doi.org/10.51891/rease.v12i8.29772

A INCERTEZA TÉCNICA E A HERMENÊUTICA JURÍDICO-PENAL NA CIBERSEGURANÇA: ANÁLISE DOGMÁTICA E TECNOLÓGICA DO INCIDENTE DE REDES NA UNITEL SOB A ÓTICA DA GOVERNANÇA DE TECNOLOGIA DA INFORMAÇÃO E DO DIREITO PENAL ECONÓMICO ANGOLANO.

TECHNOLOGICAL UNCERTAINTY AND LEGAL-PENAL HERMENEUTICS IN CYBERSECURITY: DOGMATIC AND TECHNOLOGICAL ANALYSIS OF THE NETWORK INCIDENT AT UNITEL FROM THE PERSPECTIVE OF INFORMATION TECHNOLOGY GOVERNANCE AND ANGOLAN ECONOMIC CRIMINAL LAW.

LA INCERTIDUMBRE TÉCNICA Y LA HERMENÉUTICA JURÍDICO-PENAL EN LA CIBERSEGURIDAD: ANÁLISIS DOGMÁTICO Y TECNOLÓGICO DEL INCIDENTE DE REDES EN UNITEL DESDE LA PERSPECTIVA DE LA GOBERNANZA DE TECNOLOGÍA DE LA INFORMACIÓN Y DEL DERECHO PENAL ECONÓMICO ANGOLANO.

Joaquim Afonso Mucuambi[1]

RESUMO: Esse artigo buscou analisar a complexa intersecção entre a investigação forense computacional e a hermenêutica jurídico-penal no âmbito dos crimes cibernéticos contra infraestruturas críticas de informação. Tomando como estudo de caso a interrupção massiva de serviços sofrida pela operadora UNITEL em Angola, o trabalho examina o hiato epistemológico entre o tempo de resposta da engenharia informática caraterizado pela incerteza inicial e opacidade dos rastos digitais e a exigência de imputação causal e subjetiva do Direito Penal Económico. A metodologia adotou uma abordagem qualitativa, exploratória e analítico-dedutiva, combinando revisão documental e análise dogmático-tecnológica do quadro legislativo angolano. Os resultados demonstram que a elaboração e interpretação da Lei dos Crimes Cibernéticos angolana por juristas sem acoplagem técnica com a Governança de Tecnologias de Informação (TI) resulta em riscos de desfasamento tipológico, ineficácia punitiva e violações às garantias processuais basilares. Conclui-se pela urgência de formulação de um modelo de hermenêutica interdisciplinar que integre os padrões internacionais de cibersegurança e a prova digital ao devido processo penal em Angola.

Palavras-chave: Cibersegurança. Hermenêutica Jurídica. Direito Penal Económico. Forense Digital. Infraestruturas Críticas.

[1]Doutorando em Projetos; (Ph.D. Candidato); Linha de Pesquisa TIC; Docente Universitário Colaborador a mais de 15 anos pelo Instituto Superior Politécnico Gregório Semedo, Universidad Internacional Iberoamericana - UNINI, México, no âmbito do convênio com a Universidade Internacional do CUANZA (UNIC - Bié, Angola).

ABSTRACT: This article aims to analyze the complex intersection between digital forensics investigation and legal-penal hermeneutics within cybercrime targeting critical information infrastructures. Using the massive service outage experienced by telecommunications operator UNITEL in Angola as a case study, this research examines the epistemological gap between computer engineering response time characterized by initial uncertainty and digital footprint opacity and the requirements of causal and subjective attribution in Economic Criminal Law. The methodology adopted a qualitative, exploratory, and analytical-deductive approach, combining legal and documentary analysis with a dogmatic-technological study of the Angolan legal framework. Results demonstrate that drafting and interpreting Angolan cybercrime legislation by legal scholars without technical coupling with Information Technology (IT) Governance leads to typological mismatches, punitive ineffectiveness, and violations of fundamental procedural guarantees. The study concludes with the urgent need for an interdisciplinary hermeneutic model integrating international cybersecurity standards and digital evidence into due criminal process.

Keywords: Cybersecurity. Legal Hermeneutics. Economic Criminal Law. Digital Forensics. Critical Infrastructures.

RESUMEN: Este artículo pretendió analizar la compleja intersección entre la investigación forense computacional y la hermenéutica jurídico-penal en el ámbito de los delitos cibernéticos contra infraestructuras críticas de información. Tomando como estudio de caso la interrupción masiva de servicios sufrida por la operadora UNITEL en Angola, el trabajo examina la brecha epistemológica entre el tiempo de respuesta de la ingeniería informática caracterizado por la incertidumbre inicial y la opacidad de las huellas digitales y la exigencia de imputación causal y subjetiva del Derecho Penal Económico. La metodología adoptó un enfoque cualitativo, exploratorio y analítico-deductivo, combinando la revisión documental y el análisis dogmático-tecnológico del marco legislativo angoleño. Los resultados demuestran que la elaboración e interpretación de la Ley de Delitos Cibernéticos angoleña por parte de juristas sin acoplamiento técnico con la Gobernanza de Tecnologías de la Información (TI) genera riesgos de desfase tipológico, ineficacia punitiva y violaciones a las garantías procesales fundamentales. Se concluye sobre la urgencia de formular un modelo de hermenéutica interdisciplinaria que integre los estándares internacionales de ciberseguridad y la prueba digital al debido proceso penal en Angola.

Palabras clave: Ciberseguridad. Hermenéutica jurídica. Derecho Penal Económico. Forense Digital. Infraestructuras Críticas.

INTRODUÇÃO

A constante digitalização do tecido socioeconómico e a consolidação de infraestruturas críticas de informação transformaram a cibersegurança de uma mera exigência operacional de Tecnologia da Informação (TI) num pilar estratégico da segurança nacional e da estabilidade económica de Estados soberanos (ENISA, 2023; NIST, 2024). Em ecossistemas de telecomunicações modernos, qualquer disrupção funcional gera impactos em cadeia que transbordam o meio estritamente tecnológico, atingindo transações financeiras, serviços

governamentais e os direitos fundamentais dos cidadãos à comunicação e ao livre desenvolvimento da personalidade.

Em Angola, a gravidade e magnitude do incidente de redes que resultou na interrupção prolongada e severa dos serviços prestados pela operadora de telecomunicações UNITEL evidenciaram não apenas a vulnerabilidade técnica dos sistemas de suporte à vida económica, mas também um hiato epistemológico profundo entre a engenharia de redes e a ciência jurídica. No calor do incidente, emergiu a expetativa mediática, social e institucional de um diagnóstico imediato por parte dos peritos e engenheiros informáticos. Todavia, essa expetativa fundamenta-se num mito positivista de omnisciência técnica que desconhece completamente a realidade operacional da forense computacional (CASEY E, 2021; ITU, 2022).

Paralelamente, o reforço legislativo angolano em matéria de repressão dos crimes informáticos impulsionado pelo quadro legal nacional sobre criminalidade cibernética, pela Lei n.º 22/11 (Lei das Comunicações Eletrónicas) e pelo alinhamento com a Convenção da União Africana sobre Cibersegurança e Proteção de Dados Pessoais (Convenção de Malabo) traz o desafio da construção normativa e hermenêutica levada a cabo predominantemente por juristas e legisladores. Sem uma simbiose efetiva com os princípios de Governança de TI e com o Direito Penal Económico contemporâneo, a aplicação de normas penais corre o risco de estagnar na ineficácia penal ou incorrer em violações a garantias processuais e constitucionais basilares, como o princípio da culpabilidade e a presunção de inocência (SIEBER U, 2020; SILVA AP, 2024).

O presente trabalho pretende responder à seguinte questão central: Como deve a hermenêutica jurídico-penal harmonizar-se com a inerente incerteza técnica da forense digital na investigação de ataques a infraestruturas críticas de telecomunicações?

METODOLOGIA

Para o desenvolvimento da presente investigação, adotou-se a metodologia qualitativa, de índole exploratória, descritiva e analítico-dedutiva. A abordagem combina a análise documental e legislativa do quadro jurídico angolano e internacional com o estudo de caso dogmático-tecnológico relativo ao incidente de redes ocorrido na UNITEL.

Realizou-se uma revisão bibliográfica sistemática com foco na literatura académica e relatórios institucionais publicados entre 2020 e 2026 nas áreas de Cibersegurança, Governança de TI, Direito Penal Económico e Processo Penal Digital. As fontes de dados primárias e

secundárias englobam textos normativos nacionais (Constituição da República de Angola - CRA, Código Penal Angolano, Lei dos Crimes Cibernéticos), standards internacionais de segurança e governança (ISO/IEC 27001:2022, ISO/IEC 27037:2021, COBIT 2019, NIST CSF 2.0) e relatórios de organismos multilaterais como a European Union Agency for Cybersecurity (ENISA) e a International Telecommunication Union (ITU).

A análise analítico-dedutiva permitiu examinar a assimetria entre as fases temporais da resposta técnica efetuada pelas equipas de TI e as exigências do processo penal angolano, identificando as lacunas do juízo de imputação subjetiva e objetiva.

2. FUNDAMENTAÇÃO TEÓRICA E REVISÃO DA LITERATURA (2020–2026)

2.1. O Estado da Arte da Cibersegurança em Infraestruturas Críticas

De acordo com o ENISA Threat Landscape 2024, os ataques perpetrados contra operadoras de telecomunicações e infraestruturas críticas evoluíram de incidentes isolados para operações altamente sofisticadas conduzidas por atores estatais (nation-state actors) ou grupos de crime organizado cibernético (ENISA, 2024). A adoção de arquiteturas Zero Trust e quadros de governança como o NIST Cybersecurity Framework 2.0 (NIST, 2024) reflete a mudança de paradigma da "defesa de perímetro" para o pressuposto da intrusão continuada (assume breach).

Neste contexto, as redes de telecomunicações modernas de quinta geração (5G) e as infraestruturas de suporte a dados lidam com superfícies de ataque exponencialmente expandidas. A resiliência operacional exige uma visão sistémica de Governança de TI que integre mecanismos de deteção precoce, planos de continuidade de negócio (Business Continuity Management) e gestão de riscos cibernéticos em conformidade com standards internacionais como ISO/IEC 27001:2022 e COBIT 2019 (ISACA, 2021). A Governança de TI não é apenas uma atividade operacional, mas sim uma função estratégica de liderança que garante o alinhamento entre a tecnologia, a conformidade legal (compliance) e os objetivos do negócio.

2.2. A Forense Digital e a Epistemologia da Incerteza Inicial

A investigação de cenários avançados de invasão cibernética exige o cumprimento de rigorosos protocolos de recolha, preservação e análise de evidências digitais (ISO/IEC 27037:2021; CASEY E, 2021).

Conforme demonstram pesquisas recentes no âmbito da digital forensics, os atacantes empregam técnicas avançadas de anti-forense (log wiping, cifragem de artefactos, fragmentação de tráfego, uso de malware residente em memória volátil) que tornam a delimitação dos danos e a atribuição da autoria um processo lento, gradual e probabilístico (HORSMAN G, 2022; CARRIER B, 2023).

Portanto, a suposição de que a engenharia de redes dispõe de um "conhecimento absoluto" no momento pós-incidente é uma falácia técnica.

A resposta a incidentes opera sob um elevado grau de incerteza, onde a hipótese inicial de falha de hardware ou erro de configuração pode levar dias até ser confirmada como uma intrusão maliciosa complexa (GARTNER, 2023). Essa incerteza empírica inicial decorre da volatilidade dos dados e da opacidade dos rastos deixados no espaço cibernético.

2.3. Hermenêutica Jurídica e Direito Penal Económico no Meio Digital

No domínio do Direito Penal Económico e da Criminalidade Informática, autores como Sieber (2020) e Brenner (2021) enfatizam que os tipos penais tradicionais sofrem de uma desadequação estrutural frente a condutas desmaterializadas (BRENNER SW, 2021; SIEBER U, 2020). A dogmática penal angolana, ao abraçar a proteção de bens jurídicos suprasingulares tais como a integridade dos sistemas de informação, a funcionalidade do mercado financeiro digital e a estabilidade da economia nacional, exige uma reinterpretação dos conceitos de dolo, conduta omitida e imputação objetiva do resultado (CANESTRARO MH e VIANNA RL, 2023; SILVA AP, 2024).

A hermenêutica penal, quando efetuada por juristas sem o devido suporte do conhecimento computacional, incorre na rigidez dogmática, desconsiderando a volatilidade da prova digital e o nexo de causalidade complexo exigido no processo penal. A mera verificação de um dano técnico ou de uma interrupção de serviço não pode levar à presunção automática de responsabilidade criminal dos administradores ou técnicos de TI, sob pena de violação do princípio da culpabilidade (CANESTRARO MH e VIANNA RL, 2023).

3. RESULTADOS E DISCUSSÃO

3.1. A Anatomia do Incidente na UNITEL e a Visibilidade Técnica Limitada

O ataque que resultou na paralisação dos serviços da UNITEL expôs a complexidade inerente à identificação imediata dos vetores de intrusão. No momento do apagão informático,

a expetativa da sociedade civil, dos meios de comunicação social e dos órgãos reguladores por respostas instantâneas esbarrou na limitação técnica da equipa de resposta a incidentes (CERT/CSIRT).

Na fase embrionária do incidente, os engenheiros de rede dedicam-se prioritariamente ao isolamento do tráfego malicioso e ao restabelecimento das comunicações essenciais, sem que haja clareza se o evento resultou de uma falha física de infraestrutura, de um erro humano na gestão de rotas de navegação ou de uma intrusão cibernética intencional dirigida. Conforme demonstrado na Tabela 1, existe uma assimetria incontornável e um hiato temporal entre o tempo técnico da forense digital e o tempo institucional das exigências jurídicas.

Tabela 1 - Comparativo Temporal entre Resposta Técnica Forense e Exigências Jurídico - Processuais.

Fase do Incidente	Ação Técnica Forense (Tecnologia da Informação / Cibersegurança)	Exigência Jurídico-Penal / Processual
0 a 48 Horas (Contenção)	Isolamento de segmentos de rede; mitigação de danos; incerteza total sobre o vetor inicial.	Abertura de inquérito; presunção de culpa ou falha operacional por órgãos de tutela.
3 a 15 Dias (Triagem)	Análise de memória volátil (RAM) e artefactos de disco; recolha de logs dispersos.	Exigência de qualificação dos danos e imputação inicial de responsabilidade civil/penal.
30+ Dias (Atribuição)	Reconstrução do plano de ataque; tentativa de correlação IP/MAC; relatório de atribuição.	Formulação da acusação penal; verificação do nexo causal e do dolo eventual.

Fonte: Própria do Autor.

A análise da Tabela 1 comprova que a tentativa de qualificação jurídica ou de imputação penal nas primeiras 48 horas opera num vazio factual probatório.

A pressa institucional por respostas tende a penalizar indevidamente a equipa de resposta ou a formular acusações açodadas com base em meras conjeturas.

3.2. A Hermenêutica dos Juristas e o Risco de Desfasamento com a Engenharia

A aprovação da legislação referente aos crimes de cibersegurança em Angola representa um avanço inquestionável no combate à criminalidade tecnológica. No entanto, a sua hermenêutica tem sido construída quase exclusivamente por juristas, sem a acoplagem dos conceitos normativos às especificidades operacionais das redes de computadores. Esta desconexão manifesta-se em três eixos dogmáticos fulcrais:

I. O Tipo Subjetivo no Direito Penal Económico

Determinar a existência de dolo (direto ou eventual) ou negligência em ambientes onde o ataque se processa por meio de automação e inteligência artificial exige entender se a vulnerabilidade explorada decorria de um erro imperdoável ou de um zero-day exploit imprevisível (SILVA AP, 2024). Se a vulnerabilidade era completamente desconhecida no estado da arte da engenharia informática, não há que falar em violação do dever objetivo de cuidado pelos gestores de TI, situando-se o evento dentro da margem do "risco permitido" (CANESTRARO MH e VIANNA RL, 2023).

II. A Imputação Objetiva nos Sistemas Distribuídos

Em infraestruturas críticas, o resultado danoso muitas vezes decorre da confluência de múltiplos fatores técnicos e operacionais distribuídos. A aplicação cega da teoria da equivalência das condições revela-se insuficiente para fundamentar a responsabilidade criminal. Exige-se a aplicação da Teoria da Imputação Objetiva para determinar se a conduta do agente criou ou incrementou de forma juridicamente desaprovada o risco do resultado (SIEBER U, 2020). Se a operadora segue as diretrizes da ISO/IEC 27001:2022 e do COBIT 2019, os danos decorrentes do risco residual tecnológico não podem ser imputados penalmente aos seus dirigentes (ISACA, 2021).

III. A Validade Dogmática e Proporcionalidade das Medidas Cautelares

A apreensão indiscriminada de servidores centrais, roteadores ou bases de dados de uma operadora nacional de telecomunicações por ordem judicial desproporcionada pode causar a paralisação completa de serviços essenciais à sociedade, ampliando o dano económico e social em vez de resguardar a prova.

As medidas cautelares no processo penal digital devem subordinar-se estritamente ao princípio da proporcionalidade, priorizando a espelhagem e a cópia forense bit-a-bit (forensic image) sem interrupção do serviço público (ISO/IEC, 2021; SILVA AP, 2024).

3.3. A Prova Digital e o Processo Penal Angolano: A Cadeia de Custódia

A introdução de evidências digitais no processo penal angolano impõe o estrito cumprimento da cadeia de custódia da prova digital (chain of custody), sob pena de nulidade

insanável por violação das garantias constitutionais de defesa (CRA, art. 67.º; SILVA AP, 2024). Na criminalidade económica e cibernética, a mera presença de logs de servidores ou ficheiros corrompidos juntados sem verificação de hash não atesta, per se, a imputação penal subjetiva ao agente.

Como enfatiza Silva (2024):

> Sem a observância rigorosa da norma ISO/IEC 27037 no manuseamento dos dados voláteis e não voláteis, a prova digital perde a sua integridade e autenticidade, gerando sérias dúvidas razoáveis em sede de instrução preparatória e julgamento criminal (SILVA AP, 2024, p. 98).

A conformidade com os protocolos da ISO/IEC 27037:2021 exige documentação ininterrupta desde a identificação, recolha, aquisição até à preservação dos artefactos digitais. A inobservância do cálculo e validação dos algoritmos de hash (como SHA-256) no momento da extração da prova contamina a evidência, tornando-a imprestável para ilidir a presunção de inocência.

3.4. Modelo Proposto de Hermenêutica Interdisciplinar

Para solucionar a desconexão identificada, o presente trabalho propõe um Modelo de Hermenêutica Interdisciplinar e Acoplagem Normativo - Tecnológica estruturado em quatro vertentes:

I. Convergência Normativo-Conceitual: Os termos jurídicos das leis sobre crimes informáticos devem ser interpretados em consonância direta com as definições internacionais consagradas pelas normas ISO/IEC e pela ITU.

II. Utilização da Governança de TI como Parâmetro de Cuidado: A averiguação do dever objetivo de cuidado e da culpa em Direito Penal Económico deve tomar como parâmetro objetivo o nível de maturidade e conformidade da instituição com os frameworks COBIT 2019 e NIST CSF 2.0.

III. Institucionalização de Padrões Periciais Obrigatórios: Vinculação da atuação dos órgãos de investigação criminal (como o SIC e a PGR em Angola) aos protocolos da ISO/IEC 27037 para a garantia da cadeia de custódia probatória.

IV. Capacitação e Câmeras Especializadas: Criação de comissões interdisciplinares permanentes congregando magistrados, procuradores e peritos em cibersegurança para a formulação de diretrizes de obtenção e valoração da prova digital.

CONCLUSÃO

A análise dogmática e tecnológica do incidente de cibersegurança na UNITEL conduz às seguintes conclusões consolidadas:

A Incerteza Epistemológica Inicial: Os engenheiros informáticos e peritos de TI não detêm o conhecimento absoluto e imediato das causas e consequências de ataques cibernéticos em

infraestruturas críticas; a busca da verdade empírica na forense digital é um processo gradual, analítico e probabilístico.

O Hiato Hermenêutico: A hermenêutica das leis sobre cibersegurança não pode ser um exercício jurídico isolado. A ausência de acoplagem entre a técnica normativa e a Governança de TI gera normas inexequíveis ou distorções no juízo de imputação penal.

As Exigências do Processo Penal: O Direito Penal Económico e o Direito Processual Penal em Angola devem adaptar rigorosamente a avaliação da prova digital à volatilidade e complexidade dos ecossistemas de telecomunicações modernos, exigindo o estrito cumprimento da cadeia de custódia.

A Interdisciplinaridade Premissa: Recomenda-se a criação de comissões interdisciplinares permanentes em Angola, congregando juristas especializados em Direito Penal Económico e especialistas em Cibersegurança, para a elaboração de diretrizes de obtenção da prova digital e regulação de infraestruturas críticas.

REFERÊNCIAS

BONGERS F, et al. Structure and floristic composition of the lowland rain forest of Los Tuxtlas, Mexico. Vegetatio, 1988; 74: 55-80.

BRENNER SW. Cybercrime and the Law: Challenges for the Twenty-First Century. MIT Press, 2021; 384p.

CANESTRARO MH e VIANNA RL. Imputação objetiva e criminalidade informática nos crimes económicos. Revista de Direito Penal Económico e Criminologia, 2023; 11(2): 45-68.

CARRIER B. File System Forensic Analysis and Digital Investigations. 2nd ed. Addison-Wesley, 2023; 600p.

CASEY E. Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. 4th ed. Academic Press, 2021; 812p.

CLEMENT S e SHELFORD VE. Bio-ecology: an introduction. 2nd ed. New York: J. Willey, 1966; 425p.

DILLENBURG LR. Estudo fitossociológico do estrato arbóreo da mata arenosa de restinga em Emboaba, RS. Dissertação (Mestrado em Botânica) – Instituto de Biociências, Universidade Federal do Rio Grande do Sul, Porto Alegre, 1986; 400p.

ENISA – European Union Agency for Cybersecurity. ENISA Threat Landscape 2023. Publications Office of the European Union, 2023; 108p.

ENISA – European Union Agency for Cybersecurity. Cybersecurity in Telecommunications and Critical Infrastructures. Publications Office of the European Union, 2024; 92p.

FORTES AB. Geografia física do Rio Grande do Sul. Porto Alegre: Globo, 1959; 393p.

GARTNER. Market Guide for Digital Forensics and Incident Response Services. Gartner Research, 2023; 45p.

HORSMAN G. Formalising digital forensic investigative reasoning: Challenges and opportunities. Forensic Science International: Digital Investigation, 2022; 40: 301-320.

ISACA. COBIT 2019 Framework: Governance and Management Objectives. ISACA, 2021; 300p.

ISO/IEC. ISO/IEC 27037:2021 Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence. International Organization for Standardization, 2021; 58p.

ITU – International Telecommunication Union. Understanding Cybercrime: Phenomena, Challenges and Legal Response. ITU Publications, 2022; 180p.

JÚNIOR CC. Trabalho, educação e promoção da saúde. Revista Eletrônica Acervo Saúde, 2014; 6(2): 646-648.

NIST – National Institute of Standards and Technology. The NIST Cybersecurity Framework (CSF) 2.0. NIST Special Publication 800-50r2, 2024; 120p.

POLÍTICA. In: Dicionário da língua portuguesa. Lisboa: Priberam Informática, 1998.

QUADRA AA e AMÂNCIO AA. A formação de recursos humanos para a saúde. Ciência e Cultura, 1978; 30(12): 1422-1426.

SIEBER U. Criminal law for the digital age: Modernizing economic and cybercrime offenses. International Review of Penal Law, 2020; 91(1): 115-148.

SILVA AP. A prova digital no processo penal angolano: Desafios de autenticidade e cadeia de custódia. Revista Angolana de Direito e Tecnologia, 2024; 3(1): 89-112.

UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL. Faculdade de Educação. Planejamento e organização do ensino: um manual programado para treinamento de professor universitário. Porto Alegre: Globo, 2003; 400p.