta consistente em:

> Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano.

Inserida no *Código Penal* brasileiro pela Lei nº 9.983, de 14 de julho de 2000, nesta previsão estão presentes quer os elementos objetivos da "Fraude informática", quanto ao objeto, os "sistemas informatizados ou bancos de dados", e à ação de "Inserir ou facilitar [...] a inserção de dados falsos, alterar ou excluir indevidamente dados corretos"; quer relativamente ao próprio dolo específico, consistente no "fim de obter vantagem indevida para si ou para outrem ou para causar dano".

Porém, como mostra a própria colocação sistemática do preceito no Capítulo I "Dos Crimes Praticados por Funcionário Público Contra a Administração em Geral" do Título XI "Dos Crimes Contra a Administração Pública" do *Código*, estamos perante um crime próprio, pressupondo a qualidade de "funcionário" por parte do agente, isto é, de

> [...] quem, embora transitoriamente ou sem remuneração, exerce cargo, emprego ou função pública [e].
>
> § 1º - Equipara-se a funcionário público quem exerce cargo, emprego ou função em entidade paraestatal, e quem trabalha para empresa prestadora de serviço contratada ou conveniada para a execução de atividade típica da Administração Pública. (Artigo 327)

Ao que acresce a exigência de ser um "funcionário autorizado", não apenas no que se refere ao acesso aos "sistemas informatizados ou bancos de dados da Administração Pública", mas também quanto às próprias inserção, alteração ou exclusão de dados. O que afasta o concurso com a "Invasão de dispositivo", quando este pressupõe a ausência de "autoriza-

ção expressa ou tácita do titular do dispositivo", embora já não se a ação consistir no ato de "instalar vulnerabilidades" e com o dolo específico de "obter vantagem ilícita" (*Caput* do Artigo 154-A, *in fine*).

Distinguindo-se também da "Fraude informática" por se tratar de um crime formal, ou de mera conduta, consumando-se mesmo que não se verifiquem os efeitos alternativos desta, e "vantagem a indevida para si ou para outrem" ou o "dano", este afetando em particular a Administração Pública, ainda que a previsão não exclua terceiros.

Por outro lado, não é exigido que a "vantagem indevida" ou o "dano" tenham natureza apenas patrimonial, embora também não a excluindo[32]. O que, porém, afasta a pertinência da designação corrente deste tipo com "peculato eletrônico", por suceder imediatamente ao "Peculato" (Artigo 312); a que acresce não ter o Legislador brasileiro colocado a "Inserção de dados falsos em sistema de informações" no âmbito deste, nomeadamente após o "Peculato culposo" e o "Peculato mediante erro de outrem"[33].

A que se segue a ação relativa à "Modificação ou alteração não autorizada de sistema de informações" (Artigo 313-B do mesmo *Código*), concretizando-se em

---

[32] Como, aliás, ocorre em França; onde, com a *Loi no 88-19 du 5 janvier 1988 relative à la fraude informatique*, conhecida como "loi Godfrain", é bastante "Le fait d'introduire frauduleusement des données dans un système de traitement automatisé, d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données", protegendo criminalmente outros bens jurídicos para além do património da vítima, enquanto crime comum (Artigo 323-3 do *Code Pénale*).

[33] Embora, sobre esta questão, o Superior Tribunal de Justiça tenha decidido, em sentido contrário, que "1. O delito de inserção de dados falsos em sistema de informações, descrito no artigo 313-A do Código Penal, é especial ao crime de peculato delineado no artigo 312 do Estatuto Repressor. 2. Na hipótese, a vantagem indevida auferida em detrimento da administração pública (objeto de tutela do crime de peculato) foi alcançada por meio de um especial modo de agir, consistente na inserção de informações falsas nos sistemas informatizados ou banco de dados da municipalidade. 3. Tal circunstância evidencia a ocorrência de apenas uma lesão ao bem jurídico tutelado, sendo imperioso, diante do concurso aparente de normas penais aplicáveis, o afastamento da condenação referente ao crime de peculato-desvio, já que o delito descrito no artigo 313-A do Código Penal disciplina, na íntegra, os fatos praticados pelo paciente, remediando-se, por conseguinte, o *bis in idem* repudiado pelo ordenamento jurídico pátrio." (HC 213.179/SC, Rel. Min. Jorge Mussi, Quinta Seção, de 19/04/2012, publicado no DJ de 03/05/2012).

> Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente.
>
> Parágrafo único. As penas são aumentadas de um terço até a metade se da modificação ou alteração resulta dano para a Administração Pública ou para o administrado.

Neste caso, resulta ser o objeto constituído por "sistema de informações ou programa de informática" e a ação consistir em o "Modificar ou alterar […] sem autorização ou solicitação de autoridade competente". Sendo também um crime próprio, inclusive puro, apenas suscetível de ser praticado por um funcionário com competência própria ou atribuída para o fazer, ainda que não tendo de ser "autorizado", como na "Inserção de dados falsos". Sendo também um crime formal, com a efetividade do "dano para a Administração Pública ou para o administrado" a apenas relevar como agravante.

Por conseguinte, em ambos os tipos, o bem jurídico protegido em termos diretos é o controle exclusivo dos "sistemas informatizados ou bancos de dados" ou de "sistema de informações ou programa de informática" pela Administração Pública; enquanto a dimensão patrimonial recairá apenas no "dano", se este ocorrer[34], sem relevar a apropriação de quaisquer bens para o agente ou para um terceiro, essencial na "Fraude informática" , mesmo se na "Inserção", embora deva estar presente o dolo específico relativo ao "fim de obter vantagem indevida", esta nem tem porque ser de natureza patrimonial[35].

---

[34] Sendo este tipo, em parte, especial relativamente ao de dano "contra o patrimônio da União, de Estado, do Distrito Federal, de Município ou de autarquia, fundação pública, empresa pública, sociedade de economia mista ou empresa concessionária de serviços públicos" (Artigo 163 parágrafo único III).

[35] Ainda este propósito, como exemplo negativo, com toda probabilidade resultando de uma utilização acrítica de um sistema de Inteligência Artificial Generativa, encontrei na Internet a seguinte "transcrição" do preceito analisado "Art. 313-B. Inserir ou difundir código malicioso em dispositivo de informática. Pena – reclusão, de 3 (três) a 6 (seis) anos, e multa", ao qual acresce "Acórdão" supostamente proferido pelo Tribunal de Justiça do Rio de Janeiro no Processo: 0010830-90.2017.8.19.0014, de 17 de março de 2018, cuja existência não foi sequer possível confirmar, além de ter um teor em absoluto

c) Por outro lado, é de constatar que a criminalização de uma grande parte das condutas que recaem no âmbito da "Fraude informática", tal como concebida pela *Convenção de Budapeste*, ocorreu pela Lei nº 14.155, de 27 de maio de 2021[36], e teve como alicerce um outro crime contra o património, o "Furto" (Artigo 155 do *Código Penal*).

Para o que foi inserida uma nova previsão numas das suas formas qualificadas, o [Furto] "mediante fraude", passando a ser punido quem:

> Subtrair, para si ou para outrem, coisa alheia móvel: […] por meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem a violação de mecanismo de segurança ou a utilização de programa malicioso, ou por qualquer outro meio fraudulento análogo (*Caput* e § 4º I § 4º-B)

Sendo certo que estas ações não cabiam na "Inserção de dados falsos em sistema de informações", pelas razões explicitadas, nem no "Estelio-

discrepante com o conteúdo do preceito analisado (!), assim, "O crime de modificação ou alteração não autorizada de sistema de informações é uma conduta criminosa que consiste em invadir sistemas informatizados alheios, com o objetivo de modificá-los ou alterá-los sem autorização prévia do proprietário. A pena para o crime de modificação ou alteração não autorizada de sistema de informações é de reclusão, de 3 (três) a 6 (seis) anos, e multa, para a hipótese de causar prejuízo à Administração Pública, aplica-se a agravante do parágrafo único do mesmo artigo. A norma que define o crime de modificação ou alteração não autorizada de sistema de informações é importante porque protege a integridade e a confidencialidade dos sistemas de informações, garantindo a privacidade dos dados e das informações armazenadas. Os elementos do crime de modificação ou alteração não autorizada de sistema de informações são: invadir sistemas informatizados alheios, sem autorização prévia do proprietário, com o objetivo de modificá-los ou alterá-los. O crime de modificação ou alteração não autorizada de sistema de informações é uma conduta criminosa que consiste em invadir sistemas informatizados alheios, com o objetivo de modificá-los ou alterá-los sem autorização prévia do proprietário. Trata-se de uma conduta grave, que pode causar prejuízos financeiros e danos à privacidade dos dados e das informações armazenadas. É importante que empresas e pessoas físicas tomem medidas de segurança para proteger seus sistemas de informações contra invasões e ataques cibernéticos."

[36] Precisamente, esta Lei "altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato" <https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14155.htm>.

nato" (Artigo 171 do *Código Penal*), por este pressupor uma ação da própria vítima, em detrimento do seu património, e obtida maliciosamente, como resulta da estrutura da previsão legal: "Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento."

Ora, desde que me debrucei pela primeira vez sobre o preceito, o que até ocorreu poucos dias após a publicação da Lei[37], tive como evidente que esta teve por principais objetivo e efeito legitimar uma Jurisprudência do Superior Tribunal de Justiça[38], logo depois consolidada[39], a

---

[37] Assim, ainda que brevemente, M.D. MASSENO (2021).

[38] Assim, o STJ partiu do entendimento segundo a qual, "1. O furto mediante fraude não se confunde com o estelionato. A distinção se faz primordialmente com a análise do elemento comum da fraude que, no furto, é utilizada pelo agente com o fim de burlar a vigilância da vítima que, desatenta, tem seu bem subtraído, sem que se aperceba; no estelionato, a fraude é usada como meio de obter o consentimento da vítima que, iludida, entrega voluntariamente o bem ao agente. 2. Hipótese em que o agente se valeu de fraude eletrônica para a retirada de mais de dois mil e quinhentos reais de conta bancária, por meio da 'Internet Banking' da Caixa Econômica Federal, o que ocorreu, por certo, sem qualquer tipo de consentimento da vítima, o Banco. A fraude, de fato, foi usada para burlar o sistema de proteção e de vigilância do Banco sobre os valores mantidos sob sua guarda. Configuração do crime de furto qualificado por fraude, e não estelionato. 3. O dinheiro, bem de expressão máxima da idéia de valor econômico, hodiernamente, como se sabe, circula em boa parte no chamado 'mundo virtual' da informática. Esses valores recebidos e transferidos por meio da manipulação de dados digitais não são tangíveis, mas nem por isso deixaram de ser dinheiro. O bem, ainda que de forma virtual, circula como qualquer outra coisa, com valor econômico evidente. De fato, a informação digital e o bem material correspondente estão intrínseca e inseparavelmente ligados, se confundem. Esses registros contidos em banco de dados não possuem existência autônoma, desvinculada do bem que representam, por isso são passíveis de movimentação, com a troca de titularidade. Assim, em consonância com a melhor doutrina, é possível o crime de furto por meio do sistema informático." (CC 67343 / GO, Rel. Min. Laurita Vaz, Terceira Seção, de 20/03/2007, publicado no DJ de 11/12/2007); embora seja apontado como precedente o Acórdão que considerou a aplicabilidade do regime do "Furto" aos atos "[…] praticados por funcionário do Banco do Brasil, consubstanciado[s] na movimentação da conta de um falecido, cujos bens encontram-se em fase de inventário" (CC 40793 / SP, Rel. Min. José Arnaldo da Fonseca, Terceira Seção, de 24/03/2004, publicado no DJ de 19/94/2004).

[39] De este modo, é reiterado que, "Configura crime de furto qualificado a subtração de valores de conta corrente, mediante transferência bancária fraudulenta, sem o consentimento do correntista." (CC 86241 / PR, Rel. Min. Maria Thereza de Assis Moura, Terceira Seção, de 08/08/2007, publicado no DJ de 20/08/2007); que, "2. Embora esteja presente tanto no crime de estelionato, quanto no de furto qualificado,

qual procurou alternativas ao ser confrontada com práticas consistentes em várias vias de manipulação não autorizada de sistemas informáticos para a transferência de ativos financeiros de outrem em proveito próprio ou de terceiros, ao não lhes serem aplicáveis os tipos da "Inserção de dados falsos em sistema de informações" ou da "Modificação ou alteração não autorizada de sistema de informações", por estes serem crimes próprios, como antes explicitado. Mas, com todas as "boas intenções", o "Tribunal da Cidadania" foi manifestamente além da interpretação extensiva, qualificando essas condutas com recurso à *analogia legis*, mesmo estando tal vedado pelo Artigo 5º XXXIX da *Constituição Federal*, assim como pelos Artigos 1º e 2º do *Código Penal*).

Efetivamente, a referida Jurisprudência aplicou à ação de alterar dolosamente dados em sistemas informáticos, alterando regist(r)os de contas de "moeda escritural", uma disciplina apenas prevista para a de "subtrair [...] coisa móvel" e não para um qualquer ativo patrimonial, como no "Estelionato", por exemplo. Porém, diferentemente da "moeda metálica", do "papel-moeda" ou de outro "título ao portador" (Artigos 289 a 292 do *Código Penal*), a "moeda escritural" não era passível de ser tida como "coisa alheia móvel", necessariamente corpórea, por lhe faltar uma equiparação legal como a prevista para "a energia elétrica ou

a fraude atua de maneira diversa em cada qual. No primeiro caso, é utilizada para induzir a vítima ao erro, de modo que ela própria entrega seu patrimônio ao agente. A seu turno, no furto, a fraude visa burlar a vigilância da vítima, que, em razão dela, não percebe que a coisa lhe está sendo subtraída. 2. Na hipótese de transações bancárias fraudulentas, onde o agente se valeu de meios eletrônicos para efetivá-las, o cliente titular da conta lesada não é induzido a entregar os valores ao criminoso, por qualquer artifício fraudulento. Na verdade, o dinheiro sai de sua conta sem qualquer ato de vontade ou consentimento. A fraude, de fato, é utilizada para burlar a vigilância do Banco, motivo pelo qual a melhor tipificação dessa conduta é a de furto mediante fraude. No caso de fraude eletrônica para subtração de valores, o desapossamento da *res furtiva* se dá de forma instantânea, já que o dinheiro é imediatamente tirado da esfera de disponibilidade do correntista." (CC 86.862 / GO, Rel. Min. Napoleão Nunes Maia Filho, Terceira Seção, de 08/08/2007, publicado no DJ de 03/09/2007); ou, ainda, que " [...], o saque fraudulento em conta corrente por meio de internet configura o delito de furto mediante fraude, mas não o de estelionato." (AgRg no CC 74.225/SP, Rel. Min. Jane Silva (Desembargadora convocada do TJ/MG), Terceira Seção, de 25/06/2008, publicado no DJ de 04/08/2008), para apenas resenhar os que concorreram para referida consolidação.

qualquer outra que tenha valor econômico" (Artigo 155 § 3º, a propósito do "Furto")[40].

d) Por outro lado ainda, atendendo à amplitude da *Tatbestand* da "Fraude informática" na *Convenção de Budapeste*, afigura-se como viável considerar que também nela caberão as ações destinadas a obter o resultado através da intervenção da própria vítima, induzida a tal, pelo *dolus* ou pelo *metus*, sempre que estejam presentes tanto os elementos objetivos quanto os subjetivos do tipo em apreço.

No primeiro caso, estará o "Estelionato", desde que na forma qualificada de "Fraude eletrônica" (§ 2.º-A do Artigo 171 do *Código Penal* brasileiro, também inserido em 2021 pela Lei nº 14.155), isto é,

> [...] se a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo.

Assim como a "Fraude com a utilização de ativos virtuais, valores mobiliários ou ativos financeiros" (Artigo 171-A, introduzido pela Lei n.º 14.478, de 21 de dezembro de 2022[41]), pela qual são criminalizadas as ações consistentes em

---

[40] A propósito da necessidade de existir uma previsão legal específica criminalizando ações incidentes sobre dados e não coisas, em sentido próprio, dediquei as considerações iniciais desta intervenção com objetivos essencialmente de ordem didática, M.D. MASSENO (2023), embora já o tivesse feito com alcance mais amplo, M.D. MASSENO (2021); e, para um aprofundamento recente a propósito do alcance da noção de "coisa alheia", enquanto objeto material dos tipos do "Furto" e do "Dano" (*Capita* dos Artigos 155 e 163 *do Código Penal brasileiro*, os quais estão plenamente enquadrados na Cultura romano-germânica), com múltiplas referências comparatísticas e doutrinárias, J.J.F.O. MARTINS (2025).

[41] A qual, "Dispõe sobre diretrizes a serem observadas na prestação de serviços de ativos virtuais e na regulamentação das prestadoras de serviços de ativos virtuais; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para prever o crime de fraude com a utilização de ativos virtuais, valores mobiliários ou ativos financeiros; e altera a Lei nº 7.492, de 16 de junho de 1986, que define crimes contra o sistema financeiro nacional, e a Lei nº 9.613, de 3 de março de 1998, que dispõe sobre lavagem de dinheiro, para incluir as prestadoras de serviços de ativos virtuais

> Organizar, gerir, ofertar ou distribuir carteiras ou intermediar operações que envolvam ativos virtuais, valores mobiliários ou quaisquer ativos financeiros com o fim de obter vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil ou qualquer outro meio fraudulento.

O que, em especial, relevará quando a "inserção, alteração, apagamento ou supressão de dados de computador" ou "qualquer interferência no funcionamento de um computador ou de um sistema de computadores" forem possibilitadas por meio de engano da vítima, assim como de terceiro.

O mesmo se poderá dizer das ações correspondentes aos ataques de *ransomware*, as quais podem ser enquadrados no crime de "Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública" (Artigo 266 do *Código Penal*), que penaliza a conduta de quem

> Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento [ou de] quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento.

Em concurso material com a "Extorsão" (Artigo 158.º do *Código Penal*), ou seja, a ação de "Constranger alguém, mediante violência ou grave ameaça, e com o intuito de obter para si ou para outrem indevida vantagem econômica, a fazer, tolerar que se faça ou deixar de fazer alguma coisa"

No pressuposto de os interesses públicos relativos à continuidade das comunicações eletrónicas prevalecerem sobre a dimensão patrimonial, desde uma perspectiva assente na proporcionalidade entre os meios e os fins[42].

---

no rol de suas disposições", tendo objetivos semelhantes aos da Diretiva (UE) 2019/713, de 17 de abril de 2019, por várias vezes mencionada.

[42] Assim, as conclusões de M.D. MASSENO & E. WENDT (2017), bem como as de D.R. NUNES (2019a), este centrado no Direito Penal português.

4 ALGUMAS, BREVÍSSIMAS, CONSIDERAÇÕES CONCLUSIVAS

Nas páginas anteriores, intentei mostrar como o Brasil dispõe de um mosaico de tipos penais suscetíveis de sancionarem as condutas abrangidas pela "Fraude informática" na *Convenção de Budapeste*.

Mas, a sobreposição não é perfeita e as vias "originais" seguidas, em especial o enquadramento no "Furto", podem dificultar a cooperação das Autoridades Policiais e Judiciárias dos outros Estados Partes, a qual constituiu o objetivo principal da Adesão do Brasil, longamente almejada pela Polícia Federal e o Ministério Público.

A meu ver, porventura a via mais simples seria a de transformar os atuais tipos "Inserção de dados falsos em sistema de informações" e "Modificação ou alteração não autorizada de sistema de informações" em crimes comuns. O que teria a vantagem adicional de criminalizar as condutas relativas à "Violação de dados" e à "Interferência em sistema" da *Convenção*, as quais só estão parcialmente previstas nas Fontes brasileiras[43].

Em suma, Congresso Nacional deverá adequar o Ordenamento brasileiro a este novo enquadramento, o que será uma oportunidade para atualizar o Direito Penal Material. Espero ter dado mais um, necessariamente pequeno, contributo para um tal desiderato.

REFERÊNCIAS

BARREIRA, C.F. (2015). "Home banking: A Repartição dos prejuízos decorrentes de fraude informática". **RED – Revista Eletrónica de Direito,** 3. Disponível em: https://bit.ly/4bbAD7h. Acesso em: 28 mar. 2025.

BRAVO, R. (2003). "O Crime de Acesso Ilegítimo na Lei da Criminalidade Informática e na CiberConvenção". **Direito n@ Rede**, 3. Disponível em: https://bit.ly/3tY2OWk. Acesso em: 28 mar. 2025.

CARVALHO, F.P., MORALES G., O. & ÁLVAREZ F., M. (2018). "Regulamentação supranacional sobre Criminalidade Informática e Técnicas de Transposição. O Direito Penal Português e Espanhol como Paradigmas". **Actualidad Jurídica**

[43] Como procurei mostrar, ainda que sumariamente, M.D. MASSENO (2023c).

Uría Menéndez, 48, 48-64. Disponível em: https://www.uria.com/documentos/publicaciones/5801/documento/art04.pdf . Acesso em: 28 mar. 2025.

CORRÊA, I.D. & MONTEIRO Neto, J.A. (2023). "A adesão do Brasil à Convenção de Budapeste e o enfrentamento do Cibercrime: entre a Cooperação Internacional e a expansão do Direito Penal". **Revista Eletrônica Direito & TI,** 16(1), 32-60. Disponível em: https://www.direitoeti.com.br/direitoeti/article/view/155. Acesso em: 28 mar. 2025.

DIAS, P.S. (2006). "O 'hacking' enquanto crime de acesso ilegítimo. Das suas especialidades à utilização das mesmas para fundamentação de um novo direito". **Actualidad Jurídica Uría Menéndez,** n.º 14, 55-72. Disponível em: https://www.uria.com/documentos/publicaciones/1580/documento/art04.pdf. Acesso em: 28 mar. 2025.

MARTINS, J.J.F.O. (2025). "O crime de dano simples (Uma revisitação no âmbito duma visão jurídico funcional da tutela penal do património)". **JULGAR DIGITAL**. Disponível em: https://julgar.pt/o-crime-de-dano-simples-uma-revisitacao-no-ambito-duma-visao-juridico-funcional-da-tutela-penal-do-patrimonio/. Acesso em: 28 mar. 2025.

MASSENO, M.D. (2018). "Da criminalização do 'acesso ilícito' (*hacking*) nos Ordenamentos do Brasil e de Portugal". CALHEIROS, C. *et al*. (Eds.). **Direito na lusofonia:** direito e novas tecnologias. Braga: Escola de Direito da Universidade do Minho, 279-288, assim como a presentação complementar. Disponíveis em: https://bit.ly/3SfnC3L e https://bit.ly/4bVUwQs. Acesso em: 28 mar. 2025.

MASSENO, M.D. (2021a). "Nas Fronteiras da PI: os direitos patrimoniais sobre dados, uma perspectiva europeia". **Revista Rede de Direito Digital, Intelectual & Sociedade**, 1(1) 101-113. Disponível em: https://revista.ioda.org.br/index.php/rrddis/article/view/9. Acesso em: 28 mar. 2025.

MASSENO, M.D. (2021b). **Depois da Lei nº 14.155, de 27 de maio de 2021, que mais faltará fazer para o Brasil se ajustar à Convenção de Budapeste?** Palestra ao V Congresso Nacional de Direito Digital. Organizado pela Comissão de Direito Digital, *Startups* e Inovação da Seção do Amazonas da Ordem dos Advogados do Brasil, com a Comissão de Direito Digital da Seção de Santa Catarina, também da OAB, da *Digital Law Academy* e do Portal Juristas.com.br, desde Manaus, no dia 1 de junho de 2021. Disponível em: https://bit.ly/3FHvpET. Acesso em: 28 mar. 2025.

MASSENO, M.D. (2023a). **Das Fontes Internacionais e Europeias da Cibercriminalidade.** Aula ao XII Curso de Mestrado em Direito e Informática da Escola de Direito da Universidade do Minho, Braga. Disponível em: https://bit.ly/3U3XtYk. Acesso em: 28 mar. 2025.

MASSENO, M.D. (2023b). **Os cibercrimes contra o património**: alguns apontamentos sobre as fontes. Aula à Pós-Graduação em "Direito e Tecnologia" na Escola do Porto da Faculdade de Direito da Universidade Católica Portuguesa. Disponível em https://bit.ly/423SwB6. Acesso em: 28 mar. 2025.

MASSENO, M.D. (2023c). **Os Tipos Penais Brasileiros perante a Convenção de Budapeste sobre o Cibercrime, principais problemas de adequação.** Porto Alegre: WB Educação. Disponível em: https://bit.ly/46cuLXM. Acesso em: 28 mar. 2025.

MASSENO, M.D. (2023d). Dos ataques de 'ransomware' na 'Convenção de Budapeste sobre o Crime Cibernético', um ensaio de qualificação alternativa, desde Portugal. **Privacy and Data Protection Magazine - Revista Científica na Área Jurídica**, 6, 63-81. Disponível em: https://bit.ly/49ZjXzr. Acesso em: 28 mar. 2025.

MASSENO, M.D. (2025). **Da Burla [fraude] Informática**. Palestra às Jornadas sobre "Cibercrime e Direitos Humanos" da "European Law Students Association" da Escola do Porto da Faculdade de Direito da Universidade Católica Portuguesa. Disponível em: https://bit.ly/4hHSV1K. Acesso em: 28 mar. 2025.

MASSENO, M.D., MARTINS, G.M. & FALEIROS Jr. (2020). "A Segurança na Proteção de Dados: Entre o RGPD Europeu e a LGPD Brasileira". **Revista do CEJUR/TJSC: Prestação Jurisdicional**, 8(1), e346. Disponível em: https://revistadocejur.tjsc.jus.br/cejur/article/view/346. Acesso em: 28 mar. 2025.

MASSENO, M.D. & WENDT, E. (2017). "O *Ransomware* na Lei: Apontamentos Breves de Direito Português e Brasileiro". **Revista Eletrônica Direito & TI,** 1(8). Disponível em: https://direitoeti.com.br/direitoeti/article/view/80. Acesso em: 28 mar. 2025.

MOTA, P.L.R. (2019). "Crime de burla informática e nas comunicações. Enquadramento jurídico, prática e gestão processual". PEREIRA, L. M. C. S. *et al*. (Eds.), **O Crime de Abuso de Cartão de Garantia e Crédito e o Crime de Burla Informática** (Trabalhos do 2.º Ciclo do Curso de Formação – Ministério Público). Lisboa: Centro de Estudos Judiciários, 167-192. Disponível em: https://bit.ly/4aV3soa. Acesso em: 28 mar. 2025.

NUNES, D.R. (2017). "O crime de falsidade informática". **JULGAR Online**. Disponível em: https://julgar.pt/o-crime-de-falsidade-informatica/. Acesso em: 28 mar. 2025.

NUNES, D.R. (2019a). "O fenómeno do *Ransomware* e o seu enquadramento jurídico-penal". **Cyberlaw by CIJIC**, 8, 58-82. Disponível em: https://www.iuris.edu.pt/xms/files/Cyberlaw-by-CIJIC_8.pdf. Acesso em: 28 mar. 2025.

NUNES, D.R. (2019b). "Reflexões sobre as alterações às disposições penais materiais da Lei do Cibercrime". **Privacy and Data Protection Magazine - Revista Científica na Área Jurídica,** 5, 11-50. Disponível em: https://www.europeia.pt/resources/media/documents/Revista_Privacy_Data_Protection_Magazine_N5.pdf. Acesso em: 28 mar. 2025.

PALMA, D.S. (2019). "Crime de burla informática e nas comunicações. Enquadramento jurídico, prática e gestão processual". PEREIRA, L. M. C. S. *et al*. (Eds.), **O Crime de Abuso de Cartão de Garantia e Crédito e o Crime de Burla Informática** (Trabalhos do 2.º Ciclo do Curso de Formação – Ministério Público). Lisboa: Centro de Estudos Judiciários, 73-105. Disponível em: https://bit.ly/4aV3soa. Acesso em: 28 mar. 2025.

PEDRA, C.G. (2019). "Crime de burla informática e nas comunicações. Enquadramento jurídico, prática e gestão processual". PEREIRA, L. M. C. S. *et al*. (Eds.), **O Crime de Abuso de Cartão de Garantia e Crédito e o Crime de Burla Informática** (Trabalhos do 2.º Ciclo do Curso de Formação – Ministério Público). Lisboa: Centro de Estudos Judiciários, 11-38. Disponível em: https://bit.ly/4aV3soa. Acesso em: 28 mar. 2025.

RODRIGUES, C. (2019). "Crime de burla informática e nas comunicações. Enquadramento jurídico, prática e gestão processual". PEREIRA, L. M. C. S. *et al*. (Eds.), **O Crime de Abuso de Cartão de Garantia e Crédito e o Crime de Burla Informática** (Trabalhos do 2.º Ciclo do Curso de Formação – Ministério Público). Lisboa: Centro de Estudos Judiciários, 39-71. Disponível em: https://bit.ly/4aV3soa. Acesso em: 28 mar. 2025.

SOUZA, C.M. & BARBOZA, H.L. (2022). "O Enfrentamento do Cibercrime entre a Cooperação Internacional e a Expansão do Direito Penal". **Revista Jurídica Luso-Brasileira**, 8(4), 957-994. Disponível em: https://www.cidp.pt/revistas/rjlb/2022/4/2022_04_0957_0994.pdf. Acesso em: 28 mar. 2025.

VENÂNCIO, P.D. (2013). "Similarity and Competition Between Cybercrimes Related to Computer Data in the Council of Europe's Convention on Cybercri-

me". **Masaryk University Journal of Law and Technology,** 7(1), 97-105. Disponível em: https://journals.muni.cz/mujlt/article/view/2629. Acesso em: 28 mar. 2025.

VERDELHO, P. (2003). "A Convenção sobre Cibercrime do Conselho da Europa – Comentário". VERDELHO, P. *et al.* (Eds.): **Leis do Cibercrime,** I. Centro Atlântico: Vila Nova de Famalicão, 10-23. Disponível em: https://bit.ly/3TUEM9r. Acesso em: 28 mar. 2025.

Recebido em 18 de abril de 2025
Aprovado em 25 de junho de 2025