Data Venia
REVISTA JURÍDICA DIGITAL

A previsão dos crimes informáticos no Código Penal Angolano: *uma análise crítica de política criminal e direito comparado lusófono*

16
2026/2027

Abrantes Malaquias Belo Caiúve

Doutorando em Ciências Jurídicas na Escola de Direito da Universidade do Minho (Portugal); Mestre em Direito e Informática pela Escola de Direito da Universidade do Minho; Licenciado em Direito; Docente Universitário, Assessor Jurídico do Ministério Público e Investigador

Data Venia

Revista científico-jurídica em formato digital
Publicação em fluxo contínuo
ISSN 2182-8242

N.º **16** — Anos 2026/2027

Propriedade e Edição:
© DataVenia
Marca Registada 486523 INPI

Internet : www.datavenia.pt
Contacto : correio@datavenia.pt

Revista científico-jurídica em formato digital. A citação, transcrição ou reprodução dos conteúdos estão sujeitas ao Código de Direito de Autor e Direitos Conexos. É proibida a reprodução ou compilação de conteúdos para fins comerciais ou publicitários.

Citação deste artigo, norma NP ISO 690:2024

CAIÚVE, Abrantes Malaquias Belo. A previsão dos crimes informáticos no Código Penal Angolano: uma análise crítica de política criminal e direito comparado lusófono. *DataVenia*. Em linha. 2026, Vol. 16, pp. 53-74. ISSN 2182-8242.

URL: www.datavenia.pt/edicao16/datavenia16_p053-074.pdf

A previsão dos crimes informáticos no Código Penal Angolano: *uma análise crítica de política criminal e direito comparado lusófono*

Abrantes Malaquias Belo Caiúve

Doutorando em Ciências Jurídicas na Escola de Direito da Universidade do Minho (Portugal).

Mestre em Direito e Informática pela Escola de Direito da Universidade do Minho.

Licenciado em Direito.

Docente Universitário, Assessor Jurídico do Ministério Público e Investigador.

ORCID: https://orcid.org/0000-0001-8640-6295.

PALAVRAS-CHAVE: Crimes Informáticos; Código Penal Angolano; Política Criminal; Lei Especial; Direito Comparado Lusófono.

KEY WORDS: Computer-related Offences; Angolan Penal Code; Criminal Policy; Special Legislation; Lusophone Comparative Law.

RESUMO:

O Código Penal Angolano de 2020 (Lei n.º 38/20, de 11 de novembro) consagrou, pela primeira vez no ordenamento jurídico angolano, uma tipificação sistemática dos crimes informáticos no Título VIII da sua Parte Especial. Não obstante o inegável avanço normativo e simbólico que a rutura com o Código Penal de 1886 representa, a opção por encorpar a generalidade dos ilícitos cibernéticos no texto codificado comum suscita reservas dogmáticas e de política criminal. A constante evolução e extrema volatilidade das Tecnologias de Informação e Comunicação (TIC), aliadas às exigências adjetivas de obtenção e preservação de prova digital, têm levado a dogmática e a praxis legislativa internacional a privilegiar a aprovação de legislação especial extravagante. O presente artigo analisa criticamente a opção do legislador angolano, promovendo um exame dos tipos penais estatutários e um confronto analítico com as soluções adotadas no espaço da lusofonia (em especial Portugal, Cabo Verde e Brasil). Conclui-se pela conveniência de uma harmonização setorial que desloque os crimes informáticos puros e as normas adjetivas de prova digital para uma Lei do Cibercrime autónoma, reservando para o Código Penal apenas os ilícitos tradicionais que protegem diretamente bens jurídicos pessoais.

ABSTRACT:

The Angolan Penal Code of 2020 (Law No. 38/20 of 11 November) introduced, for the first time in the Angolan legal system, a systematic criminalization of

computer-related offences under Title VIII of its Special Part. Despite the undeniable normative and symbolic progress represented by the break with the 1886 Penal Code, the decision to incorporate the majority of cybercrime offences into the general codified framework raises significant concerns from both a dogmatic and criminal policy perspective. The constant evolution and extreme volatility of Information and Communication Technologies (ICTs), coupled with the procedural requirements governing the collection and preservation of digital evidence, have led international legal scholarship and legislative practice to favour the adoption of specialized standalone legislation. This article critically examines the legislative choice made by Angola, providing a dogmatic analysis of the statutory offences and a comparative assessment of the legal frameworks adopted in Lusophone jurisdictions, particularly Portugal, Cape Verde, and Brazil. It concludes that sector-specific harmonization would be desirable, whereby pure computer-related offences and procedural rules governing digital evidence would be transferred to an autonomous Cybercrime Law, while the Penal Code would be reserved for traditional offences that directly protect individual legally protected interests.

1. INTRODUÇÃO

Angola alcançou a independência a 11 de Novembro de 1975 herdando o Código Penal de 1886 da antiga potência colonial, cujos preceitos se revelavam manifestamente desatualizados face às exigências da sociedade contemporânea. O vertiginoso avanço das Tecnologias de Informação e Comunicação (TIC) – evidenciado na migração de atividades para ambientes virtuais, no uso intensivo da internet, na exposição da vida privada nas redes sociais, na expansão do trabalho remoto e no incremento das transações bancárias e pagamentos *online* – propiciou a emergência de novos bens jurídicos merecedores de tutela penal, tornando premente a criminalização das condutas informáticas nocivas.

A concretização legislativa dessa tutela ocorreu a 11 de Novembro de 2020 com a aprovação do Código Penal Angolano[1] pela Lei n.º 38/20[2] (em vigor desde 9 de Fevereiro de 2021), no qual os crimes informáticos[3] foram acolhidos nos Capítulos II e III do Título VIII do Livro II.

[1] Antes da existência deste código, o Anteprojeto de Lei do Código Penal de Angola – aprovado no dia 23 de Janeiro de 2019 pela Assembleia Nacional – já previa o tratamento da criminalidade informática. Para mais informações sobre o assunto consulte-se BELO CAIÚVE, Abrantes Malaquias. *A problemática da regulação dos crimes informáticos na proposta de lei do Código Penal angolano e a sua conformidade com a Convenção de Budapeste sobre o cibercrime*. Dissertação de Mestrado em Direito e Informática. Universidade do Minho, Setembro de 2020, Capítulo III, p. 73 e seguintes.

[2] Neste mesmo Diário consta a Lei n.º 39/20 que aprova o Código do Processo Penal Angolano que revogou, dentre os vários diplomas, o Código do Processo Penal do remoto ano de 1929.

[3] A Lei n.º 38/20, que aprova o Código Penal Angolano, utiliza a designação "crimes informáticos" para o conjunto de ilícitos que a doutrina e a legislação comparada, como a Lei n.º 109/2009, de 15 de Setembro (Lei do Cibercrime portuguesa), frequentemente denominam de "crimes cibernéticos" ou "cibercrimes". Ao longo deste trabalho, adoptaremos a terminologia consagrada pelo legislador

No Capítulo II, sob a epígrafe dos delitos contra os dados informáticos, tipificam-se o *Acesso ilegítimo a sistema de informação e devassa através de sistema de informação* (art.º 438.º); a *Intercepção ilegítima em sistema de informação* (art.º 439.º); e o *Dano em dados informáticos* (art.º 440.º).

No Capítulo III, concernente aos crimes contra as comunicações e sistemas informáticos, consagram-se a *Sabotagem informática* (art.º 441.º); a *Falsidade informática* (art.º 442.º); a *Burla informática e nas comunicações* (art.º 443.º); e a *Reprodução ilegítima de programas de computador, bases de dados e topografia de produtos semicondutores* (art.º 444.º).

Cabe assinalar que o Título VIII do Código Penal não exaure o tratamento dos ilícitos cibernéticos na codificação substantiva, visto que a pornografia infantil se encontra tipificada no art.º 198.º, inserido no Título I (Crimes contra as Pessoas), perfazendo um catálogo de oito tipos legais de crime com feição informática acolhidos na lei geral.

Nos pontos subsequentes, procedemos à análise dos elementos objetivos e subjetivos, dos bens jurídicos[4] e das modalidades de cometimento de cada um dos tipos penais enunciados, demonstrando a necessidade dogmática e prática da sua transferência para uma legislação especial. Por razões de delimitação do objeto de estudo, não se analisam aqui as infrações penais com dimensão informática previstas em legislação extravagante fora do Código Penal[5], nem se aprofunda a dimensão adjectiva do Direito do Cibercrime[6].

Metodologicamente, recorreu-se à análise dogmática dos tipos penais (pelos métodos literal, teleológico e sistemático) e ao confronto com os ordenamentos lusófonos (método comparativo), numa investigação de cariz qualitativo e documental, circunscrita ao direito substantivo codificado.

2. ASPETOS RELEVANTES QUE JUSTIFICAM A REMOÇÃO DOS CRIMES INFORMÁTICOS DO CORPUS DO CÓDIGO PENAL ANGOLANO

angolano, "crimes informáticos", sem prejuízo de, por vezes, recorrermos aos outros termos quando em contexto de direito comparado.

[4] Sobre os bens jurídicos destes delitos também pode ler-se a obra de CUNHA, Jelssimi Moisés da. *Os crimes informáticos no direito penal angolano*. JuLaw. 13 de Novembro de 2020, p. 11-21. https://julaw.ao/wp-content/uploads/2020/11/JELSSIMI-DA-CUNHA_OS-CRIMES-INFORMATICOS-NO-DIREITO-PENAL-ANGOLANO_JULAW.pdf (Acedido em 28-03-2024).

[5] Dentre os quais destacamos os tipos legais de crime constantes nos artigos 55.º, 56.º, 57.º, 58.º e 59.º da Lei n.º 22/2011, de 17 de Junho, Lei da Proteção de Dados Pessoais, sendo respectivamente: Incumprimento das obrigações relativas a proteção de dados pessoais; Acesso indevido; Viciação ou destruição de dados pessoais; Desobediência qualificada e Violação do dever de sigilo.

[6] Embora reconhecemos que o Código do Processo Penal Angolano faz uma abordagem incipiente sobre a tramitação processual dos crimes informáticos, pois não dá cabal acolhimento as questões atinentes a produção da prova digital ou electrónica, bem como a cooperação internacional que se impõe nesta tipologia criminal dada a sua natureza transfronteiriça. Na cooperação internacional releva-se a importância de pontos de contacto dos países que devem funcionar non stop 24 horas durante os 7 dias da semana, daí a Convenção de Budapeste designá-los por Rede 24/7. A relevância desses assuntos impõe o seu tratamento num artigo científico específico a ser produzido brevemente.

2.1. Os delitos contra os dados informáticos

O primeiro ilícito a analisar é o *acesso ilegítimo*[7] *a sistema de informação e devassa através de sistema de informação*, previsto no art.º 438.º do Código Penal. Na prática judiciária e social quotidiana, tem sido frequente a constatação do acesso[8] não autorizado à conta de correio eletrónico de outrem ou ao seu perfil em redes sociais (com especial incidência no *Facebook*), atuações que preenchem formalmente esta tipologia incriminadora.

A opção da legislação angolana revela-se singular ao aglutinar[9], num mesmo preceito legal, duas infrações que a doutrina e o Direito comparado autonomizam[10]. Trata-se de uma solução legislativa que se afigura desaconselhável, pelas razões que a seguir se sintetizam:

1. **Autonomia dos Bens Jurídicos:** Cada um dos ilícitos acolhidos no art.º 438.º tutela um bem jurídico próprio. Entre o bem jurídico protegido pelo acesso ilegal (*hacking*) e o tutelado pela devassa informática[11] não existe sobreposição nem contiguidade direta.

2. **Objeto do Acesso Ilegítimo:** O acesso ilegítimo a sistema de informação visa preservar a segurança e integridade do sistema informático enquanto verdadeiro "domicílio informático"[12], na medida em que a intromissão não autorizada se revela "semelhante à introdução em casa alheia"[13][14].

[7] Benjamim Silva Rodrigues distingue três modalidades de acesso ilegítimo: o acesso ilegítimo ganancioso; o acesso ilegítimo perigoso ou insidioso; e o acesso ilegítimo de exploração, aventureiro ou de curiosidade. RODRIGUES, Benjamim Silva. *Direito Penal - Parte Especial: Direito Penal Informático-Digital*. Tomo I-D. Coimbra: Coimbra Editora, 2009, p. 286.

[8] Para uma exemplificação alargada de comportamentos enquadráveis nesta modalidade criminal, *v.* NUNES, Duarte Alberto Rodrigues. *Os Crimes Previstos na Lei do Cibercrime e a Responsabilidade Penal dos Entes Coletivos*. 2.ª ed. Coimbra: Gestlegal, 2024, pp. 301-302.

[9] A intenção de unificar ambas as condutas já era visível na Versão Final do Anteprojeto de Código Penal, que subsumia o acesso ilegítimo no texto do art.º 212.º, atinente à devassa por meio de informática.

[10] A título exemplificativo, em Cabo Verde (art.º 6.º) e em Portugal (art.º 6.º) o acesso ilegítimo encontra-se previsto nas respetivas Leis do Cibercrime; em São Tomé e Príncipe integra o art.º 7.º da Lei do Cibercrime. Em contrapartida, a devassa por meio de informática é punida no Código Penal em Cabo Verde (art.º 188.º) e em São Tomé e Príncipe (art.º 202.º); em Portugal encontra-se consagrada no art.º 193.º do Código Penal e decorre do art.º 35.º, n.º 3, da Constituição da República Portuguesa.

[11] Utiliza-se no presente estudo a expressão "devassa informática" por razões de simplicidade expositiva, correspondendo formalmente ao tipo legal de "devassa através de sistema de informação" acolhido no art.º 438.º do Código Penal Angolano.

[12] PORTUGAL. Tribunal da Relação do Porto. Acórdão de 15/10/2008. *In* PORTUGAL. Ministério Público. *Jurisprudência sobre Cibercrime*. Nota Prática n.º 15/2020. Disponível em: http://cibercrime.ministeriopublico.pt/pagina/jurisprudencia-sobre-cibercrime. Acesso em: 1 mar. 2024.

[13] Idem.

[14] No Código Penal Angolano, a violação de domicílio encontra-se tipificada no art.º 228.º, encabeçando o rol dos Crimes Contra a Reserva da Vida Privada.

3. **Objeto da Devassa Informática:** A devassa através de sistema de informação protege o núcleo essencial da vida privada[15], abrangendo os dados pessoais (com especial relevo para os dados sensíveis) e as informações de caráter não pessoal. Em termos mais amplos, a devassa informática garante "o direito à autodeterminação informacional e comunicacional, no sentido de que qualquer pessoa tem o direito a não ver processados determinados dados"[16].

Acresce uma distinção atinente à natureza dogmática de ambos os crimes: o acesso ilegítimo qualifica-se como um crime informático puro ou próprio[17], unicamente perpetrável no e através do ambiente digital; por sua vez, a devassa por meio de sistema de informação constitui um tipo penal impróprio, concebido para conferir tutela ao direito à identidade, à privacidade e à intimidade, expressamente consagrado no art.º 32.º, n.º 1, da Constituição da República de Angola[18].

A utilização da conjunção copulativa "e" na epígrafe do art.º 438.º sugere que o legislador reconheceu a dualidade das condutas que pretendia punir, pois, de outro modo, teria recorrido à conjunção alternativa "ou"[19]. Ademais, a própria estrutura do preceito reflete essa divisão binária: a primeira parte (n.os 1 e 2) disciplina o acesso ilegítimo, ao passo que a segunda parte (n.º 4) regula a devassa por meio de sistema de informação.

Preconiza-se, pois, a autonomização formal e sistemática destes dois tipos legais. O acesso ilegítimo deve ser transferido para uma lei especial extravagante dedicada exclusivamente ao cibercrime (dada a sua natureza puramente tecnológica), enquanto a devassa informática deve permanecer no Código Penal, integrada no capítulo dos crimes contra a reserva da vida privada.

O segundo ilícito integrado no grupo dos delitos contra os dados informáticos é a *interceção ilegítima em sistema de informação*, prevista no art.º 439.º do Código Penal. Trata-se, tal como o acesso ilegítimo, de um crime informático puro, vocacionado para a proteção da confidencialidade das transmissões de dados informáticos.

---

[15] A devassa informática intensificou as preocupações respeitantes à proteção da vida privada, na medida em que a capacidade intrusiva dos meios informáticos expõe a intimidade a riscos permanentes de devassa. ASCENSÃO, José de Oliveira. Criminalidade informática. *In*: *Direito da Sociedade da Informação*. Vol. II. Coimbra: Coimbra Editora, 2001, p. 264.

[16] RODRIGUES, Benjamim Silva. *Op. cit.*, p. 462.

[17] Os crimes informáticos puros caracterizam-se por terem o sistema informático como meio exclusivo de execução, sendo impossível o seu cometimento sem o recurso a meios computacionais. Nestes ilícitos, o bem jurídico protegido é a própria integridade e segurança do sistema tecnológico. CASTRO, Carla Rodrigues Araújo de. *Crimes de Informática e seus Aspectos Processuais*. 2.ª ed. Rio de Janeiro: Lumen Juris, 2003, p. 230.

[18] O art.º 32.º, n.º 1, da Constituição da República de Angola estabelece: «A todos são reconhecidos os direitos à identidade pessoal, à capacidade civil, à nacionalidade, ao bom nome e reputação, à imagem, à palavra e à reserva de intimidade da vida privada e familiar.».

[19] BELO CAIÚVE, Abrantes Malaquias. *Os Crimes Informáticos: Uma Análise ao seu Tratamento no Código Penal Angolano*. Lisboa: Lisbon International Press, 2023, p. 108.

Neste âmbito, o artigo 3.º da Convenção de Budapeste sobre o Cibercrime impõe aos Estados Partes a criminalização da interceção não autorizada, efetuada por meios técnicos, de transmissões não públicas de dados informáticos dirigidas a, originadas de ou efetuadas dentro de um sistema informático, incluindo as emissões eletromagnéticas que os transportem. A incriminação visa, assim, obstar a que terceiros obtenham, sem legitimidade, o conteúdo ou os metadados de uma comunicação privada.

Não obstante o artigo 3.º da Convenção se encontrar sistematicamente inserido no Título 1 (dedicado aos crimes contra a confidencialidade, integridade e disponibilidade dos dados e sistemas – os três pilares do modelo clássico de segurança da informação[20]), não se deve inferir que a interceção ilegítima exija a lesão simultânea desses três atributos. A sua especificidade reside, primordialmente, na salvaguarda da confidencialidade das comunicações e dos dados em trânsito, distinguindo-se das condutas que provocam a alteração, destruição ou indisponibilidade dos sistemas.

A interceção ilegítima atenta predominantemente contra a confidencialidade: a espionagem cibernética executada por meio de intromissões técnicas viola o segredo das comunicações ao permitir que a informação seja captada, observada ou escutada por terceiros não autorizados.

Expurgada a dimensão especificamente tecnológica, o conteúdo do art.º 439.º aproxima-se da estrutura do crime tradicional de violação de correspondência (art.º 231.º do CP). A interceção ilegítima opera como uma modalidade de violação da correspondência no ecossistema digital, tratando-se de uma matéria que reclama futura densificação dogmática, designadamente quanto às relações de concurso ou eventual consunção entre ambos os tipos.

Este tipo incriminador salvaguarda dois imperativos constitucionais da Lei Magna angolana:

- A "inviolabilidade da correspondência e das comunicações" (art.º 34.º, n.ºs 1 e 4);
- O "direito à privacidade" (art.º 32.º), estendido à privacidade na *internet* ou "privacidade electrónico-digital"[21], evidenciando a conexão entre a tutela penal da interceção e a proteção dos dados pessoais[22].

[20] O triplo atributo da segurança da informação é comummente designado pela sigla CID (Confidencialidade, Integridade e Disponibilidade). Determinados autores aditam a esta tríade a autenticidade e o não-repúdio. *V.* https://definirtec.com/confidencialidade-integridade-e-disponibilidade-triade-cia/. Acesso em: 28 mar. 2024.

[21] Expressão utilizada por RODRIGUES, Benjamim Silva. *Op. cit.*, p. 452.

[22] A atenção das autoridades angolanas a esta matéria traduziu-se na aprovação da Lei n.º 22/11, de 17 de Junho (Lei da Proteção de Dados Pessoais); na aprovação do Estatuto Orgânico da Agência de Protecção de Dados (APD) pelo Decreto Presidencial n.º 214/16, de 10 de Outubro; e na Resolução n.º 33/19, de 9 de Julho, que aprovou a Convenção da União Africana sobre Cibersegurança e Protecção de Dados Pessoais (Convenção de Malabo).

O bem jurídico tutelado pela interceção ilegítima abrange a "privacidade na comunicação de dados"[23], vulnerada por técnicas de intromissão como o *sniffing* e os ataques do tipo *Man-in-the-Middle*. Por se tratar de um ilícito de execução estritamente tecnológica, a sua sede adequada situa-se numa lei especial do cibercrime.

Por fim, o terceiro e último delito contra os dados informáticos é o *dano em dados informáticos*, previsto no art.º 440.º do Código Penal. Na legislação europeia, o artigo 4.º da Decisão-Quadro 2005/222/JAI[24] do Conselho da União Europeia, de 24 de Fevereiro de 2005, adota para esta infração a designação "interferência em dados".

A opção terminológica acolhida pelo legislador angolano revela-se dogmaticamente correta. A fórmula adotada no art.º 4.º da Lei do Cibercrime portuguesa (Lei n.º 109/2009) – "dano relativo a programas ou outros dados informáticos" – padece de redundância, na medida em que o conceito legal de dados acolhido na alínea l) do art.º 4.º[25] da Lei de Protecção das Redes e Sistemas Informáticos[26] engloba expressamente os próprios programas de computador.

Embora guarde afinidade nominal com o crime comum de dano (art.º 410.º do CP), entre ambos os tipos "jamais existirá qualquer sobreposição"[27], porquanto o dano tradicional protege bens corpóreos, enquanto o dano em dados informáticos tutela bens incorpóreos de natureza digital.

Diversamente do acesso ilegítimo, o dano em dados informáticos não configura um crime de perigo abstrato; a estrutura do n.º 1 do art.º 440.º revela um crime de resultado, qualificável como crime informático puro.

[23] RODRIGUES, Benjamim Silva. *Op. cit.*, p. 518.

[24] UNIÃO EUROPEIA. Decisão-Quadro 2005/222/JAI do Conselho, de 24 de Fevereiro de 2005, relativa a ataques contra os sistemas de informação. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32005F0222. Acesso em: 31 mar. 2024.

[25] A alínea l) do art.º 4.º da Lei n.º 7/17 define «Dados» como: "Qualquer representação de factos, vídeos ou imagens, informações ou conceitos, incluindo de programas de computador, que são armazenados, transmitidos ou processados num sistema de informação.". Em sentido idêntico, o art.º 2.º, alínea b), da Lei do Cibercrime portuguesa (Lei n.º 109/2009, de 15 de Setembro) define «Dados informáticos» como: "Qualquer representação de factos, informações ou conceitos sob uma forma susceptível de processamento num sistema informático, incluindo os programas aptos a fazerem um sistema informático executar uma função.".

[26] Lei n.º 7/17, de 16 de Fevereiro (Lei de Protecção das Redes e Sistemas Informáticos). Disponível em: https://lex.ao/docs/assembleia-nacional/2017/lei-n-o-7-17-de-16-de-fevereiro/. Acesso em: 29 mar. 2024.

[27] NUNES, Duarte Alberto Rodrigues. O crime de dano relativo a programas ou outros dados informáticos. *Revista do Ministério Público*, Lisboa, ano 39, n.º 153, p. 142, jan./mar. 2018. Disponível em: https://rmp.smmp.pt/wp-content/uploads/2018/04/6.RMP_153_NET_Duarte_Nunes.pdf. Acesso em: 9 ago. 2026.

No concernente ao bem jurídico, subscreve-se o entendimento de que esta incriminação tutela "a integridade funcional dos dados informáticos, no que tem que ver com a disponibilidade e usabilidade dos mesmos"[28].

As modalidades de execução são heterogéneas, abrangendo a disseminação de vírus e programas maliciosos (*malware*, incluindo *Trojan horses*, *scareware*, *worms*, *spyware* e *ransomware*), bem como a distribuição massiva e não solicitada de correio eletrónico (*spam*).

Deste modo, tratando-se de uma infração que atinge a integridade funcional do património digital e que se encontra sujeita a permanente mutação semântica e tecnológica, a sua estatuição em lei especial extravagante afigura-se a solução legislativa mais consentânea com os princípios da política criminal contemporânea.

2.2. Os delitos contra as comunicações e sistemas informáticos

A *sabotagem informática*, ou interferência em sistemas, é a primeira infração a figurar neste catálogo. Apresenta-se como o cibercrime cuja consumação acarreta repercussões mais gravosas, sendo suscetível de afetar a própria segurança do Estado, à semelhança do que sucede com o crime tradicional de sabotagem, consagrado no art.º 330.º do Código Penal[29].

Em Angola, ocorreram episódios recentes que corroboram esta constatação, nomeadamente os ataques informáticos perpetrados em 2019 contra a maior empresa pública do país, a Sonangol, que resultaram no colapso temporário (*shutdown*) de todo o seu aparato informático, os ataques anteriores que, em 2016, paralisaram diversos departamentos ministeriais e direções de governos provinciais por mais de 24 horas[30], e, mais recentemente, os ciberataques dirigidos à UNITEL, a maior empresa angolana de telecomunicações móveis[31].

A maioria dos atos de ciberterrorismo e de guerra cibernética (*cyberwar*)[32] traduz-se na prática deste ilícito. O crime partilha elevada similitude com o dano em

[28] ALBUQUERQUE, Paulo Pinto de; BRANCO, José (Org.). *Comentário das Leis Penais Extravagantes*. Vol. II. Lisboa: Universidade Católica Editora, 2011, p. 511. *Apud* BELO CAIÚVE, Abrantes Malaquias. *Os Crimes Informáticos*, *cit.*, p. 123.

[29] Pertence ao Capítulo I (Crimes Contra a Segurança do Estado), Secção I (Crimes Contra a Independência e a Integridade Nacionais).

[30] BELO CAIÚVE, Abrantes Malaquias. *Os Crimes Informáticos: Uma Análise ao seu Tratamento no Código Penal Angolano*. Lisboa: Lisbon International Press, 2023, pp. 28-29, 242-243.

[31] CORREIO DA KIANDA. Ataque cibernético à Unitel deve ser investigado com rigor, defendem especialistas. *Correio da Kianda*, Luanda, 1 ago. 2026. Disponível em: https://correiokianda.info/ataque-cibernetico-a-unitel-deve-ser-investigado-com-rigor-defendem-especialistas/. Acesso em: 8 ago. 2026.

[32] *Cyberwar* (também grafada como *cyber war*, *cyberwarfare* ou guerra cibernética) consiste num conflito conduzido no e a partir de computadores e redes que os conectam, desencadeado por Estados (ou seus *proxies*) contra outras nações. A guerra cibernética é maioritariamente dirigida contra redes governamentais e militares visando perturbar, destruir ou negar a sua utilização. BRAHMANAND, Pratap; OSPANOVA, A. Cyber War. *International Journal of Innovative Research in Science, Engineering and Technology*, v. 11, n. 4, pp. 3454-3462, 2022. DOI: 10.15680/IJIRSET.2022.1104015.

dados informáticos[33], comungando de grande parte dos elementos objetivos daquele tipo; a divergência primordial reside no resultado exigido, que neste caso se consubstancia no efeito de "entravar, impedir, interromper ou perturbar gravemente o funcionamento de sistema de comunicação".

Os ataques de negação de serviço (*Denial of Service* – DoS) e, em particular, os ataques distribuídos (*Distributed Denial of Service* – DDoS), "por serem uma autêntica arma eletrónica", preenchem por excelência a factualidade típica da sabotagem informática. Integram-se igualmente no escopo desta norma condutas como o *spamming*[34] e o *mail bomb*[35].

Trata-se de um crime público, cuja moldura penal abstrata fixada no Código Penal reputamos de branda e merecedora de agravamento[36]. Em termos sintéticos, a infração visa tutelar "a confiança na segurança dos sistemas e das comunicações eletrónicas"[37], não descurando a garantia da sua integridade e do seu pleno funcionamento. Embora parte da doutrina[38] advogue que a sabotagem informática visa tutelar igualmente o património, não perfilhamos inteiramente essa tese; antes sufragamos o entendimento de que, neste contexto, "o património goza de uma tutela meramente reflexa"[39].

Conquanto partilhe o *nomen iuris* do crime tradicional, a interferência informática em sistemas assume uma feição puramente tecnológica, razão pela qual reclama consagração autónoma numa Lei do Cibercrime.

A *falsidade informática*, por seu turno, atenta contra a fé pública, guardando estreita vizinhança dogmática com o crime comum de falsificação de documentos[40]

---

[33] Mantém igualmente contiguidade dogmática com a falsidade e a burla informática, podendo suscitar relações de concurso de infrações. Para uma abordagem aprofundada, *v.* VENÂNCIO, Pedro Dias. *In*: GUEDES, Inês Sousa; GOMES, Marcus Alan de Melo (Coord.). *Cibercriminalidade: Novos Desafios, Ofensas e Soluções*. 1.ª ed. Lisboa: Pactor, jul. 2021, p. 87.

[34] SANTOS, Paulo; PIMENTEL, Carlos; BESSA, Ricardo. *Cyberwar*. Lisboa: FCA, 2008, pp. 13-14.

PEREIRA, Joel Timóteo Ramos. *Direito da Internet e Comércio Electrónico*. Lisboa: Quid Juris, 2002, pp. 251-252.

[35] MARQUES, Garcia; MARTINS, Lourenço. *Direito da Informática*. 2.ª ed. refundida e atualizada. Coimbra: Almedina, 2006, p. 693.

[36] O crime tradicional de sabotagem é cominado com uma pena máxima de 15 anos de prisão; paradoxalmente, a sabotagem informática é punida com um máximo de 8 anos de prisão. Parece-nos injustificada esta disparidade sancionatória perante duas infrações suscetíveis de causar repercussões análogas na segurança do Estado.

[37] VENÂNCIO, Pedro Dias. *In*: GUEDES, Inês Sousa; GOMES, Marcus Alan de Melo. *Cibercriminalidade*, *cit.*, p. 87.

[38] Destacam-se, neste sentido: COSTA, José Francisco de Faria. Algumas reflexões sobre o estatuto dogmático do chamado "Direito Penal Informático". *In*: *Direito Penal da Comunicação*. Coimbra: Coimbra Editora, 1998, p. 110; MACEDO, João Carlos Cruz Barbosa de. Algumas considerações acerca dos crimes informáticos em Portugal. *In*: *Direito Penal Hoje: Novos Desafios e Novas Respostas*. Coimbra: Coimbra Editora, 2009, p. 245.

[39] NUNES, Duarte Alberto Rodrigues. *Os Crimes Previstos na Lei do Cibercrime e a Responsabilidade Penal dos Entes Coletivos*. 2.ª ed. Coimbra: Gestlegal, 2024, p. 263.

[40] Em virtude dessa similitude dogmática, no Anteprojeto do Código Penal o crime de falsidade informática figurava no Capítulo I, referente à "Falsificação de Documentos, Dados Informáticos e Registos Técnicos", integrado no Título III dos "Crimes Contra a Fé Pública".

(art.º 251.º). Representa um dos ilícitos virtuais mais recorrentes, cujas primeiras manifestações remontam ao surgimento da criminalidade eletrónica na década de 1960, maioritariamente associadas ao setor bancário e financeiro. Hodiernamente, a incidência deste tipo penal verifica-se, sobretudo, no uso fraudulento de cartões de pagamento ou em transações efetuadas via *internet banking*.

A *praxis* dos cibercriminosos engloba a criação de páginas web mimetizando sítios legítimos com o fito de captar dados pessoais e bancários das vítimas (*phishing*), bem como a contrafação, clonagem e posterior utilização de cartões ou dispositivos de pagamento[41]. Neste ilícito subsumem-se, ainda, a falsificação de títulos equiparados a moeda e a captura de dados bancários gravados em bandas magnéticas[42] – condutas que integram as práticas delituosas correntemente designadas por *skimming*[43] e *carding*[44].

Da análise do elemento objetivo do tipo extrai-se que a infração assenta na manipulação de dados inseridos num sistema informático ou no seu tratamento espúrio, culminando na criação de documentos ou dados falsos que abalam a confiança e a credibilidade probatória[45] no tráfico jurídico[46], em tudo idêntico ao que sucede com os documentos falsos "em sentido clássico". Constituindo a transposição da falsificação documental para a ambiência eletrónica, a falsidade informática reveste a natureza de crime informático impróprio – a informática opera meramente como um instrumento para executar uma ofensa preexistente no mundo analógico.

A doutrina e a jurisprudência[47] convergem quanto aos bens jurídicos protegidos, localizando-os na "confiança nos documentos eletrónicos e a integridade dos sistemas informáticos enquanto valores fundamentais próprios da sociedade de

[41] Abrange, igualmente, a aquisição e distribuição de *hardware* ou equipamento destinado a concretizar tais contrafações. *V.* CAIXA GERAL DE DEPÓSITOS. Lei do Cibercrime. *Saldo Positivo*. Disponível em: https://www.cgd.pt/Site/Saldo-Positivo/formacao-e-tecnologia/Pages/lei-do-cibercrime.aspx. Acesso em: 27 abr. 2024.

[42] Neste sentido, *v.* CABRAL, Nuno Alexandre Craveiro, *citado supra*.

[43] O *skimming* consubstancia a instalação sub-reptícia, em Caixas Automáticas (ATM) ou terminais de pagamento automático (TPA), de dispositivos eletrónicos ocultos concebidos para copiar e gravar os dados alojados na banda magnética dos cartões bancários neles inseridos.

[44] O *carding* traduz-se na conduta subsequente de exploração ilícita ou comercialização fraudulenta dos dados bancários adquiridos mediante a técnica de *skimming*.

[45] No ordenamento jurídico angolano, o documento informático goza de força probatória equivalente à do documento físico. O art.º 4.º, alínea p), do Decreto Presidencial n.º 202/11, de 22 de Julho (Regulamento das Tecnologias e dos Serviços da Sociedade da Informação), estatui que o documento eletrónico oferece "as mesmas garantias de fidedignidade, inteligibilidade e conservação de um documento em suporte papel".

[46] NUNES, Duarte Alberto Rodrigues. O crime de falsidade informática. *Julgar Online*, out. 2017, p. 2. Disponível em: https://www.academia.edu/36977372/O_crime_de_falsidade_informática. Acesso em: 9 jan. 2024.

[47] Sem que exista pacífica unanimidade na jurisprudência portuguesa, como atestam os Acórdãos do Tribunal da Relação do Porto de 24/04/2013 (Proc. 841/09.0PBAVR.P1) e do Tribunal da Relação de Évora de 10/05/2011 (Proc. 268/08.1TAABF-A.E1).

informação"[48]. Trata-se de um ilícito complexo que exige dolo específico e dúplice. Contudo, os seus elementos objetivos e subjetivos aproximam-se intrinsecamente dos crimes de dano e de sabotagem informática[49].

Não obstante a falsidade informática configurar um crime impróprio, a elevada probabilidade de operar em concurso com outras infrações (como o dano, a sabotagem e a burla[50]), somada à complexidade técnica do seu preenchimento típico, evidencia a necessidade de o seu regime constar de legislação extravagante.

Relativamente à *burla informática e nas comunicações*, tal como mencionado anteriormente, a Convenção de Budapeste agrupa-a conjuntamente com a falsidade informática no Título 2, referente aos ilícitos conexos com computadores, por se tratar de um crime informático impuro de elevada recorrência no ecossistema digital[51]. Efetivamente, quer a falsidade quer a burla[52] são figuras típicas tradicionais cuja fenomenologia foi exponencialmente potenciada pelo avanço das TIC.

A burla ou fraude informática é um crime contra o património no qual o agente utiliza meios computacionais para adquirir, manipular ou modificar dados eletrónicos, ou permite o uso ilegítimo de um sistema informático, alcançando "uma transferência não consentida de activos patrimoniais de outrem"[53]. Sobre a densificação dos respetivos elementos objetivos, remetemos para o magistério do Professor Oliveira de Ascensão[54]. No plano subjetivo, exige o dolo acrescido de uma intenção de enriquecimento ilegítimo, para si ou para terceiro, à custa de correlativo empobrecimento ou prejuízo na esfera patrimonial da vítima.

A burla informática tutela, em primeira linha, "a confiança social na fiabilidade e segurança dos serviços e redes das comunicações electrónicas que proporcionam vários tipos de serviços, nomeadamente no que respeita aos *modus* electrónico-digitais de pagamento".

---

[48] Na mesma esteira, VENÂNCIO, Pedro Dias. *In*: GUEDES, Inês Sousa; GOMES, Marcus Alan de Melo. *Cibercriminalidade*, *cit.*, p. 85.

[49] ALBUQUERQUE, Paulo Pinto de; BRANCO, José. *Op. cit.*, pp. 506, 508 e 509.

[50] O Acórdão do Tribunal da Relação de Évora de 25/05/2021 (Processo 82/20.9PACTX-A.E1, Relator: Martinho Cardoso) debruça-se detidamente sobre o concurso de infrações entre a falsidade informática e a burla informática. Disponível em: https://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/f490f15b8cbb90b7802586ea004dcac8. Acesso em: 27 abr. 2024.

[51] SANTOS, Rita Coelho. *O Tratamento Jurídico-Penal da Transferência de Fundos Monetários Através da Manipulação Ilícita dos Sistemas Informáticos*. Coimbra: Coimbra Editora, 2005, p. 9.

Dada a sua complementaridade na execução do crime, falsidade e burla manifestam-se frequentemente em simultaneidade. *V.* OBSERVADOR. Ministério Público acusa homem de crimes de falsidade informática, acesso ilegítimo e burlas através do MB Way. *Observador*, 15 dez. 2023. Disponível em: https://observador.pt/2023/12/15/ministerio-publico-acusa-homem-de-crimes-de-falsidade-informatica-acesso-ilegitimo-e-burlas-atraves-do-mb-way/. Acesso em: 27 abr. 2024.

[52] Sendo suscetíveis de operar em concurso efetivo ou real. *V.* Acórdão do Tribunal da Relação do Porto de 14/09/2016 (Processo 365/15.2PIPRT.P1). Disponível em: http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/6f02100f48f04ae880258045004ea54d?OpenDocument. Acesso em: 31 mar. 2024.

[53] RODRIGUES, Benjamim Silva. *Op. cit.*, p. 358.

[54] ASCENSÃO, José Oliveira de. *Op. cit.*, p. 216.

Atendendo a este nível de proteção legal, a infração verifica-se de forma flagrante em manipulações que resultam no uso abusivo de cartões de crédito ou de garantia, e prolifera atualmente nas plataformas de vendas *online* (com destaque para o OLX), onde os criminosos capitalizam o desconhecimento de alguns utilizadores acerca do funcionamento de aplicações de pagamento instantâneo (como o MB Way[55]) para consumar o desfalque patrimonial.

Embora se trate de um ilícito de danosidade patrimonial, logo, tendencialmente reparável, o legislador angolano optou por cominá-lo com a punição mais gravosa de todo o catálogo dos crimes informáticos face à dimensão dos prejuízos que frequentemente desencadeia[56]. No tocante à exigência de previsão autónoma em lei especial, valem aqui, *mutatis mutandis*, os argumentos já esgrimidos a propósito da falsidade informática.

A *reprodução ilegítima de programas de computador, bases de dados e topografia de produtos semicondutores* encerra o rol das infrações contra as comunicações e sistemas informáticos no Código Penal. Trata-se de um tipo legal de formulação ampla, que a Convenção de Budapeste agrupa sob a chancela do "uso indevido de dispositivos informáticos".

A sua incriminação obedece à necessidade de tutelar penalmente os direitos de propriedade intelectual inerentes aos bens digitais (sujeitos à voragem da pirataria), obstando à sua reprodução, divulgação, venda, comunicação ao público, transformação e circulação desautorizada. Diferentemente das infrações anteriores, o lugar sistemático adequado para este tipo penal não seria sequer uma Lei do Cibercrime, mas sim um diploma normativo dedicado aos Direitos de Autor e Direitos Conexos ou, numa perspetiva mais integradora, à Propriedade Intelectual aplicada às TIC. O ordenamento jurídico angolano ressente-se, neste domínio específico, da ausência de legislação avulsa devidamente estruturada.

A atual Lei n.º 15/14, de 31 de Julho (Lei dos Direitos de Autor e Conexos), padece de manifesta insuficiência em matéria de proteção penal[57]. O diploma assenta sobretudo em respostas de índole cível, socorrendo-se de normas de processo civil (art.º 80.º, n.º 1), estatuindo mecanismos de responsabilidade civil (art.º 81.º) e limitando o âmbito punitivo à mera aplicação de penas de multa (art.º 89.º)[58]. Sendo

[55] Práticas criminais frequentes em Portugal, sendo objeto de aturada investigação policial. *V.* PPLWARE. Alerta GNR: Usa MB Way? Atenção às burlas no OLX e Custo Justo. *Pplware*, 2020. Disponível em: https://pplware.sapo.pt/informacao/alerta-gnr-usa-mbway-atencao-as-burlas-no-olx-e-custo-justo/. Acesso em: 27 abr. 2024.

[56] No Código Penal angolano, a burla informática não dispõe de uma moldura penal própria, sendo punida por remissão para o ilícito do furto qualificado (art.º 393.º, n.º 3), cujas balizas penais de prisão se cifram em 1 a 5 anos, 3 a 8 anos ou 3 a 12 anos, em função da gravidade da conduta.

[57] Contrariamente ao que se verifica com o Código do Direito de Autor e dos Direitos Conexos português (Decreto-Lei n.º 63/85), que tipifica autonomamente os crimes e os sanciona com penas de prisão até 3 anos e multa, punindo a forma negligente e vetando a suspensão da pena em casos de reincidência (art.º 197.º).

[58] Os crimes de contrafação e plágio (art.º 85.º, n.ºs 1 e 2) carecem de regime sancionatório específico na Lei angolana, remetendo o art.º 83.º a respetiva punição para as disposições do Código Penal e do

uma matéria que excede o escopo imediato deste trabalho, abstemo-nos de aprofundar os contornos dogmáticos da reprodução ilegítima, reservando a análise da sua modelação ideal para investigações futuras.

Por fim, no vetor da proteção da infância *online*, impõe-se a análise da *pornografia infantil* (ou "pornografia de menores", segundo a nomenclatura do Código Penal português[59]). Tratando-se do único ilícito virtual não inserido no Título VIII da Parte Especial do Código Penal (encontrando-se nos crimes contra a liberdade e autodeterminação sexual), justifica-se o seu tratamento em ponto autónomo.

Qualificável como um crime relacionado com o conteúdo dos dados, visa proteger os menores[60] contra a difusão em rede de material pornográfico ou de cariz sexual, frequentemente comercializado na *dark web*. O tipo legal almeja, outrossim, o combate à agressão e aliciamento sexual levado a cabo por predadores digitais, fenómeno comummente rotulado de ciberassédio[61].

A lei penal angolana equipara a menoridade para este efeito aos indivíduos com idade inferior a dezoito anos. Face à vulnerabilidade e hiper-exposição digital desta faixa etária, a moldura penal abstrata atinge uns expressivos dez anos de prisão. O espetro da incriminação é vastíssimo: pune quem produz, distribui, difunde, transmite, importa, exporta, vende, adquire, detém ou facilita o acesso a material pornográfico de menores. Significa, portanto, que a lei penaliza inclusivamente a simples posse ou detenção desse material.

A difusão do conteúdo ilícito com finalidade lucrativa consubstancia a conduta de maior danosidade social. O art.º 199.º, n.º 1, estipula a agravação dos limites mínimo e máximo da pena num terço sempre que a vítima seja: a) Ascendente, descendente, adotante, adotado, parente ou afim até ao terceiro grau da linha colateral do agente, ou se encontre sob sua tutela ou curatela; b) Enquadrada numa relação de dependência hierárquica, económica ou laboral perante o agente, e este se aproveite dessa sujeição.

Afigura-se criticável, no entanto, que o legislador tenha suprimido a agravação especial da pena assente na idade da vítima, especificamente quando tenha menos de 14 ou 16 anos. Esta graduação da censurabilidade, que figurava no Anteprojeto de Código Penal, desapareceu do atual diploma, num silêncio legislativo de difícil justificação político-criminal.

Código de Processo Penal. Para uma análise do evoluir legislativo da Propriedade Intelectual em Angola, *v.* BELO CAIÚVE, Abrantes Malaquias. *Os Crimes Informáticos*, *cit.*, pp. 140-149.

[59] Para desenvolvimentos pormenorizados sobre o tema, *v.* BELO CAIÚVE, Abrantes Malaquias. O Tratamento Legal da Pornografia Infantil em Angola: Enquadramento Constitucional, Penal e Jurisprudencial. *Academicus Pro*, v. 4, n. 1, pp. 72-85, 2026. DOI: 10.4314/academicus.v4i1.7. Acesso em: 9 ago. 2026.

[60] Em especial a população adolescente, atenta a incidência massiva do acesso à internet através de *smartphones* e equipamentos portáteis.

[61] PEREIRA, Filipa da Silva; MATOS, Marlene. *Ciberassédio na adolescência: Prevalência(s), reações à vitimação e mediação parental*. 2015. Tese (Doutoramento em Psicologia Aplicada) – Escola de Psicologia, Universidade do Minho, Braga, 2015. Disponível em: https://hdl.handle.net/1822/42549 Acesso em: 9 ago. 2026.

Este ilícito público e doloso abrange ainda quem, mediante *download* ou procedimento análogo, "guarda no seu computador imagens de crianças do sexo masculino, nuas e em poses de exibição dos órgãos sexuais".

Como referido, ressalta a intenção do legislador de punir categoricamente a mera detenção e o acesso a tais ficheiros[62]. A pornografia infantil não constitui apenas um crime de perigo abstrato, punindo-se a conduta face à sua intrínseca "potencialidade lesiva" para com um "bem jurídico individual" (a liberdade e a autodeterminação sexual infantis), devendo efetivar-se "independentemente de ser produzida ou não" a lesão direta[63]. Nesta óptica, a incriminação contribui para o combate eficaz às práticas relacionadas com a "ciberpornografia", a prostituição juvenil e as redes de tráfico de seres humanos.

Alinhado com a perspetiva do UNICEF, o consumo e difusão de conteúdo pornográfico induzem lesões graves nos menores, desencadeando patologias de "saúde mental, sexismo e objetificação, violência sexual e outros resultados negativos". A organização insta à adoção de políticas rigorosas de restrição de acesso e fomenta a implementação de "programas de educação para crianças por meio de iniciativas baseadas na escola", mobilizando toda a comunidade docente e familiar[64].

Em suma, propugnamos que a pornografia infantil praticada através de sistemas informáticos seja integrada numa Lei do Cibercrime, atendendo a que a dispersão normativa dificulta o tratamento harmonioso de questões dogmáticas complexas, tais como a criminalização da mera posse de ficheiros temporários (*cache*) e a uniformização do limiar etário da menoridade.

3. SINOPSE DA REGULAÇÃO DOS CIBERCRIMES NA LUSOFONIA

No ordenamento jurídico português, a construção da tutela penal do ciberespaço assentou no impulso constitucional pós-revolucionário. A Constituição da República Portuguesa (CRP) de 1976 erigiu a "utilização da informática"[65] no catálogo dos Direitos, Liberdades e Garantias (art.º 35.º), sinalizando o reconhecimento do ecossistema digital e da sociedade da informação "como um novo bem jurídico com dignidade penal"[66].

[62] SILVA, João Miguel Almeida da. *Cibercrime: O Crime de Pornografia Infantil na Internet*. 2016. Dissertação (Mestrado em Ciências Jurídico-Forenses) – Faculdade de Direito, Universidade de Coimbra, Coimbra, 2016, pp. 29 e 34.

[63] SIMAS SANTOS, Manuel; LEAL-HENRIQUES, Manuel. *Apud* VARA, Marcela; SANI, Ana Isabel. *In*: GUEDES, Inês Sousa; GOMES, Marcus Alan de Melo (Coord.). *Cibercriminalidade*, *cit.*, p. 109.

[64] UNICEF BRASIL. Proteção das crianças contra os impactos nocivos da pornografia. Disponível em: https://www.unicef.org/brazil/protecao-das-criancas-contra-os-impactos-nocivos-da-pornografia. Acesso em: 1 abr. 2024.

[65] O texto constitucional de 1976 foi objeto de revisões pelas Leis Constitucionais n.º 1/82, de 30 de Setembro, n.º 1/89, de 8 de Julho, e n.º 1/92, de 30 de Setembro.

[66] VENÂNCIO, Pedro Dias. *Lições de Direito do Cibercrime e a Tutela Penal de Dados Pessoais*. Viseu: Editora d'Ideias, 2022, p. 51.

Ancorado nesse desiderato, o Código Penal aprovado pelo Decreto-Lei n.º 400/82, de 23 de Setembro[67], tipificou pioneiramente duas infrações com matriz tecnológica: a *devassa por meio da informática*[68] (art.º 181.º) e a *violação do segredo de correspondência e telecomunicações* (art.º 182.º, n.º 2).

Com o advento da Lei n.º 109/91, de 17 de Agosto (Lei da Criminalidade Informática)[69], Portugal dotou-se de um diploma especial específico, antecipando em uma década a Convenção de Budapeste. Esse diploma consagrou os tipos de falsidade informática (art.º 4.º), dano relativo a dados ou programas informáticos (art.º 5.º), sabotagem informática (art.º 6.º), acesso ilegítimo (art.º 7.º), interceção ilegítima (art.º 8.º) e reprodução ilegítima de programa protegido (art.º 9.º).

Posteriormente, a reforma do Código Penal de 1995 (operada pelo Decreto-Lei n.º 48/95, de 15 de Março) introduziu o crime de burla informática (art.º 221.º)[70]. No preâmbulo desse diploma, o legislador português justificou expressamente a opção de manter a criminalidade informática pura em legislação extravagante, invocando razões de oportunidade técnica e sistemática[71].

A consolidação do modelo especial ocorreu com a aprovação da Lei n.º 109/2009, de 15 de Setembro (Lei do Cibercrime)[72], que ratificou a Convenção de Budapeste. Ao contrário do diploma de 1991, a Lei n.º 109/2009 integrou normas de Direito substantivo (arts. 3.º a 8.º), disposições adjetivas sobre obtenção e preservação da prova digital e um regime de cooperação judiciária internacional, conferindo aos operadores judiciários os instrumentos indispensáveis para percorrer o *iter criminis*.

Mais recentemente, a Diretiva (UE) 2019/713 foi transposta para o Direito interno português pela Lei n.º 79/2021, de 24 de Novembro[73], alterando a Lei do Cibercrime, o Código Penal e o Código de Processo Penal. A revisão aditou à Lei do Cibercrime um catálogo de infrações atinentes à aquisição, contrafação e uso ilícito de instrumentos de pagamento não em numerário (arts. 3.º-A a 3.º-G), e

[67] O Código Penal aprovado pelo Decreto-Lei n.º 400/82 sucedeu ao Código de 1886, não prevendo o texto primitivo a criminalidade informática na sua dimensão atual.

[68] Conforme assinalado pelo Tribunal da Relação do Porto (Acórdão de 15/10/2008), o tipo penal de devassa por meio de informática (art.º 193.º do CP) decorre da garantia do art.º 35.º da CRP, visando proteger a esfera privada contra os riscos de discriminação emergentes do processamento automatizado de dados. Disponível em: http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/b54faf2d4330b8d480257c6e004ff2df?OpenDocument. Acesso em: 5 abr. 2024.

[69] A Lei n.º 109/91, de 17 de Agosto, constituiu o primeiro texto legislativo português exclusivamente vocacionado para a criminalidade informática, mandando aplicar subsidiariamente as regras do Código Penal (art.º 1.º).

[70] Alteração introduzida pelo Decreto-Lei n.º 48/95, de 15 de Março.

[71] Na oportunidade da reforma de 1995, o legislador remeteu para leis especiais matérias de elevada especificidade técnica, como o combate ao branqueamento de capitais e as infrações informáticas puras. ALMEIDA, Carlota Pizarro de. *Código Penal de 2010*. 15.ª ed. Coimbra: Almedina, p. 12.

[72] A Lei n.º 109/2009 revogou o diploma de 1991, procedendo à transposição da Decisão-Quadro n.º 2005/222/JAI do Conselho da União Europeia.

[73] Corresponde à segunda revisão da Lei n.º 109/2009.

reconfigurou no Código Penal o crime de burla informática (art.º 221.º) e a tutela dos cartões e dados de pagamento (art.º 225.º).

Depreende-se, pois, que o legislador português consagrou a opção por disciplinar os cibercrimes puros em diploma extravagante autónomo[74], reservando para o Código Penal apenas as infrações tradicionais executadas por meio informático.

No ordenamento jurídico brasileiro[75], a qualificação jurídica dos ilícitos cibernéticos conheceu oscilações terminológicas e doutrinárias, emergindo expressões como "crimes de informática", "crimes digitais" e "cibercrimes".

O quadro legislativo penal brasileiro adquiriu contornos específicos em 2012 com a aprovação da Lei n.º 12.737/2012 (conhecida como "Lei Carolina Dieckmann")[76], que aditou novos tipos legais ao Código Penal[77], incriminando a "invasão de dispositivo informático" e a "interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública". Simultaneamente, a Lei n.º 12.735/2012 encarregou os órgãos policiais de estruturar delegacias especializadas no combate à delinquência em rede.

No plano regulatório sobressai o Marco Civil da Internet (Lei n.º 12.965/2014), que fixou princípios e garantias para a utilização da rede no Brasil e previu salvaguardas judiciais para a remoção de conteúdos e proteção da privacidade.

No âmbito internacional, o Brasil promulgou a Convenção de Budapeste através do Decreto n.º 11.491/2021, ano em que o legislador alterou novamente o Código Penal pela Lei n.º 14.155/2021, agravando as penas dos crimes de invasão de dispositivo, furto qualificado e estelionato mediante fraude eletrónica. Por seu turno, a Lei Geral de Proteção de Dados Pessoais (Lei n.º 13.709/2018) estabeleceu sanções administrativas e regulatórias[78].

O percurso do Direito brasileiro, marcado por sucessivas e fragmentárias edições legislativas enxertadas no Código Penal de 1940, evidencia que a codificação dos ilícitos virtuais no texto comum expõe a lei penal a constantes sobressaltos e revisões, confirmando as fragilidades dessa opção num dos países com maior índice de vitimação cibernética[79].

---

[74] O Código do Direito de Autor e dos Direitos Conexos português contempla igualmente tipos incriminadores atinentes à violação de medidas tecnológicas de proteção.

[75] A dispersão terminológica é notória na doutrina brasileira, coexistindo as designações "crimes cibernéticos", "crimes digitais" e "delitos informáticos".

[76] A denominativa decorre da repercussão do caso mediático envolvendo a atriz Carolina Dieckmann, cujos ficheiros pessoais foram subtraídos e divulgados na rede.

[77] O Código Penal brasileiro foi promulgado pelo Decreto-Lei n.º 2.848, de 7 de dezembro de 1940.

[78] Para uma análise do impacto da LGPD na repressão do cibercrime no Brasil, *v.* SILVA, Ronaldo Couto da; NOVAIS, Thyara Gonçalves. A Lei Geral de Proteção de Dados e sua aplicação no combate aos crimes cibernéticos: desafios e perspectivas. *Revista Ibero-Americana de Humanidades, Ciências e Educação*, São Paulo, v. 9, n. 10, out. 2023.

[79] Segundo o *Relatório Anual de Cibersegurança de 2022* da ClearSale, o Brasil figurou como o 5.º país mais afetado por ciberataques a nível global e o 2.º na América Latina. Disponíveis em: https://recursos.clear.sale/relat%C3%B3rio-anual-de-ciberseguran%C3%A7a-2022 e

No tocante aos países africanos de língua oficial portuguesa (PALOP), observa-se uma nítida clivagem metodológica.

Cabo Verde destaca-se por ostentar o quadro normativo mais harmonizado da região[80]. Após ratificar a Convenção de Budapeste[81], aprovou a Lei do Cibercrime (Lei n.º 08/IX/2017)[82], que contempla os tipos penais materiais (falsidade, dano, sabotagem, acesso e interceção ilícitos, uso indevido de dispositivos e pornografia infantil), normas adjetivas de prova digital e regras de cooperação internacional.

O diploma cabo-verdiano distingue-se por incriminar autonomamente a "pornografia de vingança" (*revenge porn*, no art.º 10.º)[83], tutelando a honra, a imagem e a intimidade das vítimas[84] perante a difusão não consentida de conteúdos íntimos por ex-parceiros afetivos.

O Código Penal de Cabo Verde de 2004 retém no seu texto os crimes contra a reserva da vida privada – atentado à intimidade (art.º 183.º), tratamento informático ilegal (art.º 187.º)[85], devassa por meio de informática (art.º 188.º) e violação de segredo (art.º 189.º) –, bem como a burla informática (art.º 212.º), prevendo ainda a Lei n.º 133/V/2001 (alterada pela Lei n.º 41/VIII/2013) ilícitos administrativos de proteção de dados[86]. A adesão à Convenção de Malabo da União Africana (Resolução n.º 153/IX/2020)[87] reforçou esse alinhamento internacional.

Na República da Guiné-Bissau, regista-se um quadro de omissão legislativa. O Código Penal (Decreto-Lei n.º 4/93) carece de atualização, subsistindo uma ausência

https://olhardigital.com.br/2024/02/02/seguranca/brasil-e-o-segundo-maior-alvo-de-crimes-ciberneticos-na-america-latina/. Acessos em: 22 abr. 2024.

[80] Cabo Verde figura em posição de relevo no *Global Cybersecurity Index* da União Internacional de Telecomunicações (ITU). Disponível em: https://www.mf.gov.cv/-/cabo-verde-sobe-27-posi%C3%A7%C3%B5es-no-%C3%ADndice-global-de-ciberseguran%C3%A7a-itu-. Acesso em: 19 abr. 2024.

[81] A adesão foi formalizada em 19/06/2018, vigorando desde 01/10/2018.

[82] A aprovação da lei cabo-verdiana foi noticiada no espaço angolano pela Agência Angola Press (ANGOP) em 25 de novembro de 2016. Disponível em: https://www.angop.ao/angola/pt_pt/noticias/africa/2016/10/47/Cabo-Verde-Assembleia-aprova-lei-sobre-cyber-crime-recolha-provas-suporte-electronico,a67d4fa8-2dbc-47f9-bd63-270396e8c681.html. Acesso em: 1 abr. 2024.

[83] Ao contrário de Portugal e do Brasil, que tratam a matéria no Código Penal.

[84]Sobre a dimensão cível e criminal da pornografia de vingança, *v.* SANTOS, Mikaelle Silva; OLIVEIRA, Tanira Alves Novaes de. Pornografia de vingança: a responsabilidade civil e penal pelo dano à honra, à imagem e à intimidade das vítimas. *Ciências Sociais Aplicadas*, n. 127, out. 2023.

[85] A nosso ver, a previsão autónoma do "tratamento informático ilegal" no art.º 187.º do CP cabo-verdiano é redutora, uma vez que a conduta se subsume nas infrações gerais da lei do cibercrime e da lei de proteção de dados.

[86] Disponível em: https://sniac.cv/wp-content/uploads/2018/03/SNIAC-Lei-nº-43-VIII-2013-Cria-e-Regula-SNIAC.pdf. Acesso em: 19 set. 2023.

V. EXPRESSO DAS ILHAS. Cibercrime: legislação evolui, mas tecnologia é mais rápida. *Expresso das Ilhas*, 12 out. 2018. Disponível em: https://expressodasilhas.cv/eitec/2018/10/12/cibercrime-legislacao-evolui-mas-tecnologia-e-mais-rapida/60468. Acesso em: 27 out. 2023.

[87] A Resolução n.º 153/IX/2020 foi aprovada em 17 de março. Disponível em: https://www.nosi.cv/index.php/pt/noticias/item/804-ciberseguranca-cabo-verde-aprova-resolucao-para-adesao-a-convencao-de-malabo. Acesso em: 10 abr. 2024.

de tipificação dos ilícitos cibernéticos. A própria Lei de Base das Tecnologias de Informação e Comunicação (Lei n.º 5/2010) e a falta de adesão à Convenção de Malabo confirmam a necessidade de reformas profundas com o apoio da comunidade lusófona.

O modelo adotado por Moçambique[88] aproxima-se da opção angolana ao integrar os tipos penais informáticos no texto do Código Penal de 2014: violação de correspondência (art.º 253.º), uso indevido de base de dados automatizada (art.º 254.º)[89], acesso ilegítimo (art.º 256.º), burla informática (art.º 289.º), falsidade informática (art.º 336.º), interferência em dados (art.º 337.º), interferência em sistemas (art.º 338.º), uso abusivo de dispositivo (art.º 339.º)[90] e pornografia de menores (art.º 213.º). No plano regional, Moçambique ratificou a Convenção de Malabo pela Resolução n.º 5/2019[91].

A República Democrática de São Tomé e Príncipe[92] aderiu à Convenção de Budapeste em 2017[93] e aprovou a sua Lei sobre o Cibercrime (Lei n.º 15/2017)[94]. O diploma especial prevê a falsidade, o dano, a sabotagem, o acesso e a interceção ilícitos, a reprodução ilegítima e a inserção de dados falsos (arts. 4.º a 10.º)[95], mantendo no Código Penal a pornografia de menores (art.º 180.º), a devassa informática (art.º 202.º), a violação de segredo (art.º 203.º) e a burla informática (art.º 240.º).

Sintetizando a panorama jurídico da lusofonia, sobressai a preferência clara pela aprovação de uma lei especial extravagante para sediar os ilícitos cibernéticos puros (como sucede em Portugal, Cabo Verde e São Tomé e Príncipe), reservando-se para

[88] A Lei das Telecomunicações moçambicana (Lei n.º 4/2016, de 3 de Junho) prevê infrações nos arts. 56.º a 59.º; por seu turno, a Lei das Transacções Electrónicas (Lei n.º 3/2017) não estabelece sanções penais. Disponíveis em: https://archive.gazettes.africa/archive/mz/2016/mz-government-gazette-series-i-dated-2016-06-03-no-66.pdf e https://www.oam.org.mz/wp-content/uploads/2017/07/Lei-das-Transaccoes-eletronicas.pdf. Acessos em: 10 e 15 abr. 2024.

[89] A expressão "base de dados automatizada" (art.º 254.º do CP moçambicano) afigura-se imperfeita, visando incriminar o uso indevido dessas bases.

[90] À exceção da falsidade, os ilícitos dos arts. 337.º a 339.º podem consumar-se sem falsificação documental, sendo discutível a sua inserção nos crimes contra a fé pública.

[91] PIRES, Vanessa; TANGUNE, Geth dos Santos. Crimes cibernéticos e segurança cibernética em Moçambique. *Vida Judiciária*, n. 226, pp. 42-43, nov./dez. 2022.

[92] Para um estudo sobre o ordenamento são-tomense, *v.* GRAÇA, Alciano Pereira da. *O Cibercrime em São Tomé e Príncipe: Enquadramento Jurídico-Penal do Crime de Burla Informática*. 2018. Trabalho de Conclusão de Curso – Universidade Lusíada de São Tomé e Príncipe, São Tomé, 2018.

[93] A adesão formal à Convenção de Budapeste foi acompanhada por ações de cooperação técnica dirigidas pelo Ministério Público português. Disponível em: https://cibercrime.ministeriopublico.pt/pagina/cooperacao-com-o-ministerio-publico-de-sao-tome-e-principe. Acesso em: 19 abr. 2024.

[94] Disponível em: http://cipstp.st/wp-content/uploads/2018/03/Lei_15_2017-Lei-sobre-Cibercrime.pdf. Acesso em: 16 abr. 2024.

A Lei n.º 15/2017 estrutura-se em cinco capítulos: 1. Objeto e definições; 2. Disposições penais materiais; 3. Disposições processuais; 4. Cooperação internacional; 5. Disposições finais e transitórias.

[95] Tratando-se da viciação de dados pessoais, a incriminação encontraria sede adequada na legislação sobre proteção de dados pessoais.

a codificação penal comum unicamente os crimes impróprios que atingem diretamente a reserva da vida privada e o património.

4. CONSIDERAÇÕES FINAIS E RECOMENDAÇÕES

O presente estudo procurou analisar criticamente, sob a perspetiva da dogmática penal e do Direito comparado, a opção adotada pelo legislador angolano ao incorporar a globalidade dos crimes informáticos no Título VIII da Parte Especial do Código Penal de 2020 (Lei n.º 38/20).

A análise conduzida autoriza o enunciado das seguintes conclusões e recomendações de política criminal:

1. **Reconhecimento da Emergência Regulatória:** A consolidação da sociedade da informação em Angola justificou a intervenção do legislador penal para tutelar novos bens jurídicos associados ao uso da tecnologia. Contudo, a inclusão indistinta desses ilícitos no Código Penal aproxima Angola de soluções menos funcionais, a exemplo do que sucede em Moçambique e no Brasil.

2. **Distinção entre Crimes Puros e Impróprios:** A dogmática penal e a *praxis* internacional aconselham a separação dos ilícitos. Enquanto os crimes informáticos impróprios (como a devassa por meio de informática e a burla informática) justificam a sua permanência no Código Penal por tutelarem diretamente a reserva da vida privada e o património, os crimes informáticos puros (acesso ilegítimo, interceção, dano, sabotagem e falsidade informática) exigem acolhimento em diploma especial autónomo.

3. **Autonomização da Devassa e do Acesso Ilegítimo:** A aglutinação do acesso ilegítimo (n.ºs 1 e 2) e da devassa informática (n.º 4) num único preceito legal (art.º 438.º do CP) constitui uma impropriedade sistemática. Impõe-se a sua autonomização formal, transferindo o acesso ilegítimo para a Lei Especial do Cibercrime e mantendo a devassa no capítulo dos crimes contra a reserva da vida privada do Código Penal.

4. **Reserva da Propriedade Intelectual e Dados Pessoais:** O crime de reprodução ilegítima de programas e bases de dados (art.º 444.º do CP) deve ser objeto de disciplina em legislação específica sobre Direitos de Autor e Propriedade Intelectual. Por seu turno, a proteção contra o tratamento não autorizado de dados pessoais exige articulação harmoniosa entre a Lei n.º 22/11 (LPDP) e o regime penal.

5. **Dificuldades na Conceituação e Estabilidade da Codificação:** O conceito de crime informático encontra-se em constante transformação. Como adverte a doutrina especializada, estando a criminalidade informática sujeita a uma "constante e aceleradíssima mutação tecnológica, melhor ficaria numa lei avulsa do que num Código, que deve, por definição, ser poupado a revisões frequentes"[96].

[96] BARREIROS, José Antonio. *Apud* RODRIGUES, Benjamim Silva. *Op. cit.*, p. 462.

6. **Proposta de Aprovação de uma Lei Especial do Cibercrime:** Recomenda-se ao legislador angolano a autonomização dos crimes informáticos puros numa Lei do Cibercrime, complementada por disposições adjetivas sobre obtenção e preservação da prova digital e por mecanismos operacionais de cooperação judiciária internacional (em conformidade com as diretrizes da Convenção de Budapeste e da Convenção de Malabo).

REFERÊNCIAS

ALBUQUERQUE, Paulo Pinto de; BRANCO, José (Org.). (2011). *Comentário das Leis Penais Extravagantes*. Vol. II. Lisboa: Universidade Católica Editora.

ALMEIDA, Carlota Pizarro de. (2010). *Código Penal de 2010*. 15.ª ed. Coimbra: Almedina.

ASCENSÃO, José de Oliveira. (2001). Criminalidade informática. *In*: *Direito da Sociedade da Informação*. Vol. II. Coimbra: Coimbra Editora, pp. 215-265.

BELO CAIÚVE, Abrantes Malaquias. (2020). *A problemática da regulação dos crimes informáticos na proposta de lei do Código Penal angolano e a sua conformidade com a Convenção de Budapeste sobre o cibercrime*. Dissertação (Mestrado em Direito e Informática) – Escola de Direito, Universidade do Minho, Braga. Disponível em: https://repositorium.uminho.pt/handle/1822/68832. Acesso em: 15 fev. 2024.

BELO CAIÚVE, Abrantes Malaquias. (2023). *Os Crimes Informáticos: Uma análise ao seu tratamento no Código Penal Angolano*. Lisboa: Lisbon International Press.

BELO CAIÚVE, Abrantes Malaquias. (2026). O Tratamento Legal da Pornografia Infantil em Angola: Enquadramento Constitucional, Penal e Jurisprudencial. *Academicus Pro*, v. 4, n. 1, pp. 72-85. DOI: https://dx.doi.org/10.4314/academicus.v4i1.7.

BRAHMANAND, Pratap; OSPANOVA, A. (2022). Cyber War. *International Journal of Innovative Research in Science, Engineering and Technology*, v. 11, n. 4, pp. 3454-3462. DOI: <10.15680/IJIRSET.2022.1104015>.

BRITO, Auriney Uchoa de. (2013). *Direito Penal Informático*. 1.ª ed. São Paulo: Saraiva.

CABRAL, Nuno Alexandre Craveiro. (2019). *A problemática do concurso de normas no âmbito da criminalidade informática: a falsidade informática (Art.º 3.º da Lei 109/2009, de 15 de Setembro, e os Artigos 267.º e 262.º, ambos do Código Penal)*. Dissertação (Mestrado em Direito e Prática Jurídica) – Faculdade de Direito, Universidade de Lisboa, Lisboa. Disponível em: http://hdl.handle.net/10451/44510. Acesso em: 10 jan. 2024.

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

CORREIO DA KIANDA. (2026). Ataque cibernético à Unitel deve ser investigado com rigor, defendem especialistas. *Correio da Kianda*, Luanda, 1 ago. 2026. Disponível em: https://correiokianda.info/ataque-cibernetico-a-unitel-deve-ser-investigado-com-rigor-defendem-especialistas/. Acesso em: 8 ago. 2026.

COSTA, José Francisco de Faria. (1998). Algumas reflexões sobre o estatuto dogmático do chamado "Direito penal informático". *In*: *Direito Penal da Comunicação*. Coimbra: Coimbra Editora, pp. 101-125.

CUNHA, Jelssimi Moisés da. (2020). *Os crimes informáticos no direito penal angolano*. Luanda: JuLaw. Disponível em: https://julaw.ao/wp-content/uploads/2020/11/JELSSIMI-DA-CUNHA_OS-CRIMES-INFORMATICOS-NO-DIREITO-PENAL-ANGOLANO_JULAW.pdf. Acesso em: 28 mar. 2024.

GRAÇA, Alciano Pereira da. (2018). *O Cibercrime em São Tomé e Príncipe: Enquadramento Jurídico-Penal do Crime de Burla Informática*. Trabalho de Conclusão de Curso (Licenciatura em Direito) – Universidade Lusíada de São Tomé e Príncipe, São Tomé.

GUEDES, Inês Sousa; GOMES, Marcus Alan de Melo (Coord.). (2021). *Cibercriminalidade: Novos desafios, ofensas e soluções*. 1.ª ed. Lisboa: Pactor.

JESUS, Damásio de; MILAGRES, José António. (2016). *Manual de Crimes Informáticos*. São Paulo: Saraiva.

MACEDO, João Carlos Cruz Barbosa de. (2009). Algumas considerações acerca dos crimes informáticos em Portugal. *In*: *Direito Penal Hoje: Novos Desafios e Novas Respostas*. Coimbra: Coimbra Editora, pp. 235-255.

MARQUES, J. Garcia; MARTINS, Lourenço. (2006). *Direito da Informática*. 2.ª ed. refundida e atualizada. Coimbra: Almedina.

NUNES, Duarte Alberto Rodrigues. (2017). O crime de falsidade informática. *Julgar Online*, out. 2017. Disponível em: https://www.academia.edu/36977372/O_crime_de_falsidade_informática. Acesso em: 9 jan. 2024.

NUNES, Duarte Alberto Rodrigues. (2018). O crime de dano relativo a programas ou outros dados informáticos. *Revista do Ministério Público*, Lisboa, ano 39, n.º 153, pp. 141-165, jan./mar. 2018. Disponível em: https://rmp.smmp.pt/wp-content/uploads/2018/04/6.RMP_153_NET_Duarte_Nunes.pdf. Acesso em: 9 ago. 2026.

NUNES, Duarte Alberto Rodrigues. (2024). *Os crimes previstos na Lei do Cibercrime e a responsabilidade penal dos entes coletivos*. 2.ª ed. Coimbra: Gestlegal.

PEREIRA, Alexandre Dias. (2017). *Direito da Informática (Estudos)*. Vol. I. Coimbra: Faculdade de Direito da Universidade de Coimbra.

PEREIRA, Filipa da Silva; MATOS, Marlene. (2015). *Ciberassédio na adolescência: Prevalência(s), reações à vitimação e mediação parental*. Tese (Doutoramento em Psicologia Aplicada) – Escola de Psicologia, Universidade do Minho, Braga. Disponível em: https://hdl.handle.net/1822/42549.

PEREIRA, Joel Timóteo Ramos. (2002). *Direito da Internet e Comércio Electrónico*. Lisboa: Quid Juris.

PIRES, Vanessa; TANGUNE, Geth dos Santos. (2022). Crimes cibernéticos e segurança cibernética em Moçambique. *Vida Judiciária*, n.º 226, pp. 42-43, nov./dez. 2022.

RODRIGUES, Benjamim Silva. (2009). *Direito Penal - Parte Especial: Direito Penal Informático-Digital*. Tomo I-D. Coimbra: Coimbra Editora.

SANTOS, Mikaelle Silva; OLIVEIRA, Tanira Alves Novaes de. (2023). Pornografia de vingança: a responsabilidade civil e penal pelo dano à honra, à imagem e à intimidade das vítimas. *Ciências Sociais Aplicadas*, n.º 127, out. 2023.

SANTOS, Paulo; PIMENTEL, Carlos; BESSA, Ricardo. (2008). *Cyberwar*. Lisboa: FCA.

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

SILVA, João Miguel Almeida da. (2016). *Cibercrime: O Crime de Pornografia Infantil na Internet*. Dissertação (Mestrado em Ciências Jurídico-Forenses) – Faculdade de Direito, Universidade de Coimbra, Coimbra. Disponível em: https://estudogeral.uc.pt/bitstream/10316/34801/1/Cibercrime_o%20Crime%20de%20Pornografia%20Infantil%20na%20Internet.pdf. Acesso em: 9 ago. 2026.

SILVA, Ronaldo Couto da & NOVAIS, Thyara Gonçalves. (2023). A lei geral de proteção de dados e sua aplicação no combate aos crimes cibernéticos: desafios e perspectivas. Revista Ibero-Americana de Humanidades, Ciências e Educação- REASE. São Paulo, v.9.n.10. out. 2023. ISSN - 2675 – 3375. DOI: https://doi.org/10.51891/rease.v9i10.12254

VENÂNCIO, Pedro Dias. (2022). *Lições de Direito do Cibercrime e a Tutela Penal de Dados Pessoais*. 1.ª ed. Viseu: Editora d'Ideias.

ABRANTES MALAQUIAS BELO CAIÚVE