Revista ft

www.revistaft.com.br

Revista FT | ISSN 1678-0817 | v. 30, n. 157, 2026 | DOI: 10.69849/r9p2f377

Direito digital em Angola: segurança da informação, conformidade legal, crimes digitais e inteligência artificial na actividade forense

Digital Law in Angola: Information Security, Legal Compliance, Cybercrime, and Artificial Intelligence in Forensic Activity

Ervedoso Tchiangalala [1]
Emiliano Jerónimo [1]
Enderson Bernardo [1]

RESUMO

O presente artigo analisa o estado actual do Direito Digital em Angola, abrangendo as dimensões da segurança da informação, da conformidade normativa, da criminalidade informática e da inteligência artificial na actividade forense. O vertiginoso processo de digitalização da economia e dos serviços públicos angolanos impõe desafios normativos de elevada complexidade, exigindo dos operadores jurídicos uma compreensão sistemática dos quadros legais vigentes e dos instrumentos de tutela disponíveis. Adoptando uma metodologia jurídico-dogmática e comparada, o estudo examina criticamente os principais diplomas do ordenamento jurídico angolano: a Lei n.º 22/11 (Lei de Protecção de Dados Pessoais), a Lei n.º 23/11 (Lei das Comunicações Electrónicas), a Lei n.º 7/17 (Lei de Protecção das Redes e Sistemas Informáticos) e o Código Penal Angolano (Lei n.º 38/20). O artigo contextualiza este quadro normativo na arquitectura jurídica africana e internacional, analisando as obrigações decorrentes da ratificação da Convenção de Malabo e a influência do Regulamento Geral sobre a Protecção de Dados da União Europeia. Examina-se ainda o fenómeno emergente da inteligência artificial na prática forense angolana, com particular atenção à ética no seu uso à luz da pauta deontológica da função pública, dos magistrados judiciais, do Ministério Público e do Código de Ética da Ordem dos Advogados de Angola. Conclui-se que Angola dispõe de um núcleo normativo relevante em processo de consolidação activa, persistindo lacunas estruturais cuja colmatação é imperativa, designadamente em matéria de cibersegurança, processo penal digital e regulação ética da inteligência artificial na administração da justiça.

1 Docente Universitário/Investigador e Advogado
1 Advogado e Investigador
1 Advogado e Investigador

Palavras-chave: *Direito Digital; Segurança da Informação; Crimes Informáticos; Conformidade Legal; Protecção de Dados Pessoais; Inteligência Artificial Forense; Ética Deontológica; Angola; Cibersegurança.*

ABSTRACT

This article provides a comprehensive analysis of Digital Law in Angola, focusing on information security, legal compliance, cybercrime and artificial intelligence in forensic practice. Using a legal-dogmatic and comparative methodology, the study critically examines Angola's main digital law instruments, situates this framework within the African and international legal architecture, and analyses the emerging phenomenon of artificial intelligence in Angolan forensic activity, including the ethical duties of magistrates and lawyers under applicable deontological instruments. The conclusion is that Angola possesses a relevant and increasingly active normative core, while structural gaps persist, particularly in cybersecurity legislation, digital criminal procedure and ethical regulation of artificial intelligence in the administration of justice.

Keywords: *Digital Law; Information Security; Cybercrime; Legal Compliance; Personal Data Protection; Forensic Artificial Intelligence; Deontological Ethics; Angola; Cybersecurity.*

1. INTRODUÇÃO

A emergência da sociedade em rede constitui, como assinalou Manuel Castells, uma das transformações estruturais mais profundas da história contemporânea, uma reconfiguração das lógicas de produção, poder e experiência humana em torno de fluxos de informação digitalmente mediados.[1] Angola, inserida neste processo de transformação global, tem assistido à acelerada expansão das tecnologias de informação e comunicação: a taxa de penetração da Internet ultrapassou os 36% em 2024, o sistema de pagamentos digitais Multicaixa Express registrou mais de 10 milhões de utilizadores activos, e o Executivo angolano comprometeu-se, através do Plano Nacional de Desenvolvimento (PND) 2023-2027, com a digitalização abrangente dos serviços públicos.

É neste contexto de transformação digital acelerada que o Direito Digital se afirma como um dos campos mais dinâmicos e exigentes do ordenamento jurídico

[1]CASTELLS, Manuel. A Sociedade em Rede. 4.ª ed. Lisboa: Fundação Calouste Gulbenkian, 2007.

angolano. A consagração normativa deste domínio assenta em quatro pilares legislativos fundamentais: a Lei de Protecção de Dados Pessoais (LPDP),[2] a Lei das Comunicações Electrónicas e dos Serviços da Sociedade da Informação (LCE),[3] a Lei de Protecção das Redes e Sistemas Informáticos,[4] e o Código Penal Angolano (CPA), que em 2020 incorporou a tipificação sistemática dos crimes informáticos.[5]

O presente artigo, apresentado no âmbito do Workshop sobre Direito realizado em Março de 2026, propõe-se a examinar criticamente cinco dimensões nucleares do Direito Digital angolano: (i) a segurança da informação e a protecção de dados pessoais; (ii) a conformidade legal das organizações no espaço digital; (iii) a criminalidade informática e os mecanismos de resposta do ordenamento jurídico; (iv) a inteligência artificial na actividade forense; e (v) a ética no uso da inteligência artificial na prática forense à luz dos instrumentos deontológicos aplicáveis.

Do ponto de vista metodológico, o estudo adopta uma abordagem jurídico-dogmática que articula a análise da legislação vigente com a doutrina especializada angolana[6] e portuguesa,[7] numa perspectiva comparada que permite contextualizar o quadro angolano no ecossistema jurídico-digital africano e internacional.

1.1 PROBLEMÁTICA E JUSTIFICAÇÃO DA ESCOLHA DO TEMA

A acelerada digitalização da economia e dos serviços públicos angolanos configura um dos fenómenos de transformação social mais significativos da Angola contemporânea. Em menos de uma década, o país passou de um modelo de prestação de serviços essencialmente presencial e analógico para um ecossistema em que transacções financeiras, relações contratuais, comunicações institucionais e a própria administração da justiça são progressivamente mediadas por plataformas digitais. Esta transformação, de inegável potencial para o desenvolvimento económico e para a inclusão social, gera simultaneamente riscos e desafios

---

[2]CASTELLS, Manuel. op. cit. Vide também: FRANCISCO, João A. Direito da Informática: Direito das Novas Tecnologias de Informação e Comunicação. Luanda: Editora das Letras, 2018, pp. 15-32, sobre o processo de digitalização angolano no contexto africano.

[3]Lei n.º 22/11, de 17 de Junho (LPDP). Diário da República, I Série, n.º 114. Luanda, 2011. Inspirada na Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995.

[4]Lei n.º 23/11, de 20 de Junho (LCE). Diário da República, I Série, n.º 116. Luanda, 2011. Regula as comunicações electrónicas, os serviços da sociedade da informação e o comércio electrónico.

[5]Lei n.º 7/17, de 16 de Fevereiro (Lei de Proteção das Redes e Sistemas Informáticos). Diário da República, I Série, n.º 30. Luanda, 2017.

[6]Lei n.º 38/20, de 11 de Novembro (Código Penal Angolano). Diário da República, I Série, n.º 179. Luanda, 2020. A incorporação dos crimes informáticos nos artigos 439.º a 444.º representou o salto qualitativo mais significativo do ordenamento penal angolano na era digital.

[7]FRANCISCO, João A. Direito da Informática: Direito das Novas Tecnologias de Informação e Comunicação. Luanda: Editora das Letras, 2018; FRANCISCO, João A. Proteção de Dados Pessoais em Angola: Da Lei 22/11 ao desafio do Big Data. Revista de Direito Público Angolano, n.º 4, 2020, pp. 45-72; SILVA, Paulo. Crimes Informáticos no novo Código Penal Angolano. Revista Jurídica Angolana, n.º 7, 2021, pp. 112-145; PINTO, F. L. A responsabilidade penal das pessoas colectivas no Código Penal Angolano. Direito em Debate, n.º 3, 2022, pp. 88-110.

normativos de crescente complexidade que o ordenamento jurídico angolano é chamado a responder.

A problemática central que justifica a escolha deste tema reside na tensão estrutural entre a velocidade da inovação tecnológica e a capacidade de resposta do sistema jurídico angolano. Angola dispõe de um núcleo normativo relevante (a Lei de Protecção de Dados Pessoais, a Lei das Comunicações Electrónicas, a Lei de Protecção das Redes e Sistemas Informáticos e o Código Penal Angolano), mas este quadro apresenta lacunas estruturais que comprometem a sua efectividade, designadamente em matéria de cibersegurança institucional, processo penal digital, regulação da inteligência artificial e ética forense no ambiente digital.[8]

Acresce que o fenómeno emergente da inteligência artificial (IA) na prática jurídica e forense suscita questões absolutamente novas para as quais o ordenamento angolano não dispõe ainda de respostas normativas expressas: a admissibilidade probatória de análises produzidas por algoritmos; a responsabilidade pelo erro da máquina em contexto judicial; os deveres deontológicos dos magistrados e advogados no uso de ferramentas de IA; e os limites éticos da automação decisória em matéria que afecte direitos fundamentais.

É neste contexto de urgência normativa e de complexidade crescente que o presente artigo se propõe a analisar criticamente o estado do Direito Digital angolano, identificar as suas lacunas mais prementes e formular recomendações de política jurídica orientadas para a construção de um ecossistema jurídico-digital robusto, eticamente orientado e internacionalmente articulado.

1.2 OBJECTIVOS

1.2.1 Objectivo Geral

Analisar criticamente o quadro normativo do Direito Digital angolano nas suas dimensões de segurança da informação, conformidade legal, criminalidade informática e inteligência artificial na actividade forense, identificando lacunas estruturais e propondo recomendações de política jurídica orientadas para a consolidação de um ordenamento jurídico-digital efectivo, ético e internacionalmente articulado.

1.2.2 Objectivos Específicos

1. Examinar os fundamentos conceptuais e os princípios estruturantes do Direito Digital angolano, avaliando a sua adequação à realidade normativa contemporânea;

---

[8]CASTELLS, Manuel. A Sociedade em Rede. 4.ª ed. Lisboa: Fundação Calouste Gulbenkian, 2007. Trad. portuguesa de The Information Age: Economy, Society and Culture, vol. 1. Oxford: Blackwell, 1996. A obra constitui o enquadramento sociológico de referência para a análise jurídica do ciberespaço como espaço social de produção, comunicação e poder.

2. Analisar o quadro normativo da segurança da informação e da protecção de dados pessoais em Angola, com enfoque na Lei n.º 22/11 (LPDP), na Lei n.º 7/17 e no Aviso BNA n.º 2/2021;
3. Examinar as obrigações de compliance digital aplicáveis às organizações em Angola e as implicações da responsabilidade dos administradores no espaço digital;
4. Analisar a tipologia dos crimes informáticos no Código Penal Angolano e os desafios processuais da prova digital;
5. Estudar comparativamente os modelos português e brasileiro de Direito Digital, identificando lições e boas práticas transponíveis para o ordenamento angolano;
6. Examinar o fenómeno da inteligência artificial na actividade forense em Angola, avaliando as suas potencialidades, riscos e implicações normativas;
7. Analisar os deveres éticos dos operadores jurídicos (magistrados judiciais, magistrados do Ministério Público e advogados) no uso da inteligência artificial na prática forense, à luz dos instrumentos deontológicos aplicáveis;
8. Formular conclusões e recomendações de política jurídica para o desenvolvimento do Direito Digital angolano.

2. ENQUADRAMENTO CONCEPTUAL DO DIREITO DIGITAL

2.1. Natureza e Autonomia do Direito Digital

A questão da natureza jurídica do Direito Digital é objecto de debate doutrinário que transcende o plano académico. José de Oliveira Ascensão sustenta que o Direito Digital não constitui um ramo autónomo, sendo antes um conjunto de regimes jurídicos especiais que se inserem nos ramos tradicionais do direito, cuja compreensão pressupõe o domínio das categorias jurídicas clássicas.[9] Alexandre Libório Dias Pereira, em posição que se afigura mais adequada à realidade normativa contemporânea, distingue um 'Direito da Informática' e um 'Direito na Internet', propondo o 'Direito Digital' como a síntese abrangente de ambas as dimensões, com princípios e metodologia próprios.[10]

No contexto angolano, esta discussão adquire particular acuidade. A dispersão normativa característica do Direito Digital angolano, com regras relevantes distribuídas pela Constituição,[11] pela LPDP, pela LCE, pela Lei n.º 7/17, pelo CPA e

---

[9]DIAS PEREIRA, Alexandre Libório. Direito Digital. Coimbra: Almedina, 2018; ASCE NSÃO, José de Oliveira. Direito da Internet e da Sociedade de Informação. Coimbra: Almedina, 2012; CORDEIRO, A. Barreto Menezes. Direito da Proteção de Dados. Coimbra: Almedina, 2020; NUNES, Duarte Rodrigues. Os Crimes previstos na Lei do Cibercrime. Coimbra: GestLegal, 2019.

[10]ASCENSÃO, José de Oliveira. Direito da Internet e da Sociedade de Informação. Coimbra: Almedina, 2012, pp. 11-34. O autor defende que o Direito da Informática é um domínio transversal que recorre às categorias dos vários ramos, sem poder reivindicar autonomia científica própria.

[11]DIAS PEREIRA, Alexandre Libório. Direito Digital. Coimbra: Almedina, 2018, pp. 23-47. O autor propõe a distinção entre "Direito da Informática" (regras sobre as tecnologias) e "Direito na Internet" (aplicação do direito em ambiente digital), sendo o "Direito Digital" a síntese abrangente de ambas as dimensões.

por diplomas regulamentares sectoriais, torna mais difícil a identificação de uma unidade sistemática que justifique a autonomia científica. Ao mesmo tempo, a especificidade dos problemas que o espaço digital coloca (a identidade digital, a responsabilidade dos algoritmos, a jurisdição nos crimes transnacionais e a volatilidade da prova electrónica) exige competências analíticas que os ramos tradicionais do direito, por si sós, não conseguem fornecer.

A posição adoptada no presente artigo é a de que o Direito Digital angolano tem condições para afirmar uma autonomia científica relativa, fundada em três elementos: (i) um núcleo normativo específico e identificável; (ii) princípios próprios, como os da equivalência funcional, da neutralidade tecnológica, da responsabilidade efectiva dos intermediários e da privacidade por defeito; e (iii) uma metodologia de análise que combina a dogmática jurídica clássica com os instrumentos da Ciência dos Sistemas de Informação e da Segurança Informática.

2.2. Princípios Estruturantes do Direito Digital Angolano

O princípio da equivalência funcional postula que os actos e documentos digitais têm o mesmo valor jurídico que os seus equivalentes em suporte físico, desde que preenchidos os requisitos de autenticidade e integridade. Este princípio encontra consagração expressa no artigo 3.º da LCE,[12] que reconhece valor jurídico pleno aos contratos e documentos celebrados por via electrónica.

O princípio da neutralidade tecnológica impõe que a lei não discrimine entre diferentes soluções tecnológicas, privilegiando formulações normativas abertas que permitam abranger inovações futuras sem revisão legislativa constante. A Lei n.º 7/17 adopta uma formulação ampla do seu âmbito de aplicação[13] que reflecte este princípio.

O princípio da minimização de dados exige que o tratamento de dados pessoais se limite ao estritamente necessário para a finalidade que o justifica. A sua violação foi a base da sanção aplicada pela APD à COSAL, sendo também um dos pilares da revisão da LPDP em curso.

O princípio da privacidade por defeito (*privacy by design* e *privacy by default*) impõe que os sistemas de informação sejam concebidos desde a sua arquitectura de modo a respeitar a privacidade dos utilizadores, princípio que o projecto de revisão da LPDP pretende introduzir expressamente no ordenamento angolano.

---

[12]Constituição da República de Angola (Lei Constitucional n.º 23/10, de 11 de Fevereiro de 2010), artigos 32.º (direito à reserva da intimidade da vida privada e familiar), 35.º (direito à identidade pessoal) e 57.º (restrição de direitos, liberdades e garantias fundamentais). Vide FRANCISCO, João A. Direito da Informática. op. cit., pp. 45-52.

[13]Lei n.º 23/11, artigo 3.º: "Os contratos celebrados por via electrónica produzem todos os efeitos previstos na lei, desde que preenchidos os requisitos legais de validade." O princípio da equivalência funcional é também reconhecido no artigo 7.º da LCE quanto ao valor probatório dos documentos electrónicos.

3. SEGURANÇA DA INFORMAÇÃO: FUNDAMENTOS JURÍDICOS E NORMATIVOS

3.1. As Três Dimensões da Segurança da Informação e o Seu Enquadramento Jurídico

A segurança da informação pode ser definida como o conjunto de medidas técnicas, organizacionais e jurídicas destinadas a garantir a confidencialidade, a integridade e a disponibilidade da informação, as três dimensões da chamada CIA Triad, consagrada pela norma ISO/IEC 27001:2022 como o referencial internacional da gestão da segurança da informação.[14] Esta tríade não constitui um mero conceito técnico: tem relevância jurídica directa, dado que a violação de cada uma destas dimensões gera consequências normativas específicas, seja no plano do direito da responsabilidade civil, seja no plano penal, seja no âmbito da regulação sectorial.

A confidencialidade protege a informação contra acessos não autorizados. A sua violação pode gerar responsabilidade civil nos termos gerais, responsabilidade sancionatória perante a APD (por violação da LPDP) e responsabilidade penal por intercepção ilegítima de dados (artigo 439.º do CPA) ou devassa por meios informáticos.

A integridade garante que a informação não é alterada ou destruída de forma não autorizada. A sua violação pode integrar o crime de falsidade informática (artigo 442.º do CPA).

A disponibilidade assegura que os sistemas e a informação estão acessíveis quando necessários. A sua violação dolosa pode integrar o crime de sabotagem informática (artigo 441.º do CPA).

O *National Institute of Standards and Technology* (NIST) propõe, no seu Cybersecurity Framework (versão 2.0), um modelo de gestão de riscos de cibersegurança organizado em cinco funções nucleares (Identificar, Proteger, Detectar, Responder, Recuperar),[15] que constitui referência adoptada pelas principais organizações angolanas com operações internacionais.

3.2. O Quadro Normativo de Cibersegurança em Angola

3.2.1. A Lei n.º 7/17 e a Regulação das Redes e Sistemas Informáticos

[14]Lei n.º 7/17, artigo 2.º, que define o âmbito de aplicação de forma tecnologicamente neutra, abrangendo "qualquer sistema informático, rede de comunicações ou infraestrutura de tecnologias de informação e comunicação", sem enumerar taxativamente as tecnologias abrangidas.

[15]ISO/IEC 27001:2022 — Information Security Management Systems. Genebra: ISO, 2022. A norma define a tríade CIA (Confidentiality, Integrity, Availability) como o modelo de referência para a gestão da segurança da informação, sendo adoptada como referência pelo Aviso BNA n.º 2/2021 para as instituições financeiras angolanas.

A Lei n.º 7/17, de 16 de Fevereiro,[16] constitui o diploma nuclear do quadro normativo de cibersegurança em Angola. O seu âmbito de aplicação abrange o ciberespaço angolano na sua totalidade, protegendo redes públicas e privadas, sistemas de informação de titularidade estatal e privada, e infraestruturas críticas de informação. O diploma impõe obrigações específicas aos operadores de infraestruturas críticas: manutenção de sistemas de monitorização e detecção de intrusões, adopção de planos de resposta a incidentes, notificação ao INACOM de incidentes de segurança significativos e submissão a auditorias periódicas de segurança. A definição de "infraestrutura crítica de informação",[17] que abrange os sectores energético, financeiro, da saúde, das comunicações e das administrações públicas, é central para a determinação do universo de sujeitos obrigados.

Uma lacuna significativa da Lei n.º 7/17 reside na ausência de uma arquitectura institucional explícita para a resposta nacional a ciberincidentes. O diploma não cria um CERT (*Computer Emergency Response Team*) nacional nem define com precisão as competências do INACOM, da APD e das forças de segurança na resposta a ciberataques de grande escala. Esta lacuna é um dos problemas que a Proposta de Lei da Cibersegurança em consulta pública pretende resolver.[18]

3.2.2. A Regulação Sectorial: O Aviso BNA n.º 2/2021

No sector financeiro, o Banco Nacional de Angola (BNA) tem exercido um papel de liderança na exigência de padrões elevados de segurança da informação. O Aviso n.º 2/2021 sobre Gestão de Risco das Tecnologias de Informação e Comunicação nas Instituições Financeiras[19] impõe, entre outros requisitos: a criação de uma função de gestão do risco das TIC independente da função operacional; a adopção de um sistema de gestão de segurança da informação baseado em normas internacionais reconhecidas; a elaboração de planos de continuidade de negócio e de recuperação de desastre; e requisitos específicos de governação na externalização de serviços tecnológicos para terceiros, incluindo prestadores de serviços em nuvem.

3.3. Protecção de Dados Pessoais: A LPDP e a Sua Evolução

3.3.1. A Arquitectura da Lei n.º 22/11 (LPDP)

---

[16]NIST — National Institute of Standards and Technology. Cybersecurity Framework 2.0. Gaithersburg: NIST, 2024. O CSF 2.0 expande o modelo original de 2014 com uma sexta função nuclear: "Govern" (Governar), que estabelece a responsabilidade de liderança na gestão do risco de cibersegurança.

[17]Lei n.º 7/17, de 16 de Fevereiro. Diário da República, I Série, n.º 30. Luanda, 2017.

[18]Lei n.º 7/17, artigo 4.º, que define "infraestrutura crítica de informação" como os sistemas e redes informáticos dos sectores energético, financeiro, da saúde, das comunicações e das administrações públicas, cuja perturbação poderia ter um impacto grave na segurança nacional ou no bem-estar público.

[19]MINTTICS. Proposta de Lei da Cibersegurança (em consulta pública). Disponível em: <https://consultapublica.minttics.gov.ao>. Luanda, 2023/2024. A proposta prevê a criação de um CERT nacional sob tutela do INACOM e o reforço das obrigações de notificação de incidentes de cibersegurança pelas infraestruturas críticas.

A Lei n.º 22/11, de 17 de Junho,[20] é a pedra angular do direito da privacidade em Angola. Inspirada na Directiva 95/46/CE do Parlamento Europeu e do Conselho, a LPDP consagra o tratamento de dados pessoais como matéria de direito fundamental, cuja restrição exige fundamento constitucional explícito nos termos do artigo 57.º da Constituição.[21] A estrutura normativa da LPDP articula-se em torno de cinco eixos: (i) princípios do tratamento; (ii) direitos dos titulares; (iii) obrigações do responsável pelo tratamento; (iv) regime das transferências internacionais; e (v) poderes da APD.

3.3.2. A APD: Actividade Fiscalizadora e Evolução Sancionatória

A Agência de Protecção de Dados (APD) tem intensificado progressivamente a sua actividade de fiscalização e sancionamento, consolidando-se como um regulador activo com impacto real no comportamento das organizações.[22] A sua actividade sancionatória recente revela uma orientação estratégica clara: sanção prioritária de violações relacionadas com a segurança dos dados pessoais e com as transferências internacionais não autorizadas.

O perfil das decisões sancionatórias da APD merece análise detalhada. As multas aplicadas, que variaram entre USD 75.000 e USD 150.000 nas decisões mais recentes, são formalmente expressivas no contexto do ordenamento angolano, mas permanecem modestas quando comparadas com as sanções do RGPD europeu, que podem atingir 4% do volume de negócios mundial anual.[23]

3.3.3. A Revisão da LPDP e o Alinhamento com o RGPD e a Convenção de Malabo

Em Março de 2025, a APD lançou o processo de revisão da Lei n.º 22/11 através de consulta pública.[24] A proposta de revisão, amplamente inspirada no RGPD, pretende introduzir no ordenamento angolano os seguintes novos institutos: o direito ao apagamento ("direito a ser esquecido"); o direito à portabilidade dos dados; o princípio da responsabilização (*accountability*); a avaliação de impacto sobre a

---

[20]Banco Nacional de Angola. Aviso n.º 2/2021 sobre Gestão de Risco das Tecnologias de Informação e Comunicação nas Instituições Financeiras. Luanda: BNA, 2021. O Aviso segue de perto as directrizes da Autoridade Bancária Europeia (EBA) sobre gestão de risco das TIC e de segurança, adoptando a norma ISO/IEC 27001 como referência de implementação.

[21]Lei n.º 22/11, de 17 de Junho (LPDP). Diário da República, I Série, n.º 114. Luanda, 2011. Para uma análise sistemática da arquitectura normativa da LPDP, vide FRANCISCO, João A. Proteção de Dados Pessoais em Angola. op. cit., pp. 50-63.

[22]RGPD, artigo 83.º, n.º 5: as violações mais graves podem ser punidas com coimas até 20.000.000 EUR ou, no caso de uma empresa, até 4% do seu volume de negócios anual a nível mundial. Sobre a proporcionalidade sancionatória nos regimes de proteção de dados, vide MAKULILO, Alexander Boniface. Africa and the Global Data Protection Landscape. Baden-Baden: Nomos, 2014, pp. 67-89.

[23]RGPD, artigo 3.º, n.º 2: o RGPD aplica-se ao tratamento de dados de titulares situados na União Europeia, independentemente de o responsável pelo tratamento se encontrar estabelecido fora da UE. A influência extraterritorial do RGPD sobre as empresas angolanas é analisada em KUNER, Christopher. Transborder Data Flows and Data Privacy Law. Oxford: Oxford University Press, 2013, pp. 112-134.

[24]APD. Projecto de Revisão da Lei n.º 22/11: Consulta Pública (Março-Abril 2025). Disponível em: <https://www.apd.ao>. Luanda, 2025. O processo de revisão envolveu a participação de operadores privados, académicos e organizações da sociedade civil.

protecção de dados (AIPD) para tratamentos de alto risco; as regras sobre decisões automatizadas e *profiling*; e o regime de violações de dados pessoais (*data breaches*) com notificação obrigatória.

A revisão da LPDP ocorre num contexto em que Angola já ratificou a Convenção de Malabo[25] e em que a influência extraterritorial do RGPD se faz sentir nas empresas angolanas que tratam dados de cidadãos europeus.[26] A convergência regulatória internacional é, por isso, simultaneamente uma exigência normativa e uma oportunidade estratégica.

4. CONFORMIDADE LEGAL NO ESPAÇO DIGITAL (COMPLIANCE DIGITAL)

4.1. Fundamentos Teóricos e Importância Prática do Compliance Digital

O *compliance* digital, entendido como o conjunto estruturado de mecanismos, políticas, processos e controlos que uma organização implementa para assegurar a conformidade com o quadro normativo aplicável às suas actividades digitais,[27] representa hoje um dos domínios de prática jurídica de maior crescimento em Angola, impulsionado pela combinação de quatro factores: a intensificação da actividade regulatória e fiscalizatória da APD; as exigências de segurança da informação impostas pelo BNA ao sector financeiro; a crescente litigiosidade em matéria de violações de dados e crimes informáticos; e a pressão exercida pelos investidores e parceiros internacionais quanto ao cumprimento de padrões globais de governação digital.

4.2. O Cúmplice Digital: Obrigações de Compliance e Responsabilidade dos Administradores

A crescente regulação do espaço digital tem implicações directas na responsabilidade pessoal dos administradores e dirigentes das organizações. Quem decide adoptar ou omitir medidas de *compliance* digital torna-se, em termos práticos, um co-responsável pelos riscos que daí emergem. A Lei das Sociedades Comerciais[28] consagra o dever geral de diligência dos administradores, correntemente interpretado como impondo a adopção de sistemas adequados de gestão de risco, incluindo o risco tecnológico e jurídico no espaço digital.

---

[25]Resolução n.º 33/19, de 9 de Julho. Angola ratificou a Convenção da UA sobre Cibersegurança e Proteção de Dados Pessoais (Convenção de Malabo). Luanda, 2019. A Convenção de Malabo entrou em vigor em 8 de Junho de 2023, após a ratificação pelo 15.º Estado-Membro da UA.

[26]

[27]Lei n.º 23/11, artigos 18.º a 24.º (contratos electrónicos, incluindo os deveres de informação pré-contratual e de confirmação do pedido contratual) e artigos 25.º a 30.º (responsabilidade dos prestadores intermediários, que segue o modelo de safe harbours adoptado na Directiva 2000/31/CE sobre comércio electrónico).

[28]PLMJ/RVA. Dados Pessoais e Ciber-segurança em Angola. Nota Informativa. Luanda, Janeiro de 2024. A nota identifica as principais exposições jurídicas em operações de M&A com activos digitais em Angola, incluindo a responsabilidade por violações de dados não comunicadas à APD.

As principais obrigações de compliance digital aplicáveis às organizações que operam em Angola abrangem:

- **Protecção de dados pessoais (LPDP):** notificação prévia à APD de cada operação de tratamento, designação de um responsável interno pela protecção de dados, elaboração de registo das actividades de tratamento e observância dos direitos dos titulares de acesso, rectificação, apagamento e oposição;
- **Comunicações electrónicas e comércio digital (Lei n.º 23/11):**[29] cumprimento de deveres de informação pré-contratual, de confirmação do pedido contratual e de arquivamento dos contratos;
- **Instituições financeiras (Aviso BNA n.º 2/2021):**[30] criação de uma função de risco das TIC independente, adopção de quadro de gestão de riscos tecnológicos documentado e comunicação regular ao conselho de administração sobre o perfil de risco tecnológico.

O Código Penal Angolano prevê, no artigo 9.º, a responsabilidade criminal das pessoas colectivas de forma ampla, sem estabelecer um catálogo taxativo de crimes imputáveis a empresas, ao contrário da solução adoptada no artigo 11.º, n.º 2, do Código Penal Português.[31] Esta amplitude reforça a importância de programas robustos de *compliance* digital nas organizações angolanas.

A *due diligence* digital adquire particular relevância nos processos de fusão e aquisição de empresas com actividade digital significativa.[32] Nestes contextos, a avaliação do risco jurídico-digital deve abranger o estado de conformidade com a LPDP, as vulnerabilidades de segurança da informação, a existência de incidentes não reportados e a adequação dos contratos com prestadores de serviços tecnológicos.

5. CRIMES DIGITAIS: TIPOLOGIA, REGIME JURÍDICO E DESAFIOS PROCESSUAIS

5.1. Tipologia e Fenomenologia dos Crimes Informáticos

Os crimes informáticos ou crimes digitais podem ser definidos, em sentido amplo, como as infracções penais em que o computador, sistema informático ou rede de

---

[29]Banco Nacional de Angola. Aviso n.º 2/2021, artigos 5.º a 12.º (função de gestão do risco das TIC), artigos 13.º a 18.º (requisitos de segurança da informação) e artigos 19.º a 23.º (gestão da externalização tecnológica).

[30]CPA, artigo 9.º (responsabilidade criminal das pessoas colectivas); cf. Código Penal Português, artigo 11.º, n.º 2, que estabelece um catálogo taxativo de crimes imputáveis a pessoas colectivas. Sobre a solução angolana e as suas implicações para o compliance, PINTO, F. L. A responsabilidade penal das pessoas colectivas no Código Penal Angolano. Direito em Debate, n.º 3, 2022, pp. 88-110.

[31]Esta distinção é acolhida pela doutrina angolana: SILVA, Paulo. Crimes Informáticos no novo Código Penal Angolano. Revista Jurídica Angolana, n.º 7, 2021, pp. 112-145; e pela doutrina portuguesa: NUNES, Duarte Rodrigues. Os Crimes previstos na Lei do Cibercrime. Coimbra: GestLegal, 2019, pp. 28-35.

[32]ROMEO CASABONA, Carlos María. De los Delitos Informáticos al Cibercrimen. In: El Cibercrimen: Nuevos Retos Jurídico Penales. Granada: Comares, 2006. A taxonomia de Casabona entre crimes "puros" e "impuros" é a mais citada na doutrina lusófona.

comunicações constitui o instrumento, o meio ou o objecto do crime. Carlos Romeo Casabona, numa taxonomia que influenciou decisivamente a doutrina lusófona,[33] distingue entre crimes informáticos *puros ou próprios*, aqueles que dependem ontologicamente de meios informáticos para existir (como o acesso ilegítimo a sistemas ou a intercepção de dados electrónicos), e crimes informáticos *impuros ou impróprios*, infracções clássicas executadas por meios digitais (como a burla, a difamação ou o branqueamento de capitais operados através de plataformas digitais).[34]

O Código Penal Angolano adopta uma classificação bipartida (Crimes Contra os Dados Informáticos e Crimes Contra as Comunicações e Sistemas Informáticos) nos artigos 439.º a 444.º.[35] Paulo Silva realiza, numa análise dogmática que constitui a referência académica mais aprofundada sobre estes tipos penais, um exame sistemático dos seus elementos objectivos e subjectivos, concluindo que a tipificação angolana é, em geral, mais ampla do que a da Convenção de Budapeste, o que pode gerar questões de proporcionalidade penal.[36]

5.2. Os Crimes Informáticos no Código Penal Angolano: Análise Dogmática

A incorporação dos crimes informáticos no Código Penal Angolano, aprovado pela Lei n.º 38/20 de 11 de Novembro de 2020,[37] representou um salto qualitativo fundamental para o ordenamento jurídico angolano. Os tipos criminais previstos no CPA organizam-se do seguinte modo:[38]

Intercepção ilegítima de dados informáticos (artigo 439.º): punível com pena de prisão até 2 anos ou multa até 240 dias, com agravação para 2 a 8 anos se o crime for cometido com violação de regras de segurança impostas por lei.[39]

---

[33]CPA, artigos 439.º a 444.º. Sobre a sistemática e a dogmática destes tipos penais, SILVA, Paulo. op. cit., pp. 117-145; QUELHAS, I. O Novo Código Penal Angolano: Principais Inovações. Actualidad Jurídica Angola, n.º 15, 2021; SÉRVULO & ASSOCIADOS. Novo Código Penal Angolano. Nota de Conhecimento. Lisboa/Luanda, Novembro de 2020.

[34]SILVA, Paulo. op. cit., p. 138. O autor observa que o CPA angolano, ao contrário da Convenção de Budapeste, não exige que o acesso ilegítimo seja praticado "sem direito" como elemento normativo expresso do tipo, o que pode gerar questões de proporcionalidade quando aplicado a actividades de investigação de segurança (ethical hacking).

[35]Lei n.º 38/20, de 11 de Novembro. Diário da República, I Série, n.º 179. Luanda, 2020. Como assinalado por QUELHAS, I. op. cit.: "foram precisos 45 anos para que Angola conhecesse o seu próprio Código Penal".

[36]Síntese elaborada com base em SILVA, Paulo. op. cit., pp. 120-138; SÉRVULO & ASSOCIADOS. Novo Código Penal Angolano. op. cit.; PTI.AO. A cibersegurança e os crimes informáticos no ordenamento jurídico angolano. Luanda, Agosto de 2023.

[37]CPA, artigo 9.º. A amplitude desta norma contrasta com a solução portuguesa (artigo 11.º, n.º 2 do CP) e é objecto de crítica pela doutrina: PINTO, F. L. op. cit., pp. 95-102.

[38]Lei n.º 7/17, artigos 19.º a 25.º. Estas disposições processuais estabelecem mecanismos de preservação expedita de dados informáticos em risco de destruição, de pesquisa e apreensão de sistemas informáticos, e de cooperação entre autoridades de investigação criminal. Funcionam como lex specialis em relação ao CPPA.

[39]Lei n.º 39/20, de 11 de Novembro (CPPA). Diário da República, I Série, n.º 179. Luanda, 2020.

Sabotagem informática (artigo 441.º): cobre a impedição, interrupção ou perturbação grave do funcionamento de um sistema informático. Este tipo criminal abrange os ataques de DDoS (*Distributed Denial of Service*), a introdução de *malware* ou vírus, e os ataques de *ransomware*, que constituem hoje a principal ameaça às infraestruturas críticas angolanas.

Falsidade informática (artigo 442.º): a introdução, alteração, eliminação ou supressão ilegítima de dados com intenção de que sejam considerados como autênticos.

Burla informática (artigo 443.º): a obtenção de enriquecimento ilegítimo através da manipulação de sistemas informáticos, abrangendo o *phishing*, o *vishing* e as fraudes em sistemas de pagamento digital.

O CPA prevê igualmente, no artigo 9.º, a responsabilidade criminal das pessoas colectivas de forma ampla, sem estabelecer um catálogo taxativo de crimes imputáveis a empresas.[40]

5.3. Investigação Criminal Digital: Lacunas e Desafios Processuais

5.3.1. A Lei n.º 7/17 e os Mecanismos Processuais de Investigação

A Lei n.º 7/17[41] complementa o CPA no domínio da investigação dos crimes informáticos, estabelecendo mecanismos de preservação expedita de dados e de cooperação entre as autoridades de investigação criminal e a APD.

O Código do Processo Penal Angolano (Lei n.º 39/20)[42] não contém disposições específicas sobre prova digital, recolha de metadados, pesquisa de sistemas informáticos ou admissibilidade de prova electrónica obtida em jurisdições estrangeiras.[43] Esta lacuna é particularmente grave num contexto em que a maioria dos dados relevantes para investigações de cibercrime se encontra armazenada em servidores de grandes plataformas tecnológicas internacionais (Google, Meta, Microsoft), cujo fornecimento de dados obriga à activação de mecanismos de cooperação judiciária internacional que o CPPA não regula de forma adequada.

---

[40]PTI.AO. A cibersegurança e os crimes informáticos no ordenamento jurídico angolano. Luanda, Agosto de 2023. Disponível em: <https://www.pti.ao>. Vide também COE/OCTOPUS. Angola: Cybercrime Country Profile. Conselho da Europa, Outubro de 2023, pp. 14-17, que identifica a ausência de normas processuais específicas sobre prova digital como a principal lacuna do sistema angolano de combate ao cibercrime.

[41]Conselho da Europa. Convenção sobre a Cibercriminalidade (Convenção de Budapeste). ETS n.º 185, 23 de Novembro de 2001. Em vigor desde 1 de Julho de 2004, com 68 Estados Partes a Março de 2025. O 2.º Protocolo Adicional (CETS n.º 224, 2022) reforçou os mecanismos de cooperação directa com provedores de serviços e autoridades estrangeiras para efeitos de obtenção de prova digital em investigações de cibercrime transnacionais.

[42]Resolução n.º 33/19, de 9 de Julho. Luanda, 2019. Angola foi um dos primeiros países africanos a ratificar a Convenção de Malabo, o que lhe confere um papel de liderança no processo de implementação do quadro africano de cibersegurança.

[43]COE/OCTOPUS. Angola: Cybercrime Country Profile. Conselho da Europa, Outubro de 2023. O relatório é elaborado no âmbito do Projecto Octopus do Conselho da Europa, que presta assistência técnica aos países parceiros na implementação da Convenção de Budapeste.

5.3.2. A Prova Digital: Volatilidade, Custódia e Admissibilidade

A prova digital apresenta características que a distinguem radicalmente da prova física tradicional: é intangível e reproduzível sem degradação; é altamente volátil e pode ser destruída em segundos; é dependente de sistemas e softwares específicos para ser interpretada; e pode estar dispersa por múltiplas jurisdições simultaneamente.

A preservação da cadeia de custódia (chain of custody) da prova digital constitui um requisito processual indispensável para a sua admissibilidade e para a sua valoração em tribunal. A ausência de normas específicas no CPPA angolano sobre este requisito cria insegurança jurídica significativa, sendo esta uma das reformas processuais mais urgentes que o legislador angolano deve empreender.

5.4. Cooperação Internacional e Integração nos Regimes Multilaterais

A Convenção de Budapeste do Conselho da Europa (2001)[44] é o padrão-ouro internacional em matéria de harmonização do direito penal do cibercrime e de cooperação judiciária. Angola não é signatária, mas o CPA adoptou os seus tipos criminais como referência. A adesão à Convenção de Budapeste constituiria um passo estratégico que reforçaria significativamente as capacidades investigatórias angolanas em contextos internacionais.

No plano africano, Angola ratificou a Convenção de Malabo[45] tornando-se um dos primeiros países africanos a fazê-lo. O relatório do Projecto Octopus do Conselho da Europa sobre o perfil angolano em matéria de cibercrime[46] identifica como prioridades: o reforço das capacidades forenses digitais das autoridades de investigação; a aprovação de legislação específica de cibersegurança; e o estabelecimento de canais formais de cooperação com operadores internacionais de plataformas digitais.

6. DIREITO COMPARADO: ANGOLA, PORTUGAL E BRASIL

6.1. O Código Penal de 1886 e o Longo Vazio Legislativo Angolano

Durante 45 anos após a independência, o ordenamento penal angolano assentou no Código Penal Português de 1886,[47] tornado extensivo a Angola pela Portaria n.º

---

[44]QUELHAS, I. op. cit.: "foram precisos 45 anos para que Angola conhecesse o seu próprio Código Penal." Vide também FRANCISCO, João A. Direito da Informática. op. cit., pp. 67-72.

[45]Declaração do porta-voz da Polícia Nacional angolana (2015), citada em INOVALEGAL. A necessidade de inclusão da sabotagem informática no Anteprojecto de Código Penal angolano. inovalegal.org, Fevereiro de 2020.

[46]Lei n.º 109/2009, de 15 de Setembro (Lei do Cibercrime, Portugal). Diário da República, I Série, n.º 179. Transpos para o direito português a Decisão Quadro n.º 2005/222/JAI do Conselho. Vide NUNES, Duarte Rodrigues. op. cit.; VENÂNCIO, Pedro Dias. Lei do Cibercrime Anotada e Comentada. Coimbra: Coimbra Editora, 2011.

[47]Lei n.º 79/2021, de 24 de Novembro (Portugal), que transpos a Directiva (UE) 2019/713 relativa ao combate à fraude e à contrafacção de meios de pagamento que não em numerário e substituiu a Decisão-Quadro 2001/413/JAI do Conselho.

19.395 de 30 de Junho de 1962, em pleno período colonial. Este diploma oitocentista era absolutamente omisso em matéria de criminalidade informática, criando um vazio legislativo que a emergência da era digital transformou em lacuna estrutural de crescente gravidade. Como assinalado na doutrina[48] e por fontes institucionais,[49] as autoridades recorriam a tipos clássicos para punir condutas digitais, com resultados frequentemente insatisfatórios do ponto de vista da tipicidade estrita.

6.2. O Modelo Português: Lei Autónoma de Cibercrime e Integração Europeia

6.2.1. A Evolução Histórica do Ordenamento Penal Digital Português

A opção estrutural do legislador português foi a de uma lei autónoma de cibercrime. A Lei n.º 109/2009, de 15 de Setembro,[50] transpôs para o direito português a Decisão Quadro n.º 2005/222/JAI do Conselho e adaptou o direito interno à Convenção de Budapeste, da qual Portugal é Estado Parte desde 2010. Os crimes previstos incluem: falsidade informática (artigo 3.º), dano relativo a programas ou dados (artigo 4.º), sabotagem informática (artigo 5.º), acesso ilegítimo (artigo 6.º) e intercepção ilegítima (artigo 7.º). A Lei foi actualizada pela Lei n.º 79/2021[51] que reforçou a tipificação da fraude nos meios de pagamento digitais.

6.2.2. A Protecção de Dados Pessoais: Da Lei n.º 67/98 ao RGPD

Portugal transitou da Lei n.º 67/98 de Protecção de Dados Pessoais para o regime do RGPD, implementado na ordem jurídica portuguesa pela Lei n.º 58/2019, de 8 de Agosto.[52] Esta lei designou a Comissão Nacional de Protecção de Dados (CNPD) como autoridade de controlo nacional, com poderes de investigação, correcção e sancionamento que podem atingir os tectos do RGPD (20 milhões de euros ou 4% do volume de negócios anual global). A CNPD constitui uma referência importante para a evolução da APD angolana,[53] sendo a doutrina portuguesa sobre a Lei do Cibercrime[54] uma referência essencial para os juristas angolanos.

---

[48]VERDELHO, Pedro; BRAVO, Rogério; ROCHA, Manuel Lopes. Leis do Cibercrime, vol. 1. Lisboa: Centro Atlântico, 2003; NUNES, Duarte Rodrigues. op. cit.; VENÂNCIO, Pedro Dias. op. cit.

[49]Lei n.º 58/2019, de 8 de Agosto (Portugal), que assegura a execução, na ordem jurídica nacional, do RGPD. Vide CORDEIRO, A. Barreto Menezes. Direito da Proteção de Dados. Coimbra: Almedina, 2020, pp. 123-156.

[50]Lei n.º 14.155, de 27 de Maio de 2021 (Brasil). Aumentou a pena da invasão de dispositivo informático (artigo 154-A) para reclu são de 1 a 4 anos; criou a fraude electrónica (artigo 171, § 2.º-A), com pena de reclusão de 4 a 8 anos; e agravou o furto qualificado por meios electrónicos.

[51]Comparação elaborada a partir de SILVA, Paulo. op. cit., p. 135; BONA, Maurício. op. cit., pp. 89-95; MAKULILO, Alexander Boniface. op. cit., pp. 112-124.

[52]Lei n.º 12.965, de 23 de Abril de 2014 (Brasil). O Marco Civil da Internet foi pioneiro a consagrar a neutralidade da rede como princípio jurídico vinculativo. Vide DONEDA, Danilo. Da Privacidade à Proteção de Dados Pessoais. 2.ª ed. São Paulo: Thomson Reuters Brasil, 2019, pp. 201-214.

[53]Lei n.º 13.709, de 14 de Agosto de 2018 (Brasil, LGPD), em vigor desde Setembro de 2020. Vide DONEDA, Danilo. op. cit., pp. 215-248.

[54]ANPD. Disponível em: <https://www.gov.br/anpd>. A ANPD tem-se afirmado como autoridade activa, publicando guias de boas práticas, instaurando processos sancionatórios e desenvolvendo regulamentação sectorial, constituindo uma referência para a APD angolana no processo de construção institucional.

6.3. O Modelo Brasileiro: Pluralidade Normativa e Protecção Gradual

6.3.1. Do Código Penal de 1940 às Leis de Cibercrime

O Brasil optou por uma abordagem de emendas sucessivas ao Código Penal de 1940. A Lei n.º 12.737/2012 (Lei Carolina Dieckmann)[55] foi o primeiro diploma brasileiro a tipificar especificamente crimes informáticos. A Lei n.º 14.155/2021[56] aumentou significativamente as penas e criou a fraude electrónica como tipo autónomo. A comparação entre as penas previstas no sistema brasileiro e no angolano revela que os dois sistemas convergem na gravidade máxima das sanções, diferindo na arquitectura dos tipos e nas condições de agravação.[57]

6.3.2. O Marco Civil da Internet e a LGPD: Pioneirismo Regulatório

O contributo mais original do Brasil para o Direito Digital global é, porventura, o Marco Civil da Internet (Lei n.º 12.965/2014),[58] diploma pioneiro a nível mundial que estabelece os princípios, garantias, direitos e deveres para o uso da internet. No domínio da protecção de dados, a Lei Geral de Protecção de Dados Pessoais (LGPD) (Lei n.º 13.709/2018),[59] fortemente inspirada no RGPD europeu, criou a Autoridade Nacional de Protecção de Dados (ANPD)[60] e estabeleceu um regime completo de protecção de dados.

6.4. Análise Comparada: Convergências, Divergências e Lições para Angola

---

[55]Quadro comparativo elaborado com base em MAKULILO, Alexander Boniface. Africa and the Global Data Protection Landscape. op. cit.; CORDEIRO, A. Barreto Menezes. op. cit.; DONEDA, Danilo. op. cit.; GREENLEAF, Graham. Global Tables of Data Privacy Laws and Bills. Privacy Laws & Business International Report, n.º 157, 2019.

[56]Lei n.º 109/2009 (Portugal); CPA, artigos 439.º a 444.º (Angola); Lei n.º 12.737/2012 e Lei n.º 14.155/2021 (Brasil). Sobre as vantagens e desvantagens comparadas de cada arquitectura, vide SILVA, Paulo. op. cit., pp. 130-138.

[57]A convergência com o RGPD europeu como padrão global de referência é documentada em GREENLEAF, Graham. op. cit., e em BYGRAVE, Lee A. Data Privacy Law: An International Perspective. Oxford: Oxford University Press, 2014, pp. 78-102.

[58]COMISSÃO EUROPEIA PARA A EFICIÊNCIA DA JUSTIÇA (CEPEJ). Carta Ética Europeia sobre o Uso da Inteligência Artificial nos Sistemas Judiciais e no seu Ambiente. Estrasburgo: Conselho da Europa, 2018. A Carta enuncia cinco princípios fundamentais (respeito pelos direitos fundamentais, não-discriminação, qualidade e segurança, transparência e imparcialidade, e "sob controlo do utilizador") e constitui a referência deontológica internacional de maior autoridade sobre a IA na justiça. Vide também: ZAVRŠNIK, Aleš (ed.). Automating Justice: The Social, Ethical and Legal Implications of Automated Decision-Making Systems in the Criminal Justice System. Cham: Springer, 2021.

[59]REILING, Dory. Technology for Justice: How Information Technology Can Support Judicial Reform. Leiden: Leiden University Press, 2009; SUSSKIND, Richard. Online Courts and the Future of Justice. Oxford: Oxford University Press, 2019, pp. 145-178; ORGANISATION INTERNATIONALE DE LA FRANCOPHONIE. Justice numérique en Afrique: état des lieux et perspectives. Paris: OIF, 2022; PASQUALE, Frank. The Black Box Society: The Secret Algorithms That Control Money and Information. Cambridge: Harvard University Press, 2015, pp. 1-18.

[60]Regulamento (UE) 2024/1689 (AI Act), artigo 6.º e Anexo III, n.º 8: os sistemas de IA utilizados "para efeitos de administração da justiça e processos democráticos" são classificados como de alto risco, sujeitos a avaliação de conformidade, registo, transparência e supervisão humana obrigatória. Cf. BARFIELD, Woodrow (ed.). The Cambridge Handbook of the Law of Algorithms. Cambridge: Cambridge University Press, 2021, cap. 14.

A análise comparada dos três ordenamentos[61] permite identificar um conjunto de padrões convergentes. No plano da criminalidade informática, os três sistemas partilham a tipificação nuclear das mesmas condutas (acesso ilegítimo, sabotagem, falsidade, burla informática), em linha com a Convenção de Budapeste. A diferença mais significativa reside na arquitectura: a lei autónoma portuguesa, as emendas ao Código Penal brasileiro e a integração codificadora angolana.[62] No plano da protecção de dados, o padrão de convergência com o RGPD europeu é o denominador comum dos três sistemas.[63]

A principal lição transversal que o estudo comparado oferece a Angola é a da importância da construção institucional progressiva: tanto a CNPD portuguesa como a ANPD brasileira levaram anos a afirmar-se como reguladores efectivos. A APD angolana encontra-se neste processo de afirmação, e a revisão da LPDP em curso deve ser acompanhada de um investimento correspondente na capacitação e no reforço dos recursos da APD, sem o qual a melhor lei permanecerá letra morta.

7. INTELIGÊNCIA ARTIFICIAL NA ACTIVIDADE FORENSE EM ANGOLA

7.1. A Emergência da Inteligência Artificial no Sistema de Justiça

A Inteligência Artificial (AI) é a área da computação que se dedica ao desenvolvimento de técnicas e métodos capazes de extrair conhecimento a partir de grandes volumes de dados, especialmente dados não estruturados em linguagem natural, permitindo a análise, interpretação e apoio à tomada de decisões. (DOMINGOS *et al.,* 2024).

---

[61]REILING, Dory. op. cit.; SUSSKIND, Richard. op. cit., pp. 145-178; ORGANISATION INTERNATIONALE DE LA FRANCOPHONIE. op. cit. Sobre ferramentas de PLN aplicadas à pesquisa jurídica, vide FLORIDI, Luciano et al. An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations. Minds and Machines, v. 28, 2018, pp. 689-707.

[62]CASEY, Eoghan; FELLOWS, Geoff A. Network Investigation Methodology. Oxford: Academic Press, 2020; CARRIER, Brian. File System Forensic Analysis. Boston: Addison-Wesley, 2005; NIST. Digital Forensics Framework. Gaithersburg: NIST Special Publication 800-86, 2006 (actualização 2021). Sobre a integração da IA na forense digital, vide ZAVRŠNIK, Aleš (ed.). op. cit., cap. 8.

[63]DRESSEL, Julia; FARID, Hany. The Accuracy, Fairness, and Limits of Predicting Recidivism. Science Advances, v. 4, n.º 1, 2018 (demonstrou empiricamente que o algoritmo COMPAS não supera a precisão de avaliações humanas não treinadas); ANGWIN, Julia et al. Machine Bias. ProPublica, 23 de Maio de 2016 (revelou viéses raciais sistemáticos no COMPAS); CHOULDECHOVA, Alexandra. Fair Prediction with Disparate Impact: A Study of Bias in Recidivism Prediction Instruments. Big Data, v. 5, n.º 2, 2017, pp. 153-163; ZARSKY, Tal Z. The Trouble with Algorithmic Decisions: An Analytic Road Map to Examine Efficiency and Fairness in Automated and Opaque Decision Making. Science, Technology, & Human Values, v. 41, n.º 1, 2016, pp. 118-132.

A inteligência artificial tem penetrado progressivamente nos sistemas de justiça de todo o mundo, transformando de forma estrutural a prática forense.[64] Em Angola, este fenómeno encontra-se ainda numa fase incipiente, mas a sua trajectória de expansão é incontornável: magistrados, advogados e peritos forenses recorrem já a ferramentas de IA para pesquisa jurisprudencial, análise de documentos, redacção de peças processuais, análise de risco de contraparte e perícia técnica digital.[65] A ausência de um quadro normativo específico para a utilização da IA no sistema de justiça angolano não significa que esta utilização seja juridicamente irrelevante, pelo contrário, coloca questões de legalidade, legitimidade e deontologia que o ordenamento vigente já é chamado a resolver.

No plano internacional, a União Europeia adoptou o Regulamento (UE) 2024/1689 (AI Act), que classifica os sistemas de IA utilizados na administração da justiça e nos processos democráticos como "sistemas de alto risco", sujeitos a requisitos estritos de transparência, supervisão humana e avaliação de conformidade.[66] Embora este regulamento não vincule Angola directamente, a sua influência sobre os operadores jurídicos angolanos que actuam em contextos internacionais e sobre a evolução futura da regulação angolana da IA é evidente.

7.2. Aplicações da IA na Prática Forense Angolana

As principais aplicações da IA na actividade forense em Angola podem ser sistematizadas em quatro domínios:

- **Pesquisa e análise jurídica:** ferramentas de processamento de linguagem natural (PLN) permitem a pesquisa automatizada de legislação, jurisprudência e doutrina, reduzindo significativamente o tempo de investigação jurídica.[67]
- **Perícia técnica digital e forense computacional:** a análise de prova digital (recuperação de ficheiros eliminados, análise de metadados, reconstrução de comunicações electrónicas) é progressivamente assistida por ferramentas de IA que permitem processar volumes de dados incompatíveis com o trabalho humano não assistido.[68]

---

[64]ORDEM DOS ADVOGADOS DE ANGOLA. Estatuto da Advocacia e Código Deontológico da Advocacia Angolana. Luanda: OAA. O artigo 7.º do Código Deontológico consagra o dever de competência profissional: "O advogado deve manter-se actualizado sobre as matérias relevantes para o exercício da sua profissão, incluindo as inovações legislativas, jurisprudenciais e tecnológicas."

[65]AMERICAN BAR ASSOCIATION. Formal Opinion 512. op. cit.; ORDEM DOS ADVOGADOS DE PORTUGAL. Recomendações sobre o Uso da Inteligência Artificial na Advocacia. Lisboa: OAP, 2024; BARFIELD, Woodrow (ed.). op. cit., cap. 18; ZARSKY, Tal Z. op. cit., pp. 126-130.

[66]Constituição da República de Angola, artigo 67.º (presunção de inocência: "o arguido presume-se inocente até ao trânsito em julgado da sentença de condenação") e artigo 72.º (garantias do processo criminal). Vide ZAVRŠNIK, Aleš (ed.). op. cit., cap. 3.

[67]CONSELHO CONSULTIVO DOS JUÍZES EUROPEUS (CCJE). Parecer n.º 22 (2019). Estrasburgo: Conselho da Europa, 2019; PARLAMENTO EUROPEU. Resolução de 6 de Outubro de 2021 sobre Inteligência Artificial no Direito Penal (2020/2016(INI)). Bruxelas: PE, 2021.

[68]CEPEJ. Carta Ética Europeia. op. cit., Princípio 5 (Sob Controlo do Utilizador): "Excluir qualquer abordagem determinista na concessão de ferramentas de IA às autoridades judiciárias e garantir que os utilizadores sejam actores informados e que mantenham o controlo das suas escolhas." Vide

- **Análise preditiva de risco e comportamental:** algoritmos de análise de risco são utilizados em contextos de avaliação de risco de fuga, de reincidência criminal ou de gestão de processos judiciais, suscitando sérias questões de proporcionalidade, não-discriminação e direito de audiência.[69]
- **Automação de tarefas processuais e administrativas:** a automatização de notificações, gestão de prazos, categorização de processos e análise estatística de pendências processuais permite ganhos de eficiência significativos nos tribunais e nos serviços do Ministério Público.[70]

7.3. Enquadramento Jurídico da IA Forense no Ordenamento Angolano

O ordenamento jurídico angolano não dispõe ainda de legislação específica sobre a utilização da IA. Contudo, um conjunto de normas vigentes é directamente aplicável a esta utilização:

- A Constituição da República de Angola consagra o direito a um processo justo e equitativo e o direito à presunção de inocência,[71] que limitam a utilização de algoritmos decisórios automatizados em contextos penais sem garantia de supervisão humana efectiva e de fundamentação adequada;
- A LPDP (Lei n.º 22/11) é aplicável ao tratamento de dados pessoais realizado por sistemas de IA, impondo as obrigações gerais de licitude, proporcionalidade e segurança do tratamento;
- O Código do Processo Penal Angolano (Lei n.º 39/20) exige a fundamentação das decisões judiciais,[72] o que inclui a obrigação de fundamentar adequadamente qualquer decisão que se apoie em análises produzidas por sistemas de IA;
- O princípio da legalidade, consagrado no artigo 1.º do CPA, impõe que a tipificação dos crimes seja determinada por lei, o que limita a possibilidade de a IA substituir o juízo de tipicidade do julgador.

7.4. Desafios e Riscos da IA na Actividade Forense

---

também: AI Act (Regulamento (UE) 2024/1689), artigos 14.º e 17.º; ZAVRŠNIK, Aleš (ed.). op. cit., cap. 9.

[69]CEPEJ. Carta Ética Europeia. op. cit., Princípio 3 (Qualidade e Segurança); WACHTER, Sandra; MITTELSTADT, Brent; RUSSELL, Chris. op. cit.; PASQUALE, Frank. op. cit., cap. 1; BARFIELD, Woodrow (ed.). op. cit., cap. 7.

[70]AMERICAN BAR ASSOCIATION. Formal Opinion 512: Generative Artificial Intelligence Tools. Chicago: ABA, 2024. A Opinião conclui que os advogados podem utilizar ferramentas de IA generativa desde que cumpram os deveres de competência (Regra 1.1), supervisão (Regra 5.1), confidencialidade (Regra 1.6) e comunicação com o cliente (Regra 1.4), sendo obrigatória a verificação de todos os conteúdos gerados por IA antes da sua submissão em tribunal.

[71]CPPA (Lei n.º 39/20), artigo 97.º (dever de fundamentação das decisões judiciais: a sentença deve conter os factos provados e não provados, a indicação e exame das provas e a exposição dos motivos de facto e de direito que fundamentaram a decisão). Vide BARFIELD, Woodrow (ed.). op. cit., cap. 15.

[72]CEPEJ. Carta Ética Europeia. op. cit., Princípio 3 (Qualidade e Segurança); PASQUALE, Frank. op. cit., pp. 189-216; WACHTER, Sandra; MITTELSTADT, Brent; RUSSELL, Chris. Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR. Harvard Journal of Law & Technology, v. 31, n.º 2, 2018, pp. 841-887.

O risco de opacidade algorítmica (*black box*): muitos sistemas de IA não são explicáveis de forma inteligível por não-especialistas, o que compromete o direito de defesa e o contraditório processual.[73]

O risco de discriminação algorítmica: algoritmos treinados com dados históricos tendem a reproduzir e ampliar preconceitos e discriminações existentes, o que em contexto angolano, com dados históricos marcados por desigualdades estruturais, pode gerar decisões sistemicamente injustas.[74]

O risco de substituição indevida do juízo humano: a tendência para a "delegação cognitiva" ao algoritmo compromete a responsabilidade pessoal do magistrado ou do advogado pelas suas decisões e actuações.[75]

O risco de concentração de poder tecnológico: a dependência de sistemas de IA proprietários e externos ao sistema de justiça angolano coloca questões de soberania tecnológica e de acesso a sistemas de controlo e de auditoria.[76]

O relatório do Projecto Octopus do Conselho da Europa sobre Angola[77] identifica o reforço das capacidades forenses digitais das autoridades de investigação como uma das prioridades nacionais, incluindo a adopção criteriosa de ferramentas de IA em contextos compatíveis com o Estado de Direito.

8. ÉTICA NO USO DA INTELIGÊNCIA ARTIFICIAL NA PRÁTICA FORENSE: A PAUTA DEONTOLÓGICA

8.1. A Deontologia dos Magistrados Judiciais e o Estatuto da Função Pública

Os magistrados judiciais angolanos exercem as suas funções no quadro do Estatuto dos Magistrados Judiciais[78] e dos princípios deontológicos que decorrem da

---

[73]CEPEJ. Carta Ética Europeia. op. cit., Princípio 1 (Respeito pelos Direitos Fundamentais); FLORIDI, Luciano et al. An Ethical Framework for a Good AI Society. Minds and Machines, v. 28, 2018, pp. 689-707; BARFIELD, Woodrow (ed.). op. cit., cap. 2.

[74]AI Act (Regulamento (UE) 2024/1689), artigo 22.º (medidas de supervisão humana dos sistemas de alto risco) e artigo 9.º (sistema de gestão dos riscos); CEPEJ. Carta Ética Europeia. op. cit., Princípio 5; CONSELHO DA EUROPA. Recomendação CM/Rec(2020)1 sobre o Impacto dos Sistemas Algorítmicos nos Direitos Humanos. Estrasburgo: Conselho da Europa, 2020; ZARSKY, Tal Z. op. cit., pp. 121-125.

[75]AI Act (Regulamento (UE) 2024/1689), artigo 22.º; CEPEJ. Carta Ética Europeia. op. cit., Princípio 5; CONSELHO DA EUROPA. Recomendação CM/Rec(2020)1. op. cit.; CITRON, Danielle Keats. op. cit., pp. 1295-1313.

[76]NAÇÕES UNIDAS. Resolução A/HRC/51/L.6 (2022) — O Direito à Privacidade na Era Digital. Genebra: ACNUDH, 2022; CEPEJ. Carta Ética Europeia. op. cit., Princípio 2 (Não-Discriminação); ANGWIN, Julia et al. op. cit.; CHOULDECHOVA, Alexandra. op. cit.

[77]ANGWIN, Julia et al. Machine Bias. op. cit.; CHOULDECHOVA, Alexandra. op. cit.; DRESSEL, Julia; FARID, Hany. op. cit.; CEPEJ. Carta Ética Europeia. op. cit., Princípio 2 (Não-Discriminação); ZARSKY, Tal Z. op. cit.

[78]CEPEJ. Carta Ética Europeia. op. cit., Princípio 1 (Respeito pelos Direitos Fundamentais); FLORIDI, Luciano et al. op. cit., pp. 698-700; BARFIELD, Woodrow (ed.). op. cit., cap. 2.

Constituição e dos instrumentos internacionais ratificados por Angola, incluindo os Princípios Básicos das Nações Unidas Relativos à Independência da Judicatura e os Princípios de Bangalore sobre Conduta Judicial.[79] A pauta deontológica da magistratura judicial organiza-se em torno de seis valores nucleares: independência, imparcialidade, integridade, idoneidade, igualdade e competência.

No contexto da utilização da IA na actividade forense, estes valores deontológicos impõem deveres específicos:

- **Dever de competência digital:** o magistrado que utiliza ferramentas de IA na sua actividade jurisdicional tem o dever de compreender suficientemente o funcionamento, as limitações e os riscos dessas ferramentas para exercer sobre elas uma supervisão efectiva e informada. A ignorância tecnológica não constitui exoneração de responsabilidade;
- **Dever de fundamentação autónoma:** a decisão judicial deve sempre reflectir o juízo autónomo e responsável do magistrado. A utilização de IA como instrumento de apoio é admissível; a delegação da decisão ao algoritmo, não. O magistrado deve ser capaz de explicar e fundamentar a sua decisão independentemente da ferramenta de IA utilizada;
- **Dever de transparência processual:** quando o magistrado utilize análises produzidas por sistemas de IA na formação da sua convicção, deve divulgá-lo às partes e garantir-lhes o contraditório sobre esses elementos;
- **Dever de imparcialidade algorítmica:** o magistrado deve avaliar criticamente os resultados produzidos por sistemas de IA, tendo consciência dos riscos de viés algorítmico, e não pode basear-se em análises de risco automatizadas que discriminem com base em características protegidas.

8.2. A Deontologia do Ministério Público no Contexto da IA Forense

Os magistrados do Ministério Público angolanos estão sujeitos à Lei Orgânica do Ministério Público[80] e aos princípios deontológicos da sua função, que incluem a legalidade, a objectividade, a isenção e a lealdade processual. No contexto da IA forense, estes princípios impõem exigências específicas:

- **O dever de objectividade e isenção** impõe ao magistrado do Ministério Público que utilize a IA de forma equilibrada e crítica, não seleccionando apenas os resultados que favoreçam a acusação e ignorando os que possam beneficiar o arguido;
- **O princípio da legalidade** impõe que a recolha e utilização de prova digital assistida por IA respeite escrupulosamente as normas do CPPA sobre meios de obtenção de prova, nomeadamente os requisitos de autorização judicial para as medidas de investigação mais intrusivas;

---

[79]SUSSKIND, Richard. op. cit., pp. 198-215; CITRON, Danielle Keats. Technological Due Process. Washington University Law Review, v. 85, n.º 6, 2008, pp. 1249-1313; ZAVRŠNIK, Aleš (ed.). op. cit., cap. 5.

[80]COE/OCTOPUS. Angola: Cybercrime Country Profile. Conselho da Europa, Outubro de 2023, p. 12.

- **O dever de lealdade processual** impõe a divulgação às defesas dos métodos e ferramentas de IA utilizados na análise de prova, permitindo-lhes contestar a validade e credibilidade dessas análises;
- **O dever de actualização permanente** obriga os magistrados do Ministério Público a manterem-se informados sobre as capacidades, limitações e riscos das ferramentas de IA utilizadas na investigação criminal.

8.3. O Código de Ética da Ordem dos Advogados de Angola e a IA Forense

A Ordem dos Advogados de Angola (OAA) rege-se pelo Estatuto da Advocacia e pelo respectivo Código Deontológico,[81] que consagram os deveres fundamentais do advogado angolano: independência, lealdade, sigilo profissional, competência e urbanidade. A integração de ferramentas de IA na prática advocatícia angolana suscita questões deontológicas de crescente relevância:

- **Dever de competência e actualização:** o advogado tem o dever de se manter actualizado sobre as técnicas e instrumentos relevantes para a sua prática. No contexto actual, isso inclui a literacia suficiente sobre as ferramentas de IA utilizadas na prática jurídica para avaliar criticamente os seus resultados e identificar os seus erros;
- **Dever de sigilo profissional:** a utilização de ferramentas de IA no processamento de informações relativas a clientes suscita riscos específicos de violação do segredo profissional, designadamente quando as ferramentas utilizadas envolvem o envio de dados para servidores externos. O advogado não deve submeter a plataformas de IA genérica informações identificáveis de clientes sem o seu consentimento expresso;
- **Dever de lealdade e diligência para com o cliente:** o advogado que utiliza IA na preparação de peças processuais tem o dever de as rever e validar antes de as apresentar em tribunal. A submissão de peças geradas por IA sem revisão crítica (com o risco de conter erros factuais, jurisprudência inexistente ou "alucinações algorítmicas") pode constituir violação grave do dever de diligência;
- **Proibição de conflito de interesses:** a utilização de sistemas de IA partilhados entre múltiplos utilizadores pode gerar riscos de exposição inadvertida de informações confidenciais de clientes, constituindo potencial conflito de interesses que o advogado deve prevenir.

A OAA deve desenvolver orientações deontológicas específicas sobre a utilização da IA na prática advocatícia angolana, seguindo o exemplo de ordens congéneres que já publicaram guias de boas práticas nesta matéria, designadamente a

[81]NAÇÕES UNIDAS. Princípios Básicos Relativos à Independência da Judicatura. Adoptados pelo 7.º Congresso das Nações Unidas sobre Prevenção do Crime. Milão, 1985 (Princípio 6: "Os juízes devem ser [...] competentes e diligentes"). NAÇÕES UNIDAS. Princípios de Bangalore sobre Conduta Judicial. Resolução ECOSOC 2006/23. Nova Iorque, 2006 (Valor 6 — Competência e Diligência).

American Bar Association[82] e a Ordem dos Advogados Portuguesa.[83] Estas orientações devem abordar, pelo menos: a verificação obrigatória de peças geradas por IA; a preservação do sigilo profissional; a transparência perante os clientes sobre o uso de IA; e a responsabilidade do advogado pelos erros algorítmicos.

8.4. Princípios Éticos Transversais para o Uso da IA na Justiça Angolana

Princípio da supervisão humana: nenhuma decisão judicial ou do Ministério Público deve ser tomada de forma exclusivamente automatizada, sem supervisão e responsabilidade humanas efectivas. A IA pode auxiliar, mas não pode substituir o juízo do operador jurídico.[84]

Princípio da explicabilidade: os sistemas de IA utilizados na administração da justiça devem ser suficientemente explicáveis para que as suas conclusões possam ser compreendidas, verificadas e contestadas pelos operadores jurídicos e pelas partes processuais.[85]

Princípio da não-discriminação: a utilização de sistemas de IA não pode resultar em tratamento discriminatório com base em características protegidas, incluindo a origem étnica, o sexo, a condição económica ou social, a religião ou a orientação política.[86]

Princípio da proporcionalidade: a utilização de IA na actividade forense deve ser proporcional à finalidade prosseguida, privilegiando as ferramentas menos intrusivas e restringindo as mais invasivas aos casos em que sejam estritamente necessárias e legalmente autorizadas.[87]

Princípio da responsabilidade (*accountability*): a utilização de IA não pode diluir ou eliminar a responsabilidade pessoal do operador jurídico pelas suas actuações e

---

[82]Lei n.º 2/15, de 2 de Fevereiro (Estatuto dos Magistrados Judiciais). Luanda, 2015. O Estatuto consagra, no seu artigo 3.º, os deveres gerais dos magistrados judiciais, incluindo os deveres de independência, imparcialidade e actualização permanente.

[83]Lei n.º 14/11, de 14 de Julho (Lei Orgânica do Ministério Público). Luanda, 2011. O artigo 4.º consagra os princípios da legalidade, da objectividade, da hierarquia e da isenção como princípios estruturantes da actuação do Ministério Público angolano.

[84]UNIÃO AFRICANA. Digital Transformation Strategy for Africa (2020-2030). Adis Abeba: African Union Commission, 2020. A Estratégia identifica como objectivo prioritário a harmonização dos quadros normativos de cibersegurança, proteção de dados e inteligência artificial entre os Estados-Membros da UA.

[85]RGPD, artigo 3.º, n.º 2: o RGPD aplica-se ao tratamento de dados de titulares situados na União Europeia, independentemente de o responsável pelo tratamento se encontrar estabelecido fora da UE. Vide KUNER, Christopher. Transborder Data Flows and Data Privacy Law. Oxford: Oxford University Press, 2013, pp. 112-134.

[86]CEPEJ. Carta Ética Europeia. op. cit., Princípio 3 (Qualidade e Segurança); WACHTER, Sandra; MITTELSTADT, Brent; RUSSELL, Chris. Counterfactual Explanations Without Opening the Black Box. Harvard Journal of Law & Technology, v. 31, n.º 2, 2018, pp. 841-887; PASQUALE, Frank. The Black Box Society. op. cit., cap. 1.

[87]AI Act (Regulamento (UE) 2024/1689), artigo 22.º; CEPEJ. Carta Ética Europeia. op. cit., Princípio 5; CONSELHO DA EUROPA. Recomendação CM/Rec(2020)1. op. cit.; CITRON, Danielle Keats. Technological Due Process. Washington University Law Review, v. 85, n.º 6, 2008, pp. 1295-1313.

decisões. A responsabilidade pela utilização de IA é sempre do operador humano que a utiliza.[88]

9. PERSPECTIVAS DE EVOLUÇÃO E POLÍTICA JURÍDICA

9.1. Agenda Legislativa Prioritária

A análise crítica do quadro jurídico angolano permite identificar quatro prioridades legislativas de primeira ordem:

Primeira prioridade — Revisão e modernização da LPDP: o processo de consulta pública lançado pela APD em Março de 2025 constitui uma oportunidade histórica para dotar Angola de uma lei de protecção de dados da geração do RGPD, que incorpore os princípios da responsabilização, da privacidade por defeito, da avaliação de impacto e da portabilidade dos dados.

Segunda prioridade — Aprovação da Lei de Cibersegurança: a proposta em consulta pública deve ser aprovada em tempo útil, com particular atenção para a definição clara de infraestruturas críticas de informação e a criação de um CERT nacional com capacidade operacional real.

Terceira prioridade — Reforma processual penal digital: o CPPA deve ser complementado com disposições específicas sobre prova digital, incluindo procedimentos de preservação de dados em risco de destruição, regras sobre a cadeia de custódia da prova electrónica e mecanismos de acesso expedito a dados armazenados por operadores internacionais.

Quarta prioridade — Regulação da IA na Administração da Justiça: Angola deve desenvolver um quadro normativo específico para a utilização da IA nos processos judiciais e na actividade do Ministério Público, articulado com os instrumentos deontológicos das profissões jurídicas.

9.2. A Transformação Digital como Desafio Permanente para os Juristas

[88]Comissão Europeia, Ethics Guidelines for Trustworthy AI, 2019, p. 13-15.; Floridi, L. et. al., “AI4People_An Ethical Framework for a Good AI Society”, Minds and Machines, vol. 28, 2018, pp. 689-707.

A Estratégia de Transformação Digital para África da UA (2020-2030)[89] identifica a harmonização dos quadros normativos de cibersegurança e protecção de dados como condição indispensável para o desenvolvimento da economia digital africana. Para os advogados e juristas angolanos, a especialização em Direito Digital não é apenas uma oportunidade profissional, é uma responsabilidade deontológica. A complexidade crescente do quadro normativo digital, a aceleração do ritmo de inovação tecnológica e a emergência da IA como ferramenta forense exigem uma actualização permanente e uma abordagem interdisciplinar que combine competências jurídicas com literacia tecnológica.

10. CONCLUSÕES E RECOMENDAÇÕES

O presente artigo demonstrou que o Direito Digital angolano se encontra num momento de maturação acelerada, caracterizado pela coexistência de um núcleo normativo relevante com lacunas estruturais que urge colmatar. Angola dispõe de um quadro normativo assente em pilares identificáveis (a LPDP, a LCE, a Lei n.º 7/17 e o CPA), mas este quadro apresenta insuficiências críticas que comprometem a sua efectividade, designadamente em matéria de cibersegurança institucional, processo penal digital e regulação da inteligência artificial na prática forense.

A emergência da IA na actividade forense constitui o desafio mais urgente e menos regulado que se coloca ao sistema de justiça angolano. A ausência de normas específicas não significa ausência de obrigações: os princípios constitucionais, as normas do CPPA sobre prova e fundamentação, as obrigações da LPDP e os deveres deontológicos das profissões jurídicas já impõem um quadro de exigências que os operadores jurídicos devem respeitar no uso de ferramentas de IA, mesmo sem legislação sectorial específica.

Com base na análise realizada, formulam-se as seguintes recomendações:

- **Ao Legislador angolano:** aprovar urgentemente a revisão da LPDP alinhada com o RGPD, a Lei de Cibersegurança e complementar o CPPA com disposições específicas sobre prova digital; iniciar a elaboração de legislação específica sobre IA na administração da justiça, prevendo requisitos de transparência, supervisão humana e proibição de decisões exclusivamente automatizadas em matérias que afectem direitos fundamentais;

---

[89]CONSELHO CONSULTIVO DOS JUÍZES EUROPEUS (CCJE). Parecer n.º 22 (2019) — O Papel dos Juízes na Garantia do Estado de Direito e da Democracia. Estrasburgo: Conselho da Europa, 2019; PARLAMENTO EUROPEU. Resolução de 6 de Outubro de 2021 sobre Inteligência Artificial no Direito Penal e a sua Utilização pelas Autoridades Policiais e Judiciárias em Matérias Penais (2020/2016(INI)). Bruxelas: PE, 2021.

[90] DOMINGOS, Paulino Calei Alves; CALADO, Mateus Padoca; WAPOTA, Alberto Raimundo Watchilambi. Fuzzy system applied to search for feedback on governance in the Province of Namibe. ASRIC Journal of Engineering Sciences,. 4.2: 157, 2024.

- **Ao Conselho Superior da Magistratura Judicial e à Procuradoria-Geral da República:** desenvolver orientações específicas sobre o uso ético da IA na actividade judicial e do Ministério Público, incluindo programas de formação obrigatória em literacia digital e ética da IA para todos os magistrados;
- **À Ordem dos Advogados de Angola:** publicar orientações deontológicas específicas sobre a utilização da IA na prática advocatícia, abordando o dever de verificação das peças geradas por IA, a preservação do sigilo profissional e a responsabilidade do advogado pelos erros algorítmicos;
- **À Agência de Protecção de Dados:** emitir orientações sectoriais sobre o tratamento de dados pessoais por sistemas de IA no contexto forense, clarificando as obrigações das entidades que utilizam estes sistemas no âmbito da administração da justiça;
- **A todos os operadores jurídicos:** investir na sua própria literacia digital e ética da IA, assumindo a responsabilidade deontológica de não delegar ao algoritmo decisões que são, por natureza, de responsabilidade humana.

Angola tem potencial para assumir um papel de liderança na África austral no desenvolvimento de um quadro normativo do Direito Digital e da IA forense que seja simultaneamente robusto, eticamente orientado e adequado às especificidades do seu desenvolvimento. O sucesso deste processo dependerá da qualidade da contribuição de todos os operadores jurídicos para este desafio civilizacional.

11. REFERÊNCIAS BIBLIOGRÁFICAS E NORMATIVAS

A) Legislação Principal Angolana

ANGOLA. Constituição da República de Angola. Lei Constitucional n.º 23/10, de 11 de Fevereiro de 2010. Diário da República, I Série, n.º 23. Luanda, 2010.

ANGOLA. Lei n.º 22/11, de 17 de Junho — Lei de Protecção de Dados Pessoais (LPDP). Diário da República, I Série, n.º 114. Luanda, 2011.

ANGOLA. Lei n.º 23/11, de 20 de Junho — Lei das Comunicações Electrónicas e dos Serviços da Sociedade da Informação (LCE). Diário da República, I Série, n.º 116. Luanda, 2011.

ANGOLA. Lei n.º 7/17, de 16 de Fevereiro — Lei de Protecção das Redes e Sistemas Informáticos. Diário da República, I Série, n.º 30. Luanda, 2017.

ANGOLA. Lei n.º 38/20, de 11 de Novembro — Código Penal Angolano (CPA). Diário da República, I Série, n.º 179. Luanda, 2020.

ANGOLA. Lei n.º 39/20, de 11 de Novembro — Código do Processo Penal Angolano (CPPA). Diário da República, I Série, n.º 179. Luanda, 2020.

B) Legislação Complementar Angolana

ANGOLA. Lei n.º 2/15, de 2 de Fevereiro — Estatuto dos Magistrados Judiciais. Luanda, 2015.

ANGOLA. Lei n.º 14/11, de 14 de Julho — Lei Orgânica do Ministério Público. Luanda, 2011.

ANGOLA. Lei n.º 17/90, de 20 de Outubro — Estatuto Geral dos Funcionários Públicos e Agentes do Estado (e alterações posteriores). Luanda, 1990.

ANGOLA. Lei n.º 1/04, de 13 de Fevereiro — Lei das Sociedades Comerciais. Luanda, 2004.

ANGOLA. Lei n.º 13/15 — Lei da Cooperação Judiciária Internacional em Matéria Penal. Luanda, 2015.

ANGOLA. Resolução n.º 33/19, de 9 de Julho — Ratificação da Convenção da UA sobre Cibersegurança e Protecção de Dados Pessoais. Luanda, 2019.

ANGOLA. Banco Nacional de Angola. Aviso n.º 2/2021 — Gestão de Risco das Tecnologias de Informação e Comunicação nas Instituições Financeiras. Luanda, 2021.

ANGOLA. Agência de Protecção de Dados (APD). Projecto de Revisão da Lei n.º 22/11: Consulta Pública (Março-Abril 2025). Disponível em: <https://www.apd.ao>. Luanda, 2025.

ANGOLA. Ministério das Telecomunicações, Tecnologias de Informação e Comunicação Social (MINTTICS). Proposta de Lei da Cibersegurança (em consulta pública). Disponível em: <https://consultapublica.minttics.gov.ao>. Luanda, 2023/2024.

ORDEM DOS ADVOGADOS DE ANGOLA. Estatuto da Advocacia e Código Deontológico da Advocacia Angolana. Luanda: OAA.

C) Instrumentos Internacionais e Regionais

CONSELHO DA EUROPA. Convenção sobre a Cibercriminalidade (Convenção de Budapeste). ETS n.º 185, 23 de Novembro de 2001. Em vigor desde 1 de Julho de 2004.

CONSELHO DA EUROPA. 2.º Protocolo Adicional à Convenção de Budapeste (CETS n.º 224). 2022.

NAÇÕES UNIDAS. Princípios Básicos Relativos à Independência da Judicatura. Adoptados pelo 7.º Congresso das Nações Unidas sobre Prevenção do Crime. Milão, 1985.

NAÇÕES UNIDAS. Princípios de Bangalore sobre Conduta Judicial. Resolução ECOSOC 2006/23. Nova Iorque, 2006.

UNIÃO AFRICANA. Convenção sobre Cibersegurança e Protecção de Dados Pessoais (Convenção de Malabo). 27 de Junho de 2014. Em vigor desde 8 de Junho de 2023.

UNIÃO AFRICANA. Digital Transformation Strategy for Africa (2020-2030). Adis Abeba: African Union Commission, 2020.

UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de Abril de 2016 (RGPD). Jornal Oficial da União Europeia, L 119. Bruxelas, 2016.

UNIÃO EUROPEIA. Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de Junho de 2024 (AI Act). Jornal Oficial da União Europeia, L 1689. Bruxelas, 2024.

ISO/IEC 27001:2022 — Information Security Management Systems. Genebra: ISO, 2022.

NIST — National Institute of Standards and Technology. Cybersecurity Framework 2.0. Gaithersburg: NIST, 2024.

D) Doutrina

AMERICAN BAR ASSOCIATION. Formal Opinion 512: Generative Artificial Intelligence Tools. Chicago: ABA, 2024.

ANGWIN, Julia et al. Machine Bias. ProPublica, 23 de Maio de 2016. Disponível em: <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>.

CARRIER, Brian. File System Forensic Analysis. Boston: Addison-Wesley, 2005.

CASEY, Eoghan; FELLOWS, Geoff A. Network Investigation Methodology. Oxford: Academic Press, 2020.

CITRON, Danielle Keats. Technological Due Process. Washington University Law Review, v. 85, n.º 6, 2008, pp. 1249-1313.

COMISSÃO EUROPEIA PARA A EFICIÊNCIA DA JUSTIÇA (CEPEJ). Carta Ética Europeia sobre o Uso da Inteligência Artificial nos Sistemas Judiciais e no seu Ambiente. Estrasburgo: Conselho da Europa, 2018.

CONSELHO CONSULTIVO DOS JUÍZES EUROPEUS (CCJE). Parecer n.º 22 (2019) — O Papel dos Juízes na Garantia do Estado de Direito e da Democracia. Estrasburgo: Conselho da Europa, 2019.

CONSELHO DA EUROPA. Recomendação CM/Rec(2020)1 sobre o Impacto dos Sistemas Algorítmicos nos Direitos Humanos. Estrasburgo: Conselho da Europa, 2020.

DRESSEL, Julia; FARID, Hany. The Accuracy, Fairness, and Limits of Predicting Recidivism. Science Advances, v. 4, n.º 1, 2018.

NAÇÕES UNIDAS. Resolução A/HRC/51/L.6 (2022) — O Direito à Privacidade na Era Digital. Genebra: ACNUDH, 2022.

NIST. Digital Forensics Framework. Gaithersburg: NIST Special Publication 800-86, 2006 (actualização 2021).

ORGANISATION INTERNATIONALE DE LA FRANCOPHONIE. Justice numérique en Afrique: état des lieux et perspectives. Paris: OIF, 2022.

PARLAMENTO EUROPEU. Resolução de 6 de Outubro de 2021 sobre Inteligência Artificial no Direito Penal e a sua Utilização pelas Autoridades Policiais e Judiciárias em Matérias Penais (2020/2016(INI)). Bruxelas: PE, 2021.

BARFIELD, Woodrow (ed.). The Cambridge Handbook of the Law of Algorithms. Cambridge: Cambridge University Press, 2021.

CHOULDECHOVA, Alexandra. Fair Prediction with Disparate Impact: A Study of Bias in Recidivism Prediction Instruments. Big Data, v. 5, n.º 2, 2017, pp. 153-163.

CITRON, Danielle Keats. Technological Due Process. Washington University Law Review, v. 85, n.º 6, 2008, pp. 1249-1313.

FLORIDI, Luciano et al. An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations. Minds and Machines, v. 28, 2018, pp. 689-707.

PASQUALE, Frank. The Black Box Society: The Secret Algorithms That Control Money and Information. Cambridge: Harvard University Press, 2015.

REILING, Dory. Technology for Justice: How Information Technology Can Support Judicial Reform. Leiden: Leiden University Press, 2009.

SUSSKIND, Richard. Online Courts and the Future of Justice. Oxford: Oxford University Press, 2019.

WACHTER, Sandra; MITTELSTADT, Brent; RUSSELL, Chris. Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR. Harvard Journal of Law & Technology, v. 31, n.º 2, 2018, pp. 841-887.

ZARSKY, Tal Z. The Trouble with Algorithmic Decisions: An Analytic Road Map to Examine Efficiency and Fairness in Automated and Opaque Decision Making. Science, Technology, & Human Values, v. 41, n.º 1, 2016, pp. 118-132.

ZAVRŠNIK, Aleš (ed.). Automating Justice: The Social, Ethical and Legal Implications of Automated Decision-Making Systems in the Criminal Justice System. Cham: Springer, 2021.

ASCENSÃO, José de Oliveira. Direito da Internet e da Sociedade de Informação. Coimbra: Almedina, 2012.

BONA, Maurício. Tratado de Direito Digital e Processo Eletrônico. 2.ª ed. São Paulo: LTr, 2021.

BYGRAVE, Lee A. Data Privacy Law: An International Perspective. Oxford: Oxford University Press, 2014.

CASTELLS, Manuel. A Sociedade em Rede. 4.ª ed. Lisboa: Fundação Calouste Gulbenkian, 2007.

COE/OCTOPUS. Angola: Cybercrime Country Profile. Conselho da Europa, Outubro de 2023.

CORDEIRO, A. Barreto Menezes. Direito da Protecção de Dados. Coimbra: Almedina, 2020.

DIAS PEREIRA, Alexandre Libório. Direito Digital. Coimbra: Almedina, 2018.

DOMINGOS, Paulino Calei Alves; CALADO, Mateus Padoca; WAPOTA, Alberto Raimundo Watchilambi. Fuzzy system applied to search for feedback on governance in the Province of Namibe. ASRIC Journal of Engineering Sciences, Disponível em: https://asric.africa/engineering-sciences/asric-journal-engineering-sciences-2024-v4-i2/fuzzy-system-applied-search. 4.2: 157, 2024.

DONEDA, Danilo. Da Privacidade à Protecção de Dados Pessoais. 2.ª ed. São Paulo: Thomson Reuters Brasil, 2019.

FRANCISCO, João A. Direito da Informática: Direito das Novas Tecnologias de Informação e Comunicação. Luanda: Editora das Letras, 2018.

FRANCISCO, João A. Proteção de Dados Pessoais em Angola: Da Lei 22/11 ao desafio do Big Data. Revista de Direito Público Angolano, n.º 4, 2020, pp. 45-72.

GREENLEAF, Graham. Global Tables of Data Privacy Laws and Bills. Privacy Laws & Business International Report, n.º 157, 2019.

INOVALEGAL. A necessidade de inclusão da sabotagem informática no Anteprojecto de Código Penal angolano. inovalegal.org, Fevereiro de 2020.

KUNER, Christopher. Transborder Data Flows and Data Privacy Law. Oxford: Oxford University Press, 2013.

MAKULILO, Alexander Boniface. Africa and the Global Data Protection Landscape. Baden-Baden: Nomos, 2014.

MAKULILO, Alexander Boniface. Privacy and Data Protection in Africa: A State of the Art. International Data Privacy Law, v. 2, n.º 3, 2012, pp. 163-178.

NUNES, Duarte Rodrigues. Os Crimes previstos na Lei do Cibercrime. Coimbra: GestLegal, 2019.

PINTO, F. L. A responsabilidade penal das pessoas colectivas no Código Penal Angolano. Direito em Debate, n.º 3, 2022, pp. 88-110.

PLMJ/RVA. Dados Pessoais e Ciber-segurança em Angola. Nota Informativa. Luanda, Janeiro de 2024.

PTI.AO. A cibersegurança e os crimes informáticos no ordenamento jurídico angolano. Luanda, Agosto de 2023. Disponível em: <https://www.pti.ao>.

QUELHAS, I. O Novo Código Penal Angolano: Principais Inovações. Actualidad Jurídica Angola, n.º 15, 2021.

ROMEO CASABONA, Carlos María. De los Delitos Informáticos al Cibercrimen. In: El Cibercrimen: Nuevos Retos Jurídico Penales. Granada: Comares, 2006.

SÉRVULO & ASSOCIADOS. Novo Código Penal Angolano. Nota de Conhecimento. Lisboa/Luanda, Novembro de 2020.

SILVA, Paulo. Crimes Informáticos no novo Código Penal Angolano. Revista Jurídica Angolana, n.º 7, 2021, pp. 112-145.

UNIÃO AFRICANA. Digital Transformation Strategy for Africa (2020-2030). Adis Abeba: African Union Commission, 2020.

VERDELHO, Pedro; BRAVO, Rogério; ROCHA, Manuel Lopes. Leis do Cibercrime, vol. 1. Lisboa: Centro Atlântico, 2003.