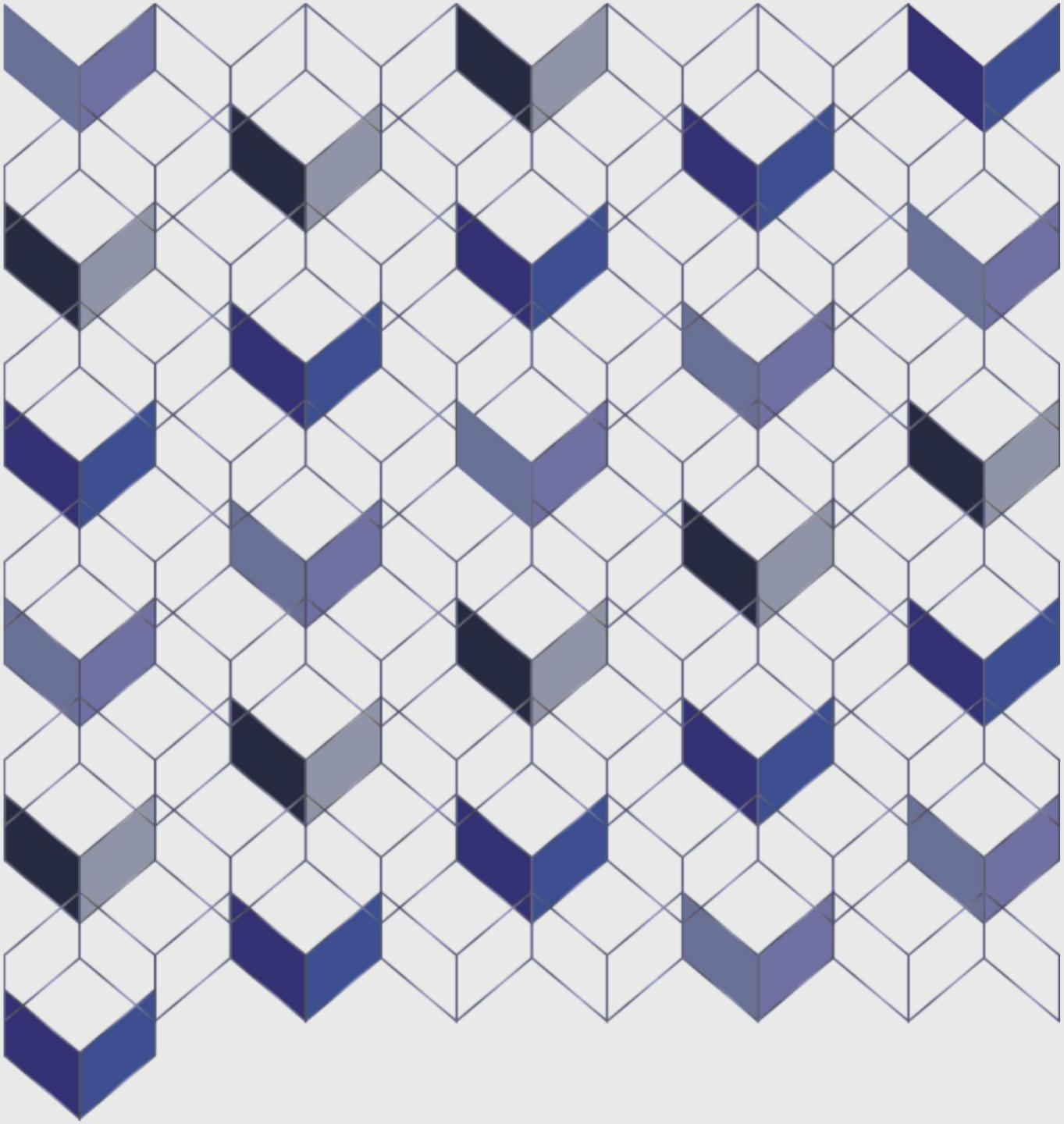
Jornal Jurídico

2025
Volume 8, Número 1
ISSN Online: 2184-3082



pontéditora
Travessia para o Conhecimento

Ficha Técnica

- **ISSN Online:** 2975-8289
- **Frequência:** Semestral
- **Propriedade:** Ponteditora, Sociedade Unipessoal, Lda.
- **NIPC:** 514 111 054
- **Composição do capital do proprietário:** 10 000€, 100% detido por Ana Leite, doutoranda
- **Gestão (não remunerada):** Eduardo Leite, Ph.D.
- **Localização:** Startup Madeira — Campus da Penteada, 9020-105, Funchal, Madeira, Portugal
- **Contacto principal:**
  - Eduardo Leite
  - Universidade da Madeira
  - +351 291 705 180
  - eduardo.leite@staff.uma.pt
- **Contacto de apoio:**
  - Ponteditora
  - +351 291 723 010
  - geral@ponteditora.org

Equipa Editorial

Estatuto Editorial

I — O Jornal Jurídico (J^2) é uma publicação periódica. Propriedade: Ponteditora.

II — Aberta a novos mundos e caminhos, reforçando a sua missão, de longo prazo, de reunir e disseminar conhecimento e aproximar as comunidades científicas dedicadas às ciências sociais. O J^2 publica, preferencialmente, em português e inglês, mas aceita outras línguas sempre que a publicação o justificar. O J^2 aceita contribuições em português anterior ao Acordo Ortográfico (AO) e pelo AO, em conformidade e respeito pela intenção expressa pelos/as autores/as em nota de intenção expressa nos manuscritos submetidos.

III — A linha editorial do J^2 publica textos dedicados às práticas e representações do campo das ciências sociais, em áreas como: direito, criminologia, ciências políticas, administração pública, sociologia e antropologia.

IV — A missão do J^2 é promover o estudo das ciências sociais e estimular a pesquisa e a elaboração de estudos e ensaios a nível global.

V — O J^2 é publicado semestralmente em formato digital (acesso aberto).

VI — Os números do J^2 terão aproximadamente de 80 a 180 páginas A4.

VII — O J^2 apresenta um conselho editorial técnico, aberto a académicos, investigadores/as, profissionais e executivos de diversas organizações e empresas relacionadas com a pesquisa das práticas e representações do campo das ciências sociais, assumindo-se como uma plataforma internacional, global e englobante que visa a promoção destas práticas e representações.

VIII — O J^2 publica e revê artigos académicos e científicos originais de acordo com critérios de relevância e qualidade científica.

IX — A aprovação de manuscritos para publicação é regulamentada por critérios de relevância, interesse, qualidade científica e respeito pela pluralidade de perspetivas. O J^2 assume-se como independente de qualquer poder político, ideológico ou económico, sendo orientado por critérios de rigor, isenção e inclusão.

X — O J^2 publica em português e inglês, sendo aceites outras línguas se o texto for submetido em versão bilíngue e/ou em caso de um número especial cuja temática o justifique. Cada artigo inclui um título, resumo e palavras-chave.

XI — O J^2 edita tanto Números Regulares como Números Especiais, confiados a investigadores credenciados nas respetivas áreas de especialização (Diretrizes para Revisores/as por Pares), sob a supervisão e aprovação da Equipa Editorial. Toda a colaboração está sujeita a um processo de seleção e revisão exigente com base na arbitragem científica de duas maneiras, por dupla revisão anónima ou aberta por pares.

XII — Visando os mais elevados padrões éticos na publicação, a Equipa Editorial do J^2 inspira o seu Código de Ética nas diretrizes estabelecidas pelo Committee on Publication Ethics (COPE); Declaração de Helsínquia (WMA); International Committee of Medical Journal Editors (ICMJE); Animal Research: Reporting of In Vivo Experiments (ARRIVE). Este código define as responsabilidades de todas as partes envolvidas no ato de publicação no J^2.

XIII — O J^2 pretende promover a troca de ideias, experiências e projetos entre autores/as e editores/as, contribuindo para a reflexão das suas editorias a nível global.

XIV — O J^2 disponibiliza Diretrizes para Autores/as para a apresentação e publicação de manuscritos.

XV — A Equipa Editorial do J^2 está empenhada em garantir o respeito pelos princípios éticos e ética profissional dos/as jornalistas, bem como pela boa fé dos/as leitores/as, nos termos do n.º 1 do artigo 17.º da Lei da Imprensa.

.

Índice

Editorial

10.29073/j2.v8i1.1130

Patrícia Azevedo, Instituto Politécnico do Porto, Portugal, patricia_anjos_azevedo86@hotmail.com.

A presente edição do *J2 – Jornal Jurídico* dedica-se a um dos domínios mais dinâmicos e desafiantes do pensamento jurídico contemporâneo: a interseção entre o Direito, a tecnologia e a proteção de dados pessoais.

Num contexto marcado pela crescente digitalização das relações sociais e económicas, a centralidade da proteção de dados, enquanto recurso estruturante das sociedades modernas, impõe ao Direito um esforço contínuo de adaptação, problematização e inovação normativa.

Este editorial tem como função a de refletir sobre temas atuais, propor debates, orientar a linha editorial e fornecer uma perspetiva crítica sobre assuntos de relevância para a comunidade científica ou jurídica[1]. O editorial serve ainda para sintetizar tendências do pensamento jurídico, comentar decisões recentes do poder judiciário ou mudanças legislativas, e indicar temas emergentes para estudo e reflexão[2]. Dessa forma, pretendemos apresentar um guia interpretativo, auxiliando os leitores a compreender a relevância dos temas apresentados[3].

A evolução tecnológica, em particular no domínio da inteligência artificial e do tratamento automatizado de dados, tem vindo a reconfigurar profundamente os modelos tradicionais de regulação, colocando em evidência a insuficiência de respostas jurídicas assentes em paradigmas estritamente formais. Neste âmbito, a proteção de dados pessoais afirma-se não apenas como um domínio autónomo do Direito, mas como um verdadeiro eixo estruturante de garantia dos direitos fundamentais em ambiente digital.

Os contributos reunidos neste número refletem de forma particularmente significativa esta transformação, abordando questões que se situam no cruzamento entre a dogmática jurídica, a arquitetura tecnológica e as exigências regulatórias emergentes.

Desde logo, a problemática do consentimento no âmbito do regime de proteção de dados é revisitada à luz das exigências de verificabilidade e operacionalização em ambientes digitais complexos, apontando para a necessidade de uma reconceptualização que ultrapasse a sua dimensão meramente formal e assegure uma efetiva capacidade de controlo por parte dos titulares dos dados.

Ainda neste domínio, a análise do papel do encarregado de proteção de dados evidencia a importância desta figura enquanto elemento central na concretização prática das exigências do regime jurídico aplicável, funcionando como interface entre organizações, titulares de dados e autoridades de controlo.

Complementarmente, a reflexão em torno dos *cookies* e das práticas associadas à recolha e tratamento de dados em ambiente digital sublinha os desafios persistentes em matéria de transparência, consentimento informado e equilíbrio entre interesses económicos e direitos fundamentais.

---

[1] VASCONCELLOS, V. G. de. (2017). Editorial: A função do periódico científico e do editor para a produção do conhecimento no Direito e nas ciências criminais. Revista Brasileira de Direito Processual Penal, v. 3, n. 1, p. 9 17.
DOI: 10.22197/rbdpp.v3i1.34
Disponível em: https://revista.ibraspp.com.br/RBDPP/article/view/34

[2] PENG, P.-C.; COLEMAN, F.T. (2024). Editorial viewpoints of scientific publishing for early career research scientists. BMC Proceedings, v. 18, art. 4.
DOI: 10.1186/s12919-023-00286-7
Disponível em: https://bmcproc.biomedcentral.com/articles/10.1186/s12919-023-00286-7

[3] MRYGLOD, O., HOLOVATCH, Y., & MRYGLOD, I. (2011). Editorial process in scientific journals: analysis and modeling. https://arxiv.org/abs/1109.6211

Porém, a presente edição alarga o seu âmbito para além da dimensão estritamente normativa, integrando contributos que exploram a vertente técnica e operacional da proteção de dados e da cibersegurança. Neste sentido, a análise dos procedimentos de investigação forense digital aplicados a dispositivos móveis em Portugal evidencia a crescente relevância da prova digital e os desafios associados à sua obtenção, preservação e valoração em contexto jurídico.

Por outro lado, a problematização de fenómenos como a cibersextorsão revela a necessidade de uma delimitação conceptual rigorosa que permita uma resposta jurídica adequada a novas formas de criminalidade emergente, marcadas pela utilização intensiva de meios digitais e pela amplificação dos seus impactos na esfera pessoal das vítimas.

Particular destaque merece, igualmente, a reflexão em torno da utilização de sistemas de inteligência artificial em processos de decisão, quer no contexto da triagem automatizada de currículos, quer no âmbito do apoio à decisão judicial. Estes contributos evidenciam, de forma clara, os riscos associados à reprodução de vieses, à opacidade algorítmica e à potencial erosão de princípios fundamentais como a igualdade, a imparcialidade e a transparência. Simultaneamente, apontam para a necessidade de desenvolver mecanismos de mitigação e modelos de governação que assegurem uma utilização ética, responsável e juridicamente conforme destas tecnologias.

No seu conjunto, os trabalhos agora publicados ilustram a complexidade dos desafios colocados ao Direito num ambiente cada vez mais mediado por sistemas tecnológicos avançados. A articulação entre inovação e regulação, entre eficiência e garantia de direitos, emerge como uma das questões centrais do nosso tempo, exigindo respostas que sejam simultaneamente tecnicamente informadas e juridicamente robustas.

A presente edição reafirma, assim, o compromisso do *J2 – Jornal Jurídico* com a promoção de uma investigação jurídica rigorosa, crítica e atenta às transformações estruturais da sociedade contemporânea. Ao proporcionar um espaço de reflexão interdisciplinar, a revista contribui para a construção de um pensamento jurídico capaz de enfrentar os desafios do presente e de antecipar os contornos do futuro.

Por fim, cumpre expressar um agradecimento a todos os autores, revisores e colaboradores que tornaram possível esta edição. O seu contributo é essencial para a consolidação de um projeto editorial que se pretende exigente, relevante e alinhado com os mais elevados padrões da produção científica.

Convida-se, assim, a comunidade académica a uma leitura crítica e aprofundada dos textos agora publicados, na expectativa de que este número possa contribuir para o desenvolvimento do debate jurídico em torno das questões fundamentais que marcam a era digital.

Declaração Ética

Conflito de Interesse: Nada a declarar. **Financiamento:** Nada a declarar.

Do consentimento formal ao consentimento verificável: contributos para uma arquitetura jurídico-digital de gestão de consentimentos no âmbito do RGPD

From formal consent to verifiable consent: contributions to a legal-digital signature management architecture under the GDPR

10.29073/j2.v8i1.1121

Recebido: 26 de fevereiro de 2026.
Aprovado: 28 de março de 2026.
Publicado: 04 de abril de 2026.

Autor/a 1 (Correspondente): Sílvia Catarina Ferreira, ESTG-IPP, Portugal, cfsolicitadora@gmail.com.
Autor/a 2: Patrícia Azevedo, ESTG-IPP, Portugal, pamv@estg.ipp.pt.
Autor/a 3: Marco Filipe Gomes, ESTG-IPP, Portugal, mfg@estg.ipp.pt.

Resumo

O consentimento constitui um dos fundamentos de licitude do tratamento de dados pessoais no quadro do Regulamento (UE) 2016/679, assumindo um papel central na tutela da autodeterminação informacional do titular dos dados. Todavia, a crescente digitalização das relações sociais, comerciais e administrativas revelou um desfasamento entre a construção normativa do consentimento e a forma como este é efetivamente recolhido nas plataformas digitais.

A repetição de pedidos de consentimento, a complexidade informacional, a utilização de interfaces manipulativas e a fragmentação dos mecanismos de escolha contribuem para a desmaterialização do consentimento enquanto ato jurídico livre, específico, informado e inequívoco. Como tem sido salientado pela doutrina e pela literatura especializada, a proteção de dados não pode ser reduzida a um formalismo procedimental, exigindo antes condições reais de controlo pelo titular dos dados (Bygrave, 2014; Menezes Cordeiro, 2022; Solove, 2010). A dissertação que está na base deste artigo parte precisamente desse problema e propõe uma reflexão jurídico-computacional sobre a necessidade de mecanismos mais transparentes, interoperáveis e auditáveis de gestão do consentimento.

Com base numa metodologia qualitativa, exploratória e descritiva, assente na análise jurídica, revisão técnico-científica e comparação de modelos existentes de gestão de consentimentos, sustenta-se que os mecanismos atualmente predominantes continuam excessivamente orientados para as necessidades de conformidade dos responsáveis pelo tratamento e insuficientemente centrados no titular dos dados.

Em resposta a estas limitações, propõe-se a reflexão sobre uma arquitetura jurídico-computacional orientada à gestão centralizada de consentimentos, alicerçada em princípios de *privacy by design*, interoperabilidade, segurança, rastreabilidade e auditabilidade, em linha com a literatura sobre proteção de dados desde a conceção e governação tecnológica da privacidade (Cavoukian, 2009; Giannopoulou, 2021; ISO/IEC 29100, 2011; ISO/IEC 27560, 2023). Tal proposta não visa substituir o regime jurídico do RGPD, mas antes contribuir para a sua efetivação material, reforçando a transparência, a prova do consentimento, a revogabilidade, a granularidade e a *accountability* no tratamento de dados pessoais.

Palavras-Chave: Arquitetura Computacional; Autodeterminação Informacional; Consentimento; Proteção de Dados Pessoais; RGPD.

Abstract

Consent constitutes one of the legal bases for the processing of personal data under Regulation (EU) 2016/679, playing a central role in protecting the informational self-determination of the data subject. However, the

increasing digitalization of social, commercial, and administrative relations has revealed a gap between the normative construction of consent and the way it is actually collected on digital platforms.

The repetition of consent requests, informational complexity, the use of manipulative interfaces, and the fragmentation of choice mechanisms contribute to the dematerialization of consent as a free, specific, informed, and unambiguous legal act. As has been highlighted by doctrine and specialized literature, data protection cannot be reduced to procedural formalism, but rather requires real conditions of control by the data subject (Bygrave, 2014; Menezes Cordeiro, 2022; Solove, 2010). The dissertation that forms the basis of this article stems precisely from this problem and proposes a legal-computational reflection on the need for more transparent, interoperable, and auditable consent management mechanisms.

Based on a qualitative, exploratory, and descriptive methodology, grounded in legal analysis, technical-scientific review, and comparison of existing consent management models, it is argued that the currently predominant mechanisms remain excessively oriented towards the compliance needs of data controllers and insufficiently focused on the data subject.

In response to these limitations, a reflection on a legal-computational architecture oriented towards the centralized management of consents is proposed, based on the principles of privacy by design, interoperability, security, traceability, and auditability, in line with the literature on data protection from the design stage and technological governance of privacy (Cavoukian, 2009; Giannopoulou, 2021; ISO/IEC 29100, 2011; ISO/IEC 27560, 2023). This proposal does not aim to replace the legal framework of the GDPR, but rather to contribute to its effective implementation, reinforcing transparency, proof of consent, revocability, granularity, and accountability in the processing of personal data.

Keywords: Computer Architecture; Consent; GDPR; Informational Self-Determination; Personal Data Protection.

1. Introdução

A proteção de dados pessoais constitui, hoje, um dos domínios mais relevantes da contemporaneidade jurídica, precisamente porque a intensificação das interações digitais veio transferir para o ambiente tecnológico uma parte substancial da vida privada, económica e relacional dos indivíduos. A recolha e o tratamento de dados pessoais deixaram de ser fenómenos marginais para se converterem em condição estrutural do funcionamento de plataformas, serviços digitais e modelos de negócio assentes na circulação informacional. Neste contexto, o Regulamento Geral sobre a Proteção de Dados surge como instrumento de harmonização normativa e de reforço da posição jurídica do titular dos dados, procurando assegurar que o tratamento seja realizado de forma lícita, transparente e respeitadora dos direitos fundamentais, numa linha já antecipada por autores como Bygrave (2014) e Lynskey (2015). A própria dissertação que serve de base a este artigo parte deste enquadramento, reconhecendo que a proteção de dados é simultaneamente um desafio jurídico e tecnológico e que a resposta regulatória europeia não pode ser dissociada das transformações técnicas que moldam o ecossistema digital.

Entre os vários fundamentos de licitude previstos no RGPD, o consentimento ocupa um lugar particularmente sensível. A sua centralidade decorre do facto de funcionar como expressão da vontade do titular dos dados e como mecanismo através do qual se pretende assegurar o controlo individual sobre o uso da informação pessoal. No plano normativo, o consentimento é configurado como manifestação de vontade livre, específica, informada e inequívoca. No plano prático, porém, o seu exercício tem vindo a ser progressivamente enfraquecido por mecanismos massificados de recolha, por interfaces desenhadas para induzir comportamentos rápidos e por um contexto de saturação cognitiva que reduz o ato de consentir a uma mera formalidade operacional, como assinalam Schermer et al. (2014), Utz et al. (2019) e Menezes Cordeiro (2018, 2022). É essa fratura entre forma jurídica e substância material que justifica a presente análise.

A questão central a que este artigo procura responder pode formular-se nos seguintes termos: pode o consentimento, tal como hoje é recolhido no ambiente digital, continuar a ser entendido como instrumento

idóneo de autodeterminação informacional? A dissertação de origem identifica como principais fatores críticos a fadiga do consentimento, o formalismo da recolha, os *dark patterns* e o paradoxo da privacidade, articulando estes fenómenos com a insuficiência das atuais plataformas de gestão de consentimento, sobretudo no que respeita à centralização, interoperabilidade, usabilidade e prova da validade do consentimento. Em consequência, o estudo não se limita à crítica do modelo vigente, antes avança para a formulação de uma proposta conceptual de arquitetura computacional juridicamente orientada, destinada a reforçar a posição do titular dos dados e a tornar mais efetivos os princípios estruturantes do RGPD.

2. O Consentimento no RGPD: Entre Fundamento de Licitude e Expressão da Autodeterminação Informacional

O consentimento não pode ser lido apenas como uma cláusula técnica de validação do tratamento de dados. A sua importância radica, antes de mais, na função que desempenha no sistema de proteção de dados: por um lado, constitui fundamento de licitude; por outro, representa a exteriorização jurídica do poder do titular sobre os seus próprios dados. Esta dupla dimensão é claramente compatível com a leitura proposta por Menezes Cordeiro (2018, 2022), Pinheiro (2015) e Bygrave (2014), para quem a proteção de dados deve ser compreendida como expressão de autonomia e controlo, e não apenas como disciplina formal de circulação informacional. A dissertação sublinha precisamente esta articulação, salientando que o consentimento funciona simultaneamente como requisito de licitude e como mecanismo de confiança nas relações digitais, na medida em que permite ao titular controlar a utilização da informação que lhe diz respeito.

O problema é que a força normativa desta construção se fragiliza quando o consentimento deixa de ser prestado num ambiente de verdadeira compreensão e liberdade. A exigência legal de que a vontade seja livre, específica, informada e inequívoca pressupõe um contexto relacional em que o titular conheça, em termos minimamente inteligíveis, a finalidade do tratamento, os intervenientes relevantes, o alcance da autorização conferida e a possibilidade real de recusar ou revogar. Ora, quando o consentimento se converte em gesto repetitivo, apressado e cognitivamente saturado, a preservação da sua substância torna-se altamente duvidosa. Como observam Schermer et al. (2014), uma maior proliferação formal do consentimento pode, paradoxalmente, conduzir a um consentimento materialmente mais fraco. O que se mantém é a aparência formal do ato; o que se perde é a sua densidade jurídica.

A erosão material do consentimento torna ainda mais evidente uma tensão estruturante do direito da proteção de dados contemporâneo: a de saber se a autonomia individual continua a ser adequadamente protegida por um modelo que, embora juridicamente exigente, é operacionalizado através de mecanismos digitais que não foram concebidos para favorecer reflexão, mas antes rapidez, adesão e fricção mínima para o acesso ao serviço. Por isso, autores como Solove (2010), Nissenbaum (2010) e Pavlou (2011) têm defendido que a privacidade e a autodeterminação não podem ser avaliadas apenas a partir da existência de uma escolha formal, mas antes da qualidade do contexto em que essa escolha ocorre.

3. A Crise do Consentimento no Ambiente Digital

Uma das principais contribuições da dissertação consiste em mostrar que o consentimento em ambiente digital atravessa uma crise de efetividade. Tal crise manifesta-se, desde logo, no fenómeno da fadiga do consentimento. O utilizador médio é permanentemente confrontado com *banners*, *pop-ups*, caixas de seleção, pedidos de aceitação de políticas de privacidade e múltiplos avisos de cookies, o que produz uma sobrecarga cognitiva incompatível com um processo decisório minimamente ponderado. O consentimento, em vez de representar uma escolha informada, transforma-se num reflexo de navegação. Esta crítica encontra eco em trabalhos como os de Utz et al. (2019), Nouwens et al. (2020) e Leslie John (2018), que mostram como os avisos e interfaces de consentimento falham frequentemente na promoção de decisões genuinamente esclarecidas.

A esta fadiga junta-se o formalismo da recolha. Em muitos contextos, o consentimento é apresentado não como expressão jurídica de autodeterminação, mas como simples etapa instrumental para aceder ao conteúdo, concluir uma compra ou continuar a utilizar uma plataforma. Tal realidade é agravada por práticas de agregação

e simplificação abusiva, em que diferentes finalidades, destinatários ou interesses de terceiros são colocados sob uma aparência de aceitação global, sem verdadeira granularidade. Trabalhos como os de Machuletz e Böhme (2020) e Budin-Ljøsne et al. (2017), ainda que em contextos distintos, sublinham a importância de modelos mais granulares, dinâmicos e compreensíveis de gestão do consentimento. A dissertação chama igualmente a atenção para o problema do consentimento prestado em favor de "fornecedores" ou "parceiros" não individualizados, sublinhando a incompatibilidade dessa prática com as exigências de especificidade, transparência e prova do consentimento.

Outro elemento central da crise é representado pelos *dark patterns*. A literatura recente tem demonstrado que as interfaces podem ser desenhadas de forma a influenciar decisões, desviando o utilizador da opção que melhor protege os seus interesses. Mathur et al. (2019a, 2019b), Nouwens et al. (2020), Kyi et al. (2023) e Berens et al. (2024) evidenciam que o design manipulativo não constitui um problema marginal, mas antes um padrão recorrente em *websites, banners* de *cookies* e ambientes digitais diversos. Em matéria de consentimento, isto traduz-se frequentemente na colocação em destaque de opções como "aceitar tudo", na ocultação da recusa em menus secundários, na assimetria visual entre aceitar e rejeitar, ou ainda na utilização de linguagem ambígua e percursos de decisão deliberadamente enviesados. Não se trata de um problema meramente estético ou ergonómico. Trata-se, antes, de um problema jurídico-material, porque a manipulação da interface afeta diretamente a liberdade da decisão e, por essa via, compromete a validade do consentimento. Também o EDPB tem vindo a advertir para esta realidade nas orientações sobre *dark patterns* e no relatório da *Cookie Banner Taskforce* (European Data Protection Board, 2022, 2023).

Finalmente, importa referir o paradoxo da privacidade, isto é, a contradição entre a preocupação declarada dos titulares relativamente à privacidade e o seu comportamento real de aceitação rápida e pouco refletida do tratamento dos seus dados. Norberg et al. (2007) identificaram este fenómeno de forma clássica, e Pavlou (2011) aprofundou a sua relevância na literatura sobre informação e privacidade. A dissertação mostra que esse paradoxo não significa falta de relevância da privacidade, mas antes evidencia as limitações do contexto em que a escolha é exercida. Políticas longas, linguagem técnica, desconhecimento do alcance dos riscos e confiança funcional no prestador do serviço contribuem para que o consentimento seja, muitas vezes, apenas formalmente válido, mas substancialmente deficiente.

4. Limites das Atuais Plataformas de Gestão de Consentimentos

O ambiente digital não é desprovido de mecanismos de gestão de consentimentos. Pelo contrário, a proliferação de *Consent Management Platforms* demonstra que o mercado reconheceu a necessidade de organizar a recolha e administração destes atos. Todavia, a dissertação evidencia que tais soluções se desenvolveram, em larga medida, sob uma lógica predominantemente empresarial, orientada para a demonstração de conformidade dos responsáveis pelo tratamento, e não prioritariamente para a capacitação do titular dos dados. Esta crítica é compatível com a leitura de Voigt e von dem Bussche (2017), segundo a qual a conformidade regulatória não deve ser confundida com efetiva proteção material dos direitos dos titulares.

É verdade que as CMP trouxeram ganhos relevantes ao nível da documentação do consentimento, da parametrização de preferências e da adaptação às exigências do RGPD. Porém, esses ganhos revelam-se insuficientes quando avaliados à luz de uma perspetiva verdadeiramente centrada no utilizador. A fragmentação permanece: cada plataforma gere consentimentos no seu próprio perímetro, com diferentes formatos, diferentes interfaces, diferentes níveis de detalhe e diferentes possibilidades de revogação. A prova também permanece dispersa, dificultando a reconstrução clara do percurso do consentimento ao longo do tempo. Acresce que, em muitos casos, a lógica de design dessas ferramentas continua a favorecer a aceitação em vez de promover uma decisão equilibrada. Assim, a mera existência de sistemas de gestão de consentimento não elimina a crise do consentimento; em certos casos, apenas a reorganiza sob uma aparência mais sofisticada de conformidade.

Foi precisamente a partir da identificação dessas lacunas que a investigação desenvolveu uma metodologia assente em três eixos complementares: a análise jurídico-dogmática do consentimento e do RGPD; a revisão técnico-científica de soluções e tecnologias relevantes; e a análise qualitativa-comparativa de modelos existentes, incluindo CMPs e sistemas alternativos como *MyData*, *Consentua*, *Solid Pods* e *IBM Data Consent Manager*. Esta aproximação metodológica é coerente com a utilização do estudo de caso e da comparação funcional como instrumentos de investigação jurídica e aplicada, em linha com Yin (2018) e com a literatura sobre ecossistemas de dados centrados no utilizador, como Verborgh et al. (2021) e Langford et al. (2022).

5. Para Além do Consentimento Formal: Proposta de Uma Arquitetura Jurídico-Computacional Orientada ao Titular

A originalidade da dissertação reside em não se limitar à crítica do modelo vigente, avançando antes com uma proposta conceptual de arquitetura computacional destinada a reforçar a autodeterminação informacional do titular dos dados. Essa proposta combina Direito e Computação como forma de repensar a recolha, gestão e validação do consentimento, partindo da premissa de que a efetividade do RGPD depende também da qualidade técnica das infraestruturas que sustentam o exercício dos direitos. Tal entendimento é compatível com a noção de *data protection by designand by default*, desenvolvida na doutrina e nas orientações regulatórias, segundo a qual as garantias jurídicas devem ser integradas na própria arquitetura dos sistemas e não apenas acrescentadas de forma posterior ou superficial (Bygrave, 2017; Cavoukian, 2009; Menezes Cordeiro, 2022). A própria dissertação afirma expressamente essa exigência de incorporação estrutural das garantias jurídicas.

A arquitetura proposta assenta em princípios de *privacy by design*, interoperabilidade e segurança, integrando mecanismos de pseudonimização, *hashing*, rastreabilidade e registo imutável. A sua lógica é eminentemente jurídico-funcional: criar condições para que o titular possa gerir os seus consentimentos de forma simplificada, transparente e segura, enquanto os responsáveis pelo tratamento dispõem de meios adequados para demonstrar a regularidade da recolha, da conservação da prova e do exercício dos direitos de modificação ou revogação. Neste plano, a ISO/IEC 29100 (2011), a ISO/IEC 27701 (2019) e a ISO/IEC 27560 (2023) oferecem enquadramentos particularmente relevantes para estruturar privacidade, gestão e registo do consentimento.

Do ponto de vista arquitetural, a investigação sustenta uma solução híbrida, articulando microserviços e eventos, com justificação ancorada na necessidade de escalabilidade, auditabilidade e adaptação dinâmica às operações associadas ao consentimento. Embora esta dimensão tenha um cariz mais técnico, ela pode ser juridicamente valorizada na medida em que suporta *accountability,* rastreabilidade e resposta eficiente aos direitos dos titulares. A literatura de arquitetura de *software*, como Bass et al. (2021) e Newman (2021), ajuda a compreender como estruturas modulares e orientadas a eventos favorecem controlo, separação de responsabilidades e flexibilidade evolutiva. O ponto essencial, porém, é jurídico: a arquitetura procura transformar a manifestação de vontade do titular em instruções operacionais verificáveis, suscetíveis de serem respeitadas por diferentes intervenientes e sistemas.

A componente de registo e prova pode igualmente beneficiar de mecanismos robustos de integridade e auditabilidade. Neste domínio, referências como Kent (2006), ISO/IEC 27037 (2012) e ISO/IEC 27560 (2023) são úteis para enquadrar requisitos de registo, preservação e estruturação da evidência digital. Já quanto ao eventual recurso a blockchain permissionada e registos imutáveis, importa adotar uma postura prudente. Trabalhos como os de Androulaki et al. (2018), Godyn et al. (2022) e Berberich (2016) mostram que estas tecnologias podem oferecer vantagens em matéria de integridade e rastreabilidade, mas levantam simultaneamente questões delicadas de conformidade com princípios como minimização, apagamento e limitação das finalidades. A dissertação reconhece essas tensões e, por isso, não apresenta a tecnologia como solução mágica, mas como instrumento a enquadrar juridicamente com cautela.

Acresce que uma arquitetura deste tipo deve ser pensada em coerência com os desafios contemporâneos colocados por sistemas automatizados e inteligência artificial. Autores como Mantelero (2018), Zarsky (2016, 2017), Giannopoulou (2021) e Lukács e Váradi (2023) mostram que a utilização de sistemas baseados em dados

exige padrões reforçados de explicabilidade, supervisão e conformidade. Isso é particularmente importante quando a gestão do consentimento deixa de ser apenas um registo passivo e passa a integrar componentes de automatização, verificação ou decisão.

6. Relevância Jurídico-Científica da Proposta

A passagem do consentimento formal ao consentimento verificável tem implicações dogmáticas relevantes. Em primeiro lugar, reforça a ideia de que a validade do consentimento não depende apenas da existência de um ato positivo, mas da qualidade do contexto em que esse ato é produzido, registado e subsequentemente gerido. Em segundo lugar, desloca o foco da mera recolha inicial para a governança integral do consentimento, compreendida como processo que inclui prova, revogabilidade, auditabilidade, portabilidade e interoperabilidade. Em terceiro lugar, contribui para reconduzir a proteção de dados à sua dimensão estrutural: a de uma tutela de direitos fundamentais que não se satisfaz com procedimentos formais, exigindo antes condições reais de exercício da autonomia informacional. Esta leitura é compatível com o pensamento de Bygrave (2014), Lynskey (2015), Menezes Cordeiro (2022) e Solove (2010), bem como com o enquadramento regulatório desenvolvido pelo EDPB.

Nesta perspetiva, a proposta de arquitetura jurídico-computacional tem valor não apenas instrumental, mas também hermenêutico. Ela permite ler o RGPD não como um conjunto de deveres abstratos desligados da realidade tecnológica, mas como um regime cuja aplicação prática depende de mecanismos de execução coerentes com os seus princípios. Assim, *privacy by design* deixa de ser mera cláusula programática e passa a exigir efetiva tradução técnica,*accountability* deixa de significar apenas dever de documentação e passa a implicar condições de reconstrução verificável do percurso do consentimento; transparência deixa de se esgotar em textos informativos extensos e passa a exigir inteligibilidade funcional. Tudo isto reforça a ideia de que a integração entre categorias jurídicas e estruturas computacionais é hoje condição da efetividade do direito da proteção de dados.

7. Conclusão

O consentimento continua a ocupar posição nuclear no regime da proteção de dados pessoais, mas a sua centralidade normativa não garante, por si só, a sua efetividade material. A análise desenvolvida demonstra que o ambiente digital contemporâneo favorece formas de consentimento apressadas, manipuladas, fragmentadas e insuficientemente compreendidas, comprometendo a liberdade e a informação que o RGPD exige. A fadiga do consentimento, o formalismo da recolha, os *dark patterns* e o paradoxo da privacidade revelam que o modelo vigente, embora juridicamente exigente, enfrenta sérias dificuldades de concretização prática, como assinalam Schermer et al. (2014), Nouwens et al. (2020), European Data Protection Board (2022, 2023) e Menezes Cordeiro (2022).

Todavia, a relevância do estudo não reside apenas nesse diagnóstico. O seu contributo decisivo está em demonstrar que a crise do consentimento não impõe necessariamente o abandono desta figura, mas antes a sua reconceptualização à luz das exigências do ambiente digital. Nesse sentido, a proposta de uma arquitetura jurídico-computacional de gestão de consentimentos apresenta-se como via promissora para reforçar a posição do titular, assegurar maior granularidade e revogabilidade, melhorar a prova da validade do consentimento e tornar mais efetivos os princípios de transparência, segurança, interoperabilidade e responsabilidade. Não se trata de substituir o Direito pela tecnologia, mas de reconhecer que, sem desenho técnico juridicamente orientado, o Direito corre o risco de permanecer apenas formalmente proclamado.

Em síntese, a passagem do consentimento formal ao consentimento verificável constitui não apenas uma possibilidade técnica, mas uma exigência jurídica coerente com a lógica do RGPD. A proteção de dados pessoais, numa era de ecossistemas digitais complexos, já não pode depender exclusivamente da repetição de cliques em interfaces opacas. Exige, antes, estruturas que devolvam ao titular controlo inteligível, escolha efetiva e capacidade de prova. É nesse ponto que a abordagem combinada entre Direito e Computação revela o seu maior mérito: o de contribuir para uma proteção de dados menos ritual e mais substantiva.

Referências

Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., Enyeart, D., Ferris, C., Laventman, G., Manevich, Y., Muralidharan, S., Murthy, C., Nguyen, B., Sethi, M., Singh, G., Smith, K., Sorniotti, A., Stathakopoulou, C., Vukolić, M., Cocco, S. W., & Yellick, J. (2018). Hyperledger Fabric: A distributed operating system for permissioned blockchains. *Proceedings of the Thirteenth EuroSys Conference*.

Bass, L., Clements, P., & Kazman, R. (2021). *Software architecture in practice* (4.ª ed.). Addison-Wesley.

Berberich, M. S. (2016). Practitioner's corner: Blockchain technology and the GDPR. *European Data Protection Law Review, 2*, 422–426.

Berens, B. M., et al. (2024). Cookie disclaimers: Dark patterns and lack of transparency. *Computers & Security, 136*, 103507.

Budin-Ljøsne, I., Teare, H. J. A., Kaye, J., Beck, S., Bentzen, H. B., Caenazzo, L., Collett, C., D'Abramo, F., Felzmann, H., Finlay, T., Javaid, M. K., Jones, E., Katić, V., Simpson, A., Mascalzoni, D., & Hansson, M. G. (2017). Dynamic consent: A potential solution to some of the challenges of modern biomedical research. *BMC Medical Ethics, 18*(1).

Bygrave, L. A. (2014). *Data privacy law: An international perspective*. Oxford University Press.

Bygrave, L. A. (2017). Data protection by design and by default. *Oslo Law Review, 4*.

Cavoukian, A. (2009). *Privacy by design: The 7 foundational principles*.

European Data Protection Board. (2022). *Guidelines 3/2022 on dark patterns in social media platform interfaces: How to recognise and avoid them*.

European Data Protection Board. (2023). *Report of the work undertaken by the Cookie Banner Taskforce*.

Giannopoulou, A. (2021). Data protection by design in the era of artificial intelligence. *International Data Privacy Law*.

Godyn, J., Maček, N., & Pustisek, M. (2022). Blockchain and GDPR compliance: Opportunities and challenges for data protection. *Computer Law & Security Review*.

International Organization for Standardization. (2011). *ISO/IEC 29100:2011 — Information technology — Security techniques — Privacy framework*.

International Organization for Standardization. (2012). *ISO/IEC 27037:2012 — Guidelines for identification, collection, acquisition and preservation of digital evidence*.

International Organization for Standardization. (2019). *ISO/IEC 27701:2019 — Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management*.

International Organization for Standardization. (2023). *ISO/IEC 27560:2023 — Privacy technologies — Consent record information structure*.

John, L. K. (2018). Uninformed consent. *Harvard Business Review*.

Kent, K. (2006). *Guide to computer security log management (NIST Special Publication 800-92)*. National Institute of Standards and Technology.

Kyi, L., et al. (2023). Investigating deceptive design in GDPR's legitimate interest. *CHI 2023*.

Langford, J., et al. (2022). Understanding MyData operators.

Lukács, A., & Váradi, S. (2023). GDPR-compliant AI-based automated decision-making. *Computer Law & Security Review, 50*.

Lynskey, O. (2015). *The foundations of EU data protection law*. Oxford University Press.

Machuletz, D., & Böhme, R. (2020). Multiple purposes, multiple problems: A user study of consent dialogs after GDPR. *PoPETs, 2020*, 481–498.

Mantelero, A. (2018). AI and Big Data: A blueprint for a human rights, social and ethical impact assessment. *Computer Law & Security Review, 34*(4), 754–772.

Mathur, A., Acar, G., Friedman, M. J., Lucherini, E., Mayer, J., Chetty, M., & Narayanan, A. (2019a). Dark patterns at scale: Findings from a crawl of 11K shopping websites. *Proceedings of the ACM on Human-Computer Interaction, 3*(CSCW), 1–32.

Mathur, A., Kshirsagar, M., Mayer, J., & Narayanan, A. (2019b). What makes a dark pattern dark? *Proceedings of the ACM on Human-Computer Interaction*.

Menezes Cordeiro, A. B. (2018). O consentimento do titular dos dados no RGPD. In *FinTech II*. Almedina.

Menezes Cordeiro, A. B. (2022). *Direito da proteção de dados*. Almedina.

Newman, S. (2021). *Building microservices* (2nd ed.). O'Reilly.

Nissenbaum, H. (2010). *Privacy in context*. University of Chicago Press.

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs, 41*(1), 100–126.

Nouwens, M., Liccardi, I., Veale, M., Karger, D., & Kagal, L. (2020). Dark patterns after the GDPR: Scraping consent pop-ups and demonstrating their influence. *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*.

Pavlou, P. A. (2011). State of the information privacy literature: Where are we now and where should we go? *MIS Quarterly, 35*(4), 977–988.

Pinheiro, A. S. (2015). *Privacy e proteção de dados pessoais*. Almedina.

Schermer, B. W., Custers, B., & van der Hof, S. (2014). The crisis of consent: How stronger legal protection may lead to weaker consent in data protection. *Ethics and Information Technology, 16*(2), 171–182.

Solove, D. J. (2010). *Understanding privacy*. Harvard University Press.

Utz, C., Degeling, M., Fahl, S., Schaub, F., & Holz, T. (2019). (Un)informed consent: Studying GDPR consent notices in the field. *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, 973–990.

Verborgh, R., Arndt, D., Vander Sande, M., Hartig, O., De Meester, B., Haesendonck, G., & Colpaert, P. (2021). Solid: Re-decentralizing the Web by giving users control over their data. *Proceedings of the Web Conference*.

Voigt, P., & von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A practical guide*. Springer.

Yin, R. K. (2018). *Case study research and applications: Design and methods* (6th ed.). Sage.

Zarsky, T. (2016). The trouble with algorithmic decisions. *Science, Technology, & Human Values, 41*(1), 118–132.

Zarsky, T. (2017). Big data: The end of privacy or a new beginning? *International Data Privacy Law, 3*(2), 74–87.

Declaração Ética

Conflito de Interesse: Nada a declarar. **Financiamento:** Nada a declarar. **Revisão por Pares:** Dupla-cega.

O encarregado de proteção de dados

Data protection officer

10.29073/j2.v8i1.1120

Recebido: 08 de março de 2026.
Aprovado: 31 de março de 2026.
Publicado: 04 de abril de 2026.

Autor/a: Sílvia Cardoso, ESTG-IPP, Portugal, silviacardosolg@gmail.com.

Resumo

O presente artigo analisa a figura jurídica do Encarregado de Proteção de Dados (EPD), prevista no Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, designado por Regulamento Geral sobre a Proteção de Dados (RGPD), e concretizada no ordenamento jurídico português pela Lei n.º 58/2019, de 8 de agosto (LE).

O estudo incide sobre o enquadramento jurídico do EPD, abordando o seu conceito, características, formação e posição na organização. Analisa-se igualmente o regime de designação desta figura, com particular enfoque nas entidades públicas, bem como as funções e obrigações que lhe são atribuídas pela legislação europeia e nacional. Por fim, procede-se à análise das consequências jurídicas associadas ao incumprimento das normas de proteção de dados e à eventual responsabilidade decorrente da atuação do EPD.

O trabalho baseia-se numa metodologia jurídico-dogmática, assente na análise da legislação aplicável, bem como da doutrina e orientações relevantes em matéria de proteção de dados.

Palavras-Chave: Administração Pública; Compliance; Encarregado de Proteção de Dados; Proteção de Dados; RGPD.

Abstract

This article analyzes the legal figure of the Data Protection Officer (DPO), established by Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, commonly known as the General Data Protection Regulation (GDPR), and implemented in the Portuguese legal system through Law No. 58/2019 of 8 August (EL).

The study examines the legal framework of the DPO, addressing its concept, characteristics, professional qualifications and position within organizations. It further analyzes the designation regime of the DPO, with particular emphasis on public entities, as well as the functions and obligations assigned to this role under European and national legislation. Finally, the article discusses the legal consequences associated with non-compliance with data protection rules and the potential liability arising from the actions of the DPO.

The research follows a legal-dogmatic methodology based on the analysis of applicable legislation, doctrinal contributions and relevant guidelines in the field of data protection.

Keywords: Compliance; Data Protection; Data Protection Officer; GDPR; Public Administration.

1. Introdução

A crescente digitalização da sociedade e o desenvolvimento das tecnologias de informação conduziram a um aumento significativo da recolha e tratamento de dados pessoais por organizações públicas e privadas. Neste contexto, a proteção de dados pessoais assumiu particular relevância no ordenamento jurídico europeu, culminando na aprovação do Regulamento (UE) 2016/679, conhecido como Regulamento Geral sobre a Proteção de Dados (RGPD).

O RGPD estabeleceu um quadro jurídico harmonizado em matéria de proteção de dados na União Europeia, introduzindo novos mecanismos destinados a reforçar a proteção dos direitos fundamentais dos titulares dos dados e a garantir maior responsabilização das organizações no tratamento de dados pessoais

Entre esses mecanismos destaca-se a figura do Encarregado de Proteção de Dados (EPD), cuja função consiste em assegurar o acompanhamento do cumprimento das normas relativas ao tratamento de dados pessoais, bem como promover a cultura de proteção de dados no seio das organizações (Cordeiro, 2021; Grupo de Trabalho do Artigo 29º, 2017).

Embora o RGPD preveja expressamente a existência e as funções do EPD, a sua concretização nos ordenamentos jurídicos nacionais exige a articulação com legislação interna. Em Portugal, essa concretização ocorreu através da Lei n.º 58/2019, de 8 de agosto (LE), que assegura a execução do RGPD e estabelece normas complementares relativas à sua aplicação no ordenamento jurídico nacional.

O presente artigo tem como objetivo analisar o regime jurídico aplicável ao Encarregado de Proteção de Dados no contexto do ordenamento jurídico português, incidindo sobre o seu enquadramento legal, as suas funções e obrigações, bem como sobre os desafios associados à sua posição nas organizações.

A investigação baseia-se numa metodologia jurídico-dogmática, assente na análise da legislação europeia e nacional aplicável, complementada pela análise de orientações doutrinárias e institucionais relevantes.

2. Enquadramento Legal

2.1. Regulamento Geral sobre a Proteção de Dados (RGPD)

O RGPD foi aprovado em 27 de abril de 2016 pelo Parlamento Europeu e pelo Conselho, tendo como objetivo reforçar a proteção das pessoas singulares no que respeita ao tratamento de dados pessoais e assegurar a livre circulação desses dados no espaço da União Europeia.

Este regulamento entrou em vigor no vigésimo dia após a sua publicação no Jornal Oficial da União Europeia, tornando-se aplicável a partir de 25 de maio de 2018, revogando a Diretiva 95/46/CE, que até então constituía o principal instrumento jurídico europeu nesta matéria.

Apesar do RGPD ser diretamente aplicável em todo o território da União Europeia (UE) desde 25 de maio de 2018, a verdade é que o mesmo permite aos Estados Membros (EM), a manutenção ou aprovação de disposições específicas no que concerne à aplicação de determinadas regras respeitantes ao tratamento de dados.

De acordo com o art.º 1º do RGPD, o objeto do RGPD consiste em regular a "*proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados*.", alcançando assim dois grandes objetivos, defender os direitos e as liberdades fundamentais das pessoas singulares, nomeadamente o seu direito à proteção de dados e, ainda, promover a livre circulação dos dados pessoais.

Entre os mecanismos previstos pelo regulamento, destaca-se no seu âmbito, a figura jurídica do Encarregado de Proteção de Dados (EPD), consagrada nos artigos 37º a 39º do RGPD, figura esta existente já em vários países antes da entrada em vigor do RGPD.

2.2. Lei de Execução do RGPD em Portugal – Lei n.º 58/2019, de 08 de Agosto (LE)

Assim, para a aplicação do Regulamento Geral de Proteção de Dados em Portugal, foi publicado no Diário da República, 2.ª série – N.º 163, o Despacho n.º 7456/2017, de 24 de agosto, que criou um Grupo de Trabalho com o objetivo de preparar a legislação portuguesa para a aplicação daquele regulamento, tendo este Grupo apresentado uma proposta de lei ao Governo, aprovada em Conselho de Ministros e remetida à Assembleia da República.

Ora, desta proposta surgiu a Lei n.º 58/2019, de 08 de agosto (Lei de execução interna do RGPD (LE)), que veio assegurar a execução do RGPD, no ordenamento jurídico português, após um longo processo legislativo.

Além de assegurar a execução do RGPD na ordem jurídica portuguesa, esta lei visou ainda harmonizar a legislação nacional e aprofundar a regulação da proteção de dados em diferentes matérias e mais detalhadamente.

Deste modo, a LE estatuiu no seu Capítulo III, designadamente os artigos 9º a 13º, as normas aplicáveis ao Encarregado de Proteção de Dados (EPD).

Destaca-se que, relativamente a esta LE, a Comissão Nacional de Proteção de Dados (CNPD) decidiu, menos de um mês após a sua entrada em vigor, desaplicar algumas normas do referido diploma legal em situações de tratamento de dados pessoais a serem avaliadas futuramente, através da Deliberação n.º 2019/494 (CNPD, 2019). Nesse documento, a CNPD, num texto extenso, formula críticas severas ao processo legislativo português que conduziu à aprovação desta LE, justificando a desaplicação de determinadas normas pelo facto de estas contrariarem o previsto no RGPD, comprometendo assim a sua aplicação uniforme e, consequentemente, a sua plena eficácia e consistência em todo o território dos Estados-Membros.

3. O Encarregado de Proteção de Dados

Apesar da relevância desta figura no sistema de proteção de dados, o artigo 4º do RGPD não contém uma definição expressa de Encarregado de Proteção de Dados. Ainda assim, o regulamento estabelece o regime jurídico aplicável a esta figura nos artigos 37º a 39º, permitindo identificar as suas características essenciais.

Assim, por interpretação extensiva do RGPD, o EPD pode ser entendido como a pessoa singular ou coletiva designada por uma organização para acompanhar e monitorizar o cumprimento das normas relativas à proteção de dados pessoais (Portal DPO). A sua atuação envolve a participação em todas as questões relacionadas com o tratamento de dados pessoais, desempenhando um papel central na implementação das políticas de proteção de dados no seio da organização (Cordeiro, 2021).

No exercício das suas funções, o EPD encontra-se sujeito a um dever de sigilo e confidencialidade relativamente às informações a que tenha acesso no âmbito da sua atividade. Este dever abrange todas as informações a que tenha tido acesso durante esse exercício, tanto as informações relativas ao responsável pelo tratamento como aquelas respeitantes aos titulares dos dados, mantendo-se mesmo após o termo das funções que lhe deram origem, nos termos do artigo 10º da LE.

Deste modo, o Encarregado de Proteção de Dados assume um papel fundamental no sistema de gestão da proteção de dados, atuando como elemento de ligação entre a organização, os titulares dos dados e a autoridade de controlo.

3.1. Características, Formação e Posição

Independentemente da natureza da relação jurídica que mantém com a organização, o encarregado de proteção de dados deve exercer as suas funções com autonomia técnica perante a entidade responsável pelo tratamento ou subcontratante, nos termos do n.º 2, do artigo 9.º da LE.

Relativamente à autonomia técnica do EPD, destaca-se o Considerando 97 do RGPD,

Que estabelece que "*O nível necessário de conhecimentos especializados deverá ser*

determinado, em particular, em função do tratamento de dados realizado e da proteção exigida para os dados pessoais tratados pelo responsável pelo seu tratamento ou pelo subcontratante" e ainda que os "*encarregados de proteção de dados, sejam ou não empregados do responsável pelo tratamento, deverão estar em condições de desempenhar as suas funções e atribuições com independência*".

Este dispositivo evidencia que a função do EPD nem sempre é fácil ou conciliável quando desempenhada por um trabalhador da organização subordinado juridicamente por um contrato individual de trabalho, acumulando simultaneamente duas funções muito distintas: a de funcionário subordinado, sujeito ao poder diretivo e disciplinar da organização, e a de EPD, responsável por fiscalizar a atuação da própria organização, sem receber

ordens de superiores hierárquicos e sem poder ser penalizado ou destituído das suas funções (n.º 3 do artigo 38º do RGPD).

Assim, a organização deve realizar uma análise baseada no risco para avaliar se a designação de um EPD interno é adequada. Caso identifique conflitos de interesse ou risco elevado, poderá optar pela designação de um EPD externo, que exerça as funções em regime de exclusividade, mediante contratação de prestação de serviços através de procedimento de contratação pública, minimizando os riscos para a organização.

Ademais, este EPD tem um dever de lealdade para com a organização, bem como um dever de cooperação com a Comissão Nacional da Proteção de Dados (CNPD), designadamente informando esta entidade fiscalizadora de eventuais incumprimentos da lei pela organização, o que poderá causar um conflito de deveres do EPD. Neste sentido, conforme se referiu anteriormente, a melhor solução será a contratação de consultor externo para o exercício das funções de EPD.

A independência funcional do EPD constitui um requisito fundamental para garantir a eficácia da sua atuação. Sempre que acumula funções de EPD com outras responsabilidades na organização, deve ser garantida uma segregação adequada de funções, de modo a prevenir conflitos de interesse. Segundo o Grupo de Trabalho do Artigo 29º para a proteção de dados (GT 29), o EPD não deve ocupar uma posição na organização em que tenha autoridade para decidir sobre as finalidades e os meios de tratamento de dados. O GT 29 apresenta ainda diversas boas práticas destinadas à prevenção de conflitos de interesse no exercício desta função.

No que respeita à formação do EPD, embora não seja exigida qualquer certificação profissional, o n.º 5 do artigo 37º do RGPD estabelece que "*O encarregado da proteção de dados é designado com base nas suas qualidades profissionais e, em especial, nos seus conhecimentos especializados no domínio do direito e das práticas de proteção de dados, bem como na sua capacidade para desempenhar as funções referidas no artigo 39.º.*".

Assim, dada a importância atribuída a tal cargo, especialmente na Administração Pública, o critério de nomeação do EPD deve ser rigoroso. O EPD deve possuir conhecimentos sólidos, adequados e específicos em matéria de proteção de dados e procedimentos administrativos do organismo, formação jurídica na área do direito e, ainda, competências na área dos sistemas de informação, de modo a garantir o desempenho eficaz das funções previstas no artigo 39º. A ausência dessas competências essenciais pode comprometer a conformidade legal da organização, expondo-a ao risco de infrações e à aplicação de coimas.

Neste contexto, a designação do EPD deve considerar a sua experiência e formação específica, bem como a natureza das atividades desenvolvidas na organização. O nível de competências exigido e o grau de apoio disponibilizado devem ser proporcionais à complexidade das operações de tratamento de dados e à quantidade de dados sensíveis processados pela organização.

Nos termos do artigo 38º do RGPD, o EPD deve ser envolvido, de forma adequada e em tempo útil, a todas as questões relacionadas com a proteção de dados pessoais, que sejam tratadas pelo responsável pelo tratamento e o subcontratante, devendo estes apoiar o EPD no exercício das suas funções, fornecendo-lhe os recursos necessários ao seu desempenho e à manutenção dos seus conhecimentos, bem como dando-lhe acesso aos dados pessoais e às operações de tratamento.

O EPD deve ser isento e imparcial no exercício das suas funções e deve informar diretamente a direção ao mais alto nível do responsável pelo tratamento ou do subcontratante.

Os titulares dos dados podem contactar o encarregado da proteção de dados sobre

todas questões relacionadas com o tratamento dos seus dados pessoais e com o exercício dos seus direitos.

Ora, a imposição obrigatória deste EPD tem como propósito uma função especializada no controlo relativamente ao *compliance* de proteção de dados. O termo *compliance* refere-se ao "*conjunto de ações ou procedimentos que visam verificar o cumprimento de leis, regulamentos, normas ou padrões estabelecidos, geralmente numa*

empresa ou instituição; verificação da conformidade (Dicionário Priberam da Língua Portuguesa online (s.d.), Contudo, a responsabilidade principal por esse controlo recai sobre a própria organização, cabendo ao EPD atuar como uma segunda linha de defesa, complementar à supervisão da autoridade de controlo e, simultaneamente, como provedor dos titulares dos dados (Cordeiro, 2021).

O EPD encontra-se subjugado ao dever de sigilo ou de confidencialidade no exercício

das suas funções, podendo exercer outras funções e atribuições, desde que estas não resultem num conflito de interesses.

A título informativo, foi criado pelo consultor Tiago Nascimento um projeto de implementação do RGPD denominado "*Portal do DPO*", um portal que permite o acesso a conceitos e informações essenciais para assegurar a conformidade das organizações com o regulamento. Este recurso foi criado em resposta às frequentes dúvidas e incertezas sobre a interpretação do RGPD, configurando-se como uma ferramenta de trabalho que reúne direitos, deveres e boas práticas relacionados com o regulamento, podendo ser esclarecidas ainda dúvidas através do grupo de rede social *LinkedIn* (Pedreira, 2019).

3.2. Designação

Conforme já referido anteriormente, apesar desta figura ser uma novidade do RGPD, o seu conceito já existia antes, sendo que apenas agora se torna legalmente obrigatória a sua designação, verificadas determinadas condições constantes do n.º 1 do artigo 37º do RGPD.

O RGPD determina a obrigatoriedade de designar um EPD apenas nos seguintes casos expressamente previstos no artigo 37º do RGPD:

a) Quando o tratamento é efetuado por uma autoridade ou um organismo público, com exceção dos tribunais, desde que, no exercício da sua função jurisdicional, podendo ser designado um único encarregado da proteção de dados para várias dessas autoridades ou organismos, tendo em conta a respetiva estrutura organizacional e dimensão.

Esta exceção deve-se ao princípio constitucional da independência dos tribunais e consequente falta de competência das autoridades de controlo relativamente àqueles, conforme n.º 3 do art.º 55º do RGPD. Em referência à LE, esta substitui no seu n.º 1 do art.º 12º, o vocabulário usado pelo RGPD, aplicando o conceito de entidade pública e descrevendo no seu n.º 2 o que se deve compreender por entidade pública.

b) Nas empresas privadas quando as atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento que, devido à sua natureza, âmbito e/ou finalidade, exijam um controlo regular e sistemático dos titulares dos dados em grande escala.

Estas presunções (atividades principais; controlo regular e sistemático e em grande

escala) apresentam algumas dificuldades uma vez que se baseiam em conceitos imprecisos e pouco concretizáveis (Cordeiro, 2021).

Esta norma determina os casos em que existe obrigatoriedade de designação de EPD

no setor privado, relevando-se aqui novamente o Considerando 97 quanto a esta matéria, pois resulta da sua leitura que as atividades principais dizem respeito às atividades primárias, sendo que quanto a estas atividades as orientações do GT 29 refere que as atividades principais podem entender-se como as operações essenciais necessárias para alcançar os objetivos do responsável pelo tratamento ou do subcontratante, no entanto, esta interpretação não deve excluir as atividades em que o tratamento de dados constitui uma parte indissociável das atividades do responsável pelo tratamento ou do subcontratante.

Quanto ao controlo, de acordo com o GT 29, este compreende a observação do comportamento do titular dos dados, comportamento este definido no Considerando 24 do RGPD, significando que o controlo regular é

permanente ou repetido periodicamente e o controlo sistemático ocorre de forma metódica, como parte de uma estratégia, de forma planeada e organizada, e como parte de um plano universal de recolha de dados pessoais. Relativamente à presunção de grande escala faz-se referência ao Considerando 91, em que se entende que as operações de tratamento de dados que digam respeito a uma grande quantidade de dados podem afetar um número considerável de titulares, resultando num risco elevado, pelo que o GT 29 recomenda que devam ser considerados certos fatores para determinar se o tratamento é efetuado em grande escala, tais como, o número de titulares de dados, a quantidade e a diversidade de tipos de dados, a duração ou permanência das atividades de tratamento de dados e a extensão geográfica da atividade de tratamento.

c) Quando as atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento em grande escala de categorias especiais de dados (art.º 9º) ou de dados pessoais relacionados com condenações penais e infrações (art.º 10º). Esta designação está relacionada com a natureza sensível destes dados, obtendo assim uma proteção acrescida.

Refere ainda este artigo que um grupo empresarial (grupo composto pela empresa que exerce o controlo e pelas empresas controladas (Considerando 37 e definição 19 do artigo 4º do RGPD), poderá também designar um único encarregado de proteção de dados desde que haja um encarregado de proteção de dados que seja facilmente acessível a partir de cada estabelecimento.

E ainda, quando o responsável pelo tratamento ou o subcontratante for uma autoridade ou organismo público, pode ser designado um único EPD para várias dessas autoridades ou organismos, tendo em conta a respetiva estrutura organizacional e dimensão.

É de salientar a designação voluntária do n.º 4 em que, no caso do responsável pelo tratamento de uma empresa opte, ainda que não seja obrigatório, por designar um EPD, fica desde logo obrigado ao cumprimento de todas as obrigações subjacentes como se se tratasse de uma designação obrigatória (Universidade de Coimbra, s.d.).

Quando é designado um EPD pelas organizações, é obrigatória a publicação dos seus contactos, bem como existe o dever de informação pelo responsável de tratamento e o dever de comunicação sobre o EPD à autoridade de controlo (CNPD).

No que concerne à LE, esta apenas vem complementar o disposto no RGPD, no que respeita a critérios de designação do EPD e à autonomia técnica do mesmo, temas estes já abordados no ponto 1.3.

3.2.1. Designação em Autoridades ou Organismos Públicos

As entidades públicas estão sempre obrigadas a ter um EPD, encontrando-se essa regulação mais concretamente no artigoº 12º da LE, dispondo o n.º 2 sobre quais as entidades que são consideradas públicas.

O n.º 3 impõe a existência de pelo menos um EPD e qual o respetivo responsável de tratamento em cada uma das entidades, a saber:

a) Por cada ministério ou área governativa, no caso do Estado, sendo designado pelo respetivo ministro, com faculdade de delegação em qualquer secretário de Estado que o coadjuvar;

b) Por cada secretaria regional, no caso das regiões autónomas, sendo designado pelo respetivo secretário regional, com faculdade de delegação em dirigente superior de 1.º grau;

c) Por cada município, sendo designado pela câmara municipal, com faculdade de delegação no presidente e subdelegação em qualquer vereador;

d) Nas freguesias em que tal se justifique, nomeadamente naquelas com mais de 750 habitantes, sendo designado pela junta de freguesia, com faculdade de delegação no presidente.

No que respeita à exigência quantitativa (750 habitantes) referida nesta alínea, a mesma não pode ser aplicada, uma vez que a legislação nacional não se pode sobrepor à obrigação imposta pelo RGPD na sua alínea a) do n.º

1 do art.º 37º, i.é., a mera designação de um EPD sempre que o tratamento for efetuado por uma autoridade ou um organismo público;

e) Por cada entidade, no caso das demais entidades referidas no número anterior, sendo designada pelo respetivo órgão executivo, de administração ou gestão, com faculdade de delegação no respetivo presidente.

Conforme se disse anteriormente, tendo em conta a respetiva estrutura organizacional e dimensão das autoridades ou organismos públicos, pode ainda ser designado um único EPD de acordo com o preceituado no n.º 4 deste artigo 12º, conjugado com o n.º 3 do artigo 37º do RGPD.

A designação do EPD cabe a cada entidade, não sendo obrigatório o exercício de funções em regime de exclusividade.

No entanto, O EPD de uma entidade pública que tenha atribuições de regulação ou controlo não pode exercer essas funções simultaneamente em entidade sujeita ao controlo, ou inserida no perímetro regulatório daquela entidade.

3.3. Funções e Obrigações

A função de EPD deve ser atribuída sempre que exista processamento de dados pessoais e sensíveis em larga escala, envolvendo o aconselhamento, a monitorização e conformidade de toda a segurança e proteção de dados.

O artigo 39º do RGPD estabelece para o EPD as seguintes funções/obrigações:

a) Informar e aconselhar o responsável pelo tratamento ou o subcontratante, sobre todas as questões relacionadas com a proteção de dados, bem como os trabalhadores que tratem os dados, a respeito das suas obrigações nos termos do regulamento e da LE;

b) Controlar a conformidade com o regulamento, com a LE e com as políticas do responsável pelo tratamento ou do subcontratante relativas à proteção de dados pessoais, incluindo a repartição de responsabilidades, a sensibilização e formação do pessoal implicado nas operações de tratamento de dados, e as auditorias correspondentes;

No que respeita à realização de auditorias, não se afigura que estas devam ser executadas diretamente pelo EPD. Nos termos da alínea a) do artigo 11º da LE, incumbe ao EPD garantir a existência de mecanismos de controlo do cumprimento das normas de proteção de dados, designadamente através da implementação de programas de auditorias independentes. Tal função não implica, contudo, que o próprio EPD seja responsável pela sua realização.

Com efeito, uma parte significativa do objeto dessas auditorias incide precisamente sobre o sistema de controlo da conformidade cuja monitorização compete ao próprio EPD. Se a realização das auditorias fosse assegurada diretamente pelo EPD, tal poderia configurar uma situação de autoverificação capaz de afetar a independência e a eficácia da função de monitorização que lhe está atribuída, criando um potencial conflito de interesses (Cordeiro, 2021).

De um modo geral, a auditoria interna em matéria de proteção de dados visa avaliar a conformidade das práticas organizacionais com os requisitos legais aplicáveis, bem como verificar a eficácia das ações implementadas na sequência de auditorias anteriores. Paralelamente, permite identificar aspetos organizacionais suscetíveis de melhoria, através da análise de evidências e da verificação da adequação e eficácia dos controlos existentes para a mitigação dos riscos associados ao tratamento de dados pessoais.

Nesse contexto, as auditorias possibilitam a identificação de situações de não conformidade e de oportunidades de melhoria que deverão ser posteriormente tratadas pela organização, contribuindo para o reforço contínuo do sistema de gestão da proteção de dados.

Assim, não se afigura adequado que a sua realização seja assegurada pelo próprio EPD, uma vez que tal poderia comprometer o efeito útil da atividade de monitorização que lhe está atribuída, ao colocar na mesma entidade a responsabilidade simultânea pela avaliação e pela supervisão do sistema de controlo do cumprimento.

c) Prestar aconselhamento, quando tal lhe for solicitado, no que respeita à avaliação de impacto sobre a proteção de dados, controlando a sua realização nos termos do artigo 35º;

d) Cooperar com a autoridade de controlo (CNPD);

e) Contactar a CNPD sobre questões relacionadas com o tratamento, incluindo a consulta prévia referida no art.º 36.º, bem como consultar a CNPD sobre qualquer outro assunto.

Em relação à LE as funções do EPD encontram-se estatuídas no artigo 11º, acrescentando este dispositivo legal três funções além das já elencadas no RGPD, designadamente:

a) Assegurar a realização de auditorias, quer periódicas, quer não programadas (ponto já desenvolvido anteriormente);

b) Sensibilizar os utilizadores para a importância da deteção atempada de incidentes de segurança e para a necessidade de informar imediatamente o responsável pela segurança;

Esta função é uma duplicação das funções já existentes nas alíneas a) e b) do artigo 39º do RGPD que preveem a informação, aconselhamento, sensibilização e formação dos trabalhadores;

c) Assegurar as relações com os titulares dos dados nas matérias abrangidas pelo RGPD e pela LE.

Também esta função em nada vem acrescentar às funções já estabelecidas no RGPD, pois que o n.º 4 do artigo 38º daquele regulamento incumbe ao EPD a função de ponto de contacto com os titulares dos dados sobre todas as questões relacionadas com o tratamento dos seus dados pessoais.

3.4. Incumprimento e Violação

O regime sancionatório aplicável às violações das normas de proteção de dados encontra-se previsto no Capítulo VIII do RGPD (artigos 77º a 84º), que regula as vias de recurso, a responsabilidade e as sanções.

No ordenamento jurídico português, a LE estabelece igualmente um regime contraordenacional aplicável às infrações em matéria de proteção de dados na Secção II do Capítulo VII (artigos 37º a 45º).

Importa salientar que as sanções previstas na legislação incidem essencialmente sobre o responsável pelo tratamento ou o subcontratante, não recaindo diretamente sobre o EPD.

Não obstante, em determinadas circunstâncias poderá existir responsabilidade, caso se verifique que a violação resultou de uma atuação negligente do EPD. Nessa hipótese, poderá assistir ao responsável pelo tratamento ou ao subcontratante o direito de regresso contra aquele, nos termos dos números 2 e 5 do artigo 82º do RGPD, bem como em conformidade com a parte final do Considerando 146 do mesmo diploma, segundo o qual: "…*Qualquer responsável pelo tratamento ou subcontratante que tenha pago uma indemnização integral, pode posteriormente intentar uma ação de regresso contra outros responsáveis pelo tratamento ou subcontratantes envolvidos no mesmo tratamento*.".

Ademais, nos termos do artigo 51º da LE, o EPD pode ser ainda responsável criminalmente no caso de violação do dever de sigilo profissional a que está obrigado nos termos da lei se, sem justa causa e sem o devido consentimento, revelar ou divulgar no todo ou em parte dados pessoais, sendo punido com pena de prisão até 2 anos ou com pena de multa até 240 dias, uma vez que estas penas são agravadas quando praticadas por EPD. Por outro lado, a negligência também é punível, embora de modo mais ligeiro, com pena de prisão até 6 meses ou com pena de multa até 60 dias.

4. Conclusão

Face ao exposto, conclui-se que, no atual quadro normativo de proteção de dados pessoais, o Encarregado de Proteção de Dados (EPD) assume um papel estruturante na concretização das obrigações decorrentes do Regulamento Geral sobre a Proteção de Dados (RGPD) e da legislação nacional aplicável. Esta figura jurídica configura-se como um elemento central no sistema de gestão da proteção de dados, na medida em que assegura a monitorização do cumprimento das normas legais e promove a implementação, no seio das organizações públicas e privadas, de mecanismos e procedimentos destinados a garantir a licitude, integridade, confidencialidade e segurança no tratamento de dados pessoais. Neste contexto, a designação de um EPD implica um elevado grau de responsabilidade e complexidade funcional, o que se reflete na exigência de qualificações técnicas especializadas, bem como de competências profissionais adequadas ao exercício destas funções.

No âmbito da presente análise foram igualmente consideradas potenciais situações de conflito de interesses à designação de um EPD enquanto trabalhador da própria organização. Tal problemática revela particular relevância quando o titular desta função se encontra simultaneamente sujeito ao poder diretivo e disciplinar da entidade e incumbido de fiscalizar a conformidade das suas práticas com o regime jurídico aplicável, devendo, nos termos do RGPD, exercer as suas funções com autonomia e independência, sem receber instruções quanto ao desempenho das mesmas e sem sofrer qualquer tipo de penalização ou destituição em razão da sua atuação. Neste sentido, entende-se que as organizações deverão proceder a uma avaliação prévia baseada no risco, com vista a determinar a adequação da designação de um EPD interno. Caso se conclua pela existência de constrangimentos suscetíveis de comprometer a independência funcional exigida, a designação de um EPD externo poderá constituir uma solução adequada, permitindo assegurar o pleno exercício das suas atribuições, nomeadamente no que respeita à cooperação com a CNPD.

Foram também ponderadas eventuais tensões decorrentes da atribuição ao EPD da responsabilidade de assegurar a realização de auditorias ao sistema de proteção de dados. Considerando que compete ao EPD monitorizar o cumprimento das normas aplicáveis, a sua intervenção direta na execução dessas auditorias poderá comprometer a imparcialidade e a eficácia do sistema de controlo, recomendando-se, por conseguinte, a clara delimitação de funções no âmbito das estruturas de *compliance* organizacional.

Em termos conclusivos, pode sustentar-se que a conformidade das organizações com o RGPD, designadamente através da designação de um EPD e da efetiva valorização do seu papel na definição e implementação de medidas adequadas de proteção de dados, constitui um fator determinante para a consolidação de uma cultura organizacional orientada para a responsabilidade e a transparência no tratamento de dados pessoais. Tal realidade não só reforça o cumprimento das obrigações legais, como contribui igualmente para o fortalecimento da confiança institucional e da credibilidade das organizações perante titulares de dados, entidades reguladoras e a sociedade em geral.

Referências

Barreto Menezes Cordeiro, A. (2021). *Comentário ao Regulamento Geral de Proteção de Dados e à Lei n.º 58/2019*. Edições Almedina.

Comissão Nacional de Proteção de Dados. (2019, setembro 3). *Deliberação/2019/494*. https://www.cnpd.pt/decisoes/historico-de-decisoes/?year=2019&type=2&ent=

Despacho n.º 7456/2017 (2017, agosto 24). *Diário da República, 2ª série, n.º 163*. https://dre.pt/dre/detalhe/despacho/7456-2017-108041501

Dicionário Priberam da Língua Portuguesa. (n.d.). *Compliance*. https://dicionario.priberam.org/compliance

Grupo de Trabalho do Artigo 29.º para a Proteção de Dados. (2016). *Orientações sobre os encarregados da proteção de dados (EPD) (WP243 rev.01)*. https://www.cnpd.pt/media/meplvdie/wp243rev01_pt.pdf

Lei n.º 58/2019. (2019, agosto 8). *Diário da República, 1ª série, n.º 151*. https://dre.pt/dre/detalhe/lei/58-2019-123815982

Pedreira, F. (2019, novembro 5). Uma nova porta para os dados pessoais. *ECO*. https://eco.sapo.pt/2019/11/05/uma-nova-porta-para-os-dados-pessoais/

Parlamento Europeu & Conselho da União Europeia. (2016, abril 27). *Regulamento (UE) 2016/679 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (Regulamento Geral sobre a Proteção de Dados)*. Jornal Oficial da União Europeia, L 119. https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32016R0679

Portal do DPO. (n.d.). *Glossário RGPD*. https://www.portaldodpo.pt/glossario/

Universidade de Coimbra. (n.d.). *Encarregado de Proteção de Dados*. https://www.uc.pt/protecao-de-dados/protecao-de-dados-pessoais/encarregado-protecao-dedados/

Declaração Ética

Conflito de Interesse: Nada a declarar. **Financiamento:** Nada a declarar. **Revisão por Pares:** Dupla-cega.

Procedimento de análise forense digital a dispositivos móveis em Portugal

Digital forensic analysis procedure for mobile devices in Portugal

10.29073/j2.v8i1.1110

Recebido: 01 de março de 2026.
Aprovado: 30 de março de 2026.
Publicado: 04 de abril de 2026.

Autor/a 1 (Correspondente): Carla Pinto, ESTG-IPP, Portugal, pinto.carla@gmail.com.

Autor/a 2: Patrícia Azevedo, ESTG-IPP, Portugal. pamv@estg.ipp.pt.

Autor/a 3: Pedro Pinto, ISEP, Portugal, pfp@isep.ipp.pt.

Resumo

A análise forense digital de dispositivos móveis constitui uma área emergente e de crescente relevância no âmbito da investigação criminal, atendendo à quantidade e à relevância da informação armazenada nestes dispositivos. O presente trabalho tem como objetivo definir um procedimento estruturado e padronizado para a realização de análise forense digital a dispositivos móveis em Portugal, em conformidade com o enquadramento jurídico nacional e europeu, designadamente a Lei do Cibercrime (Lei n.º 109/2009, de 15 de setembro) e o Regulamento Geral sobre a Proteção de Dados (Regulamento (UE) 2016/679).

No desenvolvimento deste trabalho, são identificados diversos desafios técnicos e jurídicos, entre os quais a encriptação de dados, os mecanismos de autenticação biométrica e a inexistência de uma metodologia uniformizada aplicável ao contexto português. A ausência de procedimentos padronizados pode comprometer a integridade da prova digital e a sua admissibilidade em processo judicial, tornando necessária a definição de boas práticas alinhadas com normas internacionais de investigação forense digital.

Pretende-se, assim, contribuir para o apoio aos profissionais da área jurídica e forense, propondo um procedimento estruturado que assegure a preservação da cadeia de custódia, a integridade dos dados e o cumprimento das exigências legais e éticas aplicáveis à recolha e análise de prova digital.

Palavras-Chave: Cadeia de Custódia; Dispositivos Móveis; Forense Digital; Lei do Cibercrime; Prova Digital.

Abstract

Digital forensic analysis of mobile devices is an emerging and increasingly relevant area in criminal investigation, given the quantity and relevance of the information stored on these devices. This work aims to define a structured and standardized procedure for conducting digital forensic analysis of mobile devices in Portugal, in accordance with the national and European legal framework, namely the Cybercrime Law (Law No. 109/2009, of September 15) and the General Data Protection Regulation (Regulation (EU) 2016/679).

In the development of this work, several technical and legal challenges are identified, including data encryption, biometric authentication mechanisms, and the lack of a standardized methodology applicable to the Portuguese context. The absence of standardized procedures can compromise the integrity of digital evidence and its admissibility in judicial proceedings, making it necessary to define best practices aligned with international standards for digital forensic investigation.

The aim is to contribute to supporting professionals in the legal and forensic field by proposing a structured procedure that ensures the preservation of the chain of custody, the integrity of the data, and compliance with the legal and ethical requirements applicable to the collection and analysis of digital evidence.

Keywords: Chain Of Custody; Cybercrime Law; Digital Evidence; Digital Forensics; Mobile Devices.

1. Introdução

Com o crescimento das tecnologias de comunicação e informação, a análise forense digital tem assumido um papel cada vez mais relevante no contexto da investigação criminal, particularmente no que respeita à análise de dispositivos móveis. Estes equipamentos armazenam grandes volumes de informação pessoal e profissional, podendo conter dados essenciais para a reconstrução de acontecimentos e para a obtenção de prova digital com relevância processual. Ao contrário do que sucedia em décadas anteriores, em que a investigação se baseava sobretudo em registos de chamadas telefónicas, os dispositivos atuais armazenam mensagens, correio eletrónico, fotografias, vídeos, dados de localização e histórico de utilização, ampliando significativamente o potencial probatório da análise digital (Xu, 2019; Kiran et al., 2019; Santos, 2024; Cruz-Cunha & Mateus-Coelho, 2020).

Neste contexto, crescente digitalização da sociedade tem transformado profundamente os métodos de investigação criminal, conduzindo ao aumento da relevância da análise forense digital como instrumento de recolha e interpretação de prova eletrónica.

A elevada taxa de utilização de dispositivos móveis na sociedade contemporânea reforça a importância da informática forense neste domínio. Estudos recentes indicam que a maioria da população utiliza diariamente smartphones para comunicação, acesso à Internet e armazenamento de dados pessoais, aumentando a probabilidade de estes dispositivos conterem elementos relevantes para processos judiciais. Consequentemente, a perícia forense aplicada a dispositivos móveis tornou-se uma área crítica da investigação digital, exigindo métodos rigorosos e tecnicamente fundamentados que garantam a integridade, autenticidade e fiabilidade da prova obtida[1].

Apesar da sua relevância, a análise forense de dispositivos móveis apresenta diversas dificuldades técnicas. Cada equipamento possui características próprias, diferentes sistemas operativos e mecanismos específicos de segurança, o que implica a utilização de metodologias distintas para a recolha e análise de dados. A constante evolução tecnológica agrava esta complexidade, uma vez que novos dispositivos incorporam mecanismos avançados de proteção, como encriptação de dados, autenticação biométrica e códigos de acesso, dificultando o acesso à informação armazenada. Como consequência, as ferramentas forenses necessitam de atualização permanente para acompanhar estas alterações, garantindo que os dados podem ser extraídos de forma fiável e sem comprometer a sua integridade (Kiran et al., 2019).

Outro fator que contribui para a complexidade desta área é a inexistência de procedimentos uniformes e universalmente aceites na prática forense, em especial no contexto jurídico português. Embora existam orientações internacionais para a recolha, preservação e análise de prova digital, designadamente as publicadas pelo National Institute of Standards and Technology (NIST) e por organismos internacionais de cooperação policial, a sua aplicação prática pode variar entre instituições, tribunais e investigadores. Esta falta de uniformização pode originar inconsistências metodológicas e colocar em causa a credibilidade da prova digital, comprometendo a sua admissibilidade em tribunal e a eficácia das investigações (Ramalho, 2013).

Para além das dificuldades técnicas e metodológicas, a análise forense digital encontra-se fortemente condicionada por requisitos legais e éticos. A recolha e o tratamento de dados pessoais devem respeitar o enquadramento jurídico aplicável, nomeadamente as normas relativas à proteção de dados e aos direitos fundamentais dos cidadãos. O Regulamento (UE) 2016/679 estabelece regras rigorosas quanto ao tratamento de dados pessoais, impondo que a recolha seja realizada de forma proporcional, transparente e segura, garantindo o respeito pela privacidade e pelos direitos dos titulares dos dados (European Union, 2016). No ordenamento jurídico português, a investigação criminal deve ainda observar o Código de Processo Penal, a Lei do Cibercrime e a legislação relativa à proteção de dados, que definem os limites legais da obtenção de prova

[1] https://invoicexpress.com/relatorio-digital-portugal-2024/

digital e as condições da sua utilização em processo judicial (República Portuguesa, 1987; Assembleia da República, 2009; Portugal, 2019).

Face a este enquadramento, torna-se necessário desenvolver procedimentos técnicos e jurídicos que permitam realizar a análise forense de dispositivos móveis de forma consistente, garantindo simultaneamente a validade científica e a admissibilidade legal da prova.

O presente artigo tem como objetivo contribuir para a normalização da análise forense digital de dispositivos móveis no contexto jurídico português, propondo um procedimento estruturado para a recolha, preservação e análise de evidência digital, alinhado com a legislação nacional e europeia e com as boas práticas internacionais na área da informática forense.

A prova digital pode ser definida como qualquer informação armazenada, processada ou transmitida por sistemas informáticos ou redes de comunicações que possua valor probatório, incluindo ficheiros, registos de atividade, mensagens, dados de tráfego ou metadados (National Institute of Standards and Technology, 2006). A natureza desta prova apresenta características específicas, como intangibilidade, volatilidade e facilidade de alteração, o que exige procedimentos especializados para garantir a autenticidade e integridade da informação recolhida (National Institute of Justice, 2008).

Para alcançar este objetivo, definem-se dois objetivos específicos. O primeiro consiste na análise do enquadramento legal nacional e europeu aplicável à prova digital, com especial destaque para a Lei do Cibercrime, o Código de Processo Penal, a legislação de proteção de dados e o Regulamento Geral sobre a Proteção de Dados. A revisão destas normas permite identificar limitações jurídicas, lacunas regulatórias e requisitos formais que devem ser respeitados para garantir a validade da prova digital em tribunal.

O segundo consiste na definição de um procedimento técnico para a análise forense de dispositivos móveis, destinado a ser utilizado por autoridades judiciais e órgãos de investigação criminal. Este procedimento deverá ser adaptável a diferentes tipos de dispositivos e sistemas operativos, respeitando simultaneamente as exigências legais e as boas práticas internacionais de informática forense. A padronização das etapas de recolha, preservação e análise pretende reduzir erros metodológicos e assegurar a cadeia de custódia da prova digital.

O restante artigo encontra-se organizado da seguinte forma: a Secção 2 apresenta o enquadramento da análise forense digital, incluindo os principais conceitos, o enquadramento jurídico e as principais normas e diretrizes internacionais aplicáveis; a Secção 3 discute o atual enquadramento e as lacunas identificadas; a Secção 4 apresenta o procedimento proposto para a análise forense digital de dispositivos móveis; por fim, são apresentadas as conclusões finais do estudo.

2. Análise Forense Digital - Enquadramento e Desafios Técnicos e Éticos

A análise forense digital corresponde ao conjunto de métodos técnicos e procedimentos jurídicos destinados à recolha, preservação, exame, análise e apresentação de dados digitais com relevância probatória. Esta prática é utilizada em investigações criminais, processos civis, auditorias e outras situações em que a informação eletrónica possa assumir valor de prova (Cohen, 2012).

A prova digital pode ser definida como qualquer informação armazenada, processada ou transmitida por sistemas informáticos ou redes de comunicações que possua valor probatório, incluindo ficheiros, registos de atividade, mensagens, dados de tráfego ou metadados (National Institute of Standards and Technology, 2006). A natureza desta prova apresenta características específicas, como intangibilidade, volatilidade e facilidade de alteração, o que exige procedimentos especializados para garantir a autenticidade e integridade da informação recolhida (National Institute of Justice, 2008).

Para que os resultados obtidos sejam admissíveis em tribunal, é necessário assegurar simultaneamente o cumprimento de requisitos técnicos e legais, garantindo a autenticidade, integridade e fiabilidade da informação analisada (Kist, 2019). No ordenamento jurídico português, a admissibilidade da prova digital encontra

fundamento nos princípios constitucionais do processo penal, designadamente nas garantias de defesa, no princípio da legalidade e na proibição da utilização de provas obtidas por meios ilícitos. O Código de Processo Penal não contém uma definição autónoma de prova digital, sendo aplicáveis, por analogia, os regimes previstos para outros meios de obtenção de prova, complementados por legislação específica relativa ao cibercrime e à obtenção de dados eletrónicos.

A Lei n.º 109/2009, conhecida como Lei do Cibercrime, introduziu no ordenamento jurídico português mecanismos próprios para a obtenção de prova digital, adaptando o sistema processual às exigências do ambiente tecnológico. Este diploma transpõe para o direito interno a Convenção sobre o Cibercrime e estabelece medidas como a pesquisa informática, a apreensão de dados, a interceção de comunicações e a preservação de informação eletrónica (Assembleia da República, 2009; Conselho da União Europeia, 2001). Complementarmente, a Lei n.º 32/2008 regula a conservação e transmissão de dados de tráfego e de localização por operadores de comunicações, permitindo o seu acesso em investigações criminais, sobretudo em crimes graves (Lei n.º 32/2008, 2008).

Do ponto de vista técnico, a análise forense digital segue frequentemente modelos metodológicos reconhecidos internacionalmente. Um dos mais utilizados é o modelo proposto pelo National Institute of Standards and Technology (NIST), que organiza o processo forense em quatro fases principais: apreensão, aquisição, análise e reporte (National Institute of Standards and Technology, 2006). A fase de apreensão visa assegurar a preservação dos dados desde o momento da recolha; a aquisição corresponde à extração e tratamento da informação; a análise envolve a interpretação dos resultados e a reconstrução de eventos; e o reporte consiste na elaboração de um relatório técnico detalhado destinado às autoridades judiciais (Cohen, 2012).

A validade da prova digital depende da conformidade com normas legais e com boas práticas técnicas reconhecidas pela comunidade científica. A utilização de mecanismos de verificação de integridade, como funções de hash, bem como a preservação da autenticidade e confidencialidade dos dados são essenciais para garantir que a prova não foi alterada desde a sua recolha até à sua apresentação em tribunal (Cohen, 2012; Ramos, 2014). Neste contexto, a cooperação entre peritos forenses, autoridades de investigação criminal e magistrados assume particular relevância para assegurar o respeito simultâneo pelos requisitos técnicos e jurídicos.

Um elemento fundamental na análise forense digital é o conceito de metadados, entendidos como dados que descrevem outros dados e que fornecem informação sobre a sua origem, estrutura e contexto (Gilliland, 2016). A norma ISO 23081-1 classifica os metadados em categorias descritivas, estruturais e administrativas, todas relevantes para a gestão e preservação da informação digital (International Organization for Standardization, 2017). No contexto forense, os metadados permitem estabelecer a proveniência de um ficheiro, reconstruir sequências temporais e detetar alterações.

Outro conceito essencial é o da cadeia de custódia, correspondente ao conjunto de procedimentos destinados a documentar todas as fases do tratamento da prova digital, desde a sua identificação até à sua apresentação em tribunal. Este registo deve assegurar a integridade da prova, identificando responsáveis, datas, locais e transferências de responsabilidade (National Institute of Justice, 2008). A doutrina portuguesa sublinha que a observância rigorosa destes procedimentos é determinante para a admissibilidade da prova digital em juízo (Ramos, 2014).

Deste modo, a análise forense digital constitui uma área interdisciplinar que exige a articulação entre conhecimento técnico e enquadramento jurídico, sendo necessária a atualização permanente de métodos e normas para assegurar que a prova digital possa ser utilizada de forma válida, fiável e juridicamente admissível.

Esta secção apresenta o enquadramento da análise forense digital, abordando o enquadramento jurídico da prova digital em Portugal, seguido das principais normas e diretrizes internacionais aplicáveis à investigação forense digital.

2.1. Enquadramento Jurídico da Prova Digital

A análise forense digital de dispositivos móveis desenvolve-se no âmbito de um enquadramento jurídico complexo, destinado a garantir simultaneamente a eficácia da investigação criminal e a proteção dos direitos fundamentais. Em Portugal, este enquadramento resulta da articulação entre legislação penal, processual penal, normas específicas relativas à criminalidade informática e legislação de proteção de dados pessoais.

A Lei n.º 109/2009, conhecida como Lei do Cibercrime, estabelece os principais mecanismos de recolha e preservação de prova digital, em conformidade com a Convenção sobre o Cibercrime do Conselho da Europa (Convenção de Budapeste) (Assembleia da República, 2009; Council of Europe, 2001). O Regulamento (UE) 2016/679, relativo à proteção de dados pessoais, complementado pela Lei n.º 58/2019, impõe limites rigorosos ao tratamento de informação, atendendo à natureza sensível dos dados armazenados em dispositivos móveis.

O Código Penal tipifica crimes informáticos, enquanto o Código de Processo Penal regula as diligências de busca, apreensão e perícia, garantindo a integridade e a rastreabilidade da prova. Neste contexto, a investigação digital exige uma articulação permanente entre requisitos técnicos e princípios jurídicos, sob pena de comprometer a validade da prova em tribunal.

Como refere Rakha (2024), o combate ao cibercrime exige uma abordagem integrada entre os aspetos técnicos da investigação digital e os princípios jurídicos e éticos que a sustentam, sendo que a ausência dessa harmonização pode comprometer a admissibilidade e a legitimidade da prova digital.

Em conjunto, estas normas procuram assegurar um equilíbrio entre a eficácia da investigação criminal e o respeito pela legalidade processual e pela privacidade dos cidadãos, impondo que a recolha e análise de dados digitais sejam autorizadas, fundamentadas e realizadas segundo procedimentos controláveis.

2.1.1. Lei Cibercrime

A Lei n.º 109/2009, de 15 de setembro, conhecida como Lei do Cibercrime, estabelece o regime jurídico aplicável à criminalidade informática e define mecanismos específicos de obtenção de prova digital, transpondo para o ordenamento jurídico português a Convenção sobre o Cibercrime do Conselho da Europa e instrumentos europeus relativos à cooperação penal em matéria informática (Assembleia da República, 2009; Council of Europe, 2001; União Europeia, 2005).

O diploma introduz conceitos fundamentais como sistema informático, dados informáticos e fornecedor de serviços, que constituem a base para a aplicação das normas penais e processuais relativas à investigação digital. No plano substantivo, prevê crimes como acesso ilegítimo, interceção ilícita, sabotagem informática, falsidade informática e reprodução não autorizada de programas protegidos, bem como a responsabilidade penal das pessoas coletivas e a perda de instrumentos utilizados na prática do crime (Assembleia da República, 2009).

No plano processual, a lei estabelece meios específicos de obtenção de prova digital, incluindo a preservação expedita de dados, a revelação de dados de tráfego, a injunção para apresentação de informação, a pesquisa em sistemas informáticos, a apreensão de dados e a interceção de comunicações. Estes mecanismos assumem especial relevância na investigação forense digital, atendendo à natureza volátil da informação eletrónica, que pode ser rapidamente alterada ou eliminada.

A Lei do Cibercrime prevê ainda a aplicação subsidiária do Código de Processo Penal sempre que não exista regime próprio, assegurando que as diligências respeitam as garantias processuais fundamentais. A jurisprudência constitucional tem reforçado a necessidade de autorização judicial prévia quando estejam em causa direitos fundamentais, nomeadamente no acesso a comunicações eletrónicas, sublinhando a importância do controlo judicial na obtenção de prova digital (Tribunal Constitucional, 2021).

2.1.2. Proteção de Dados Pessoais e RGPD

A investigação forense digital envolve frequentemente o tratamento de dados pessoais, pelo que deve respeitar o regime jurídico da proteção de dados. O Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho

estabelece o quadro jurídico aplicável ao tratamento de dados pessoais na União Europeia, reconhecendo a proteção de dados como direito fundamental e definindo princípios como a limitação da finalidade, a minimização dos dados, a proporcionalidade e a responsabilidade do responsável pelo tratamento (União Europeia, 2016).

Em Portugal, a Lei n.º 58/2019 assegura a execução do regulamento no ordenamento jurídico nacional, enquanto a Lei n.º 59/2019 regula o tratamento de dados pessoais por autoridades competentes para efeitos de prevenção, investigação e repressão de infrações penais, estabelecendo salvaguardas específicas para conciliar a segurança pública com a proteção dos direitos fundamentais (Portugal, 2019a; Portugal, 2019b).

A supervisão do cumprimento destas normas cabe à Comissão Nacional de Proteção de Dados, autoridade independente responsável pela fiscalização do tratamento de dados pessoais e pela aplicação de sanções em caso de violação das regras legais (Portugal, 2004).

A doutrina tem destacado o impacto do Regulamento Geral sobre a Proteção de Dados na investigação digital, exigindo que a recolha e tratamento de informação sejam autorizados, documentados e limitados ao estritamente necessário para a finalidade processual. Técnicas como a pseudonimização e a anonimização são frequentemente recomendadas para reduzir riscos para os titulares dos dados, mantendo simultaneamente a utilidade probatória da informação (Osório, 2023; Limberger et al., 2023).

No contexto da análise forense digital, o cumprimento destas normas é essencial para garantir que a prova obtida respeita os direitos fundamentais e pode ser utilizada validamente em processo judicial.

2.1.3. Código Penal

O Código Penal português define os tipos legais de crime e estabelece as respetivas sanções, tendo sido progressivamente adaptado para incluir normas relativas à criminalidade informática (Portugal, 1982). A ratificação da Convenção de Budapeste reforçou a necessidade de harmonização legislativa, conduzindo à introdução de disposições específicas relativas a sistemas informáticos e comunicações eletrónicas (Portugal, 2009).

A Lei do Cibercrime complementa o Código Penal ao tipificar condutas relacionadas com sistemas informáticos e redes de comunicação, devendo a interpretação destas normas respeitar os princípios gerais da tipicidade, ilicitude e culpa. Entre os crimes relevantes destacam-se o acesso ilegítimo, a sabotagem informática, a falsidade informática e a burla informática, frequentemente associados à obtenção de prova digital em dispositivos móveis.

A investigação de crimes informáticos exige a recolha de prova digital capaz de demonstrar a autoria, a materialidade do facto e a ligação entre o agente e o sistema informático. A volatilidade dos dados eletrónicos obriga à utilização de procedimentos técnicos adequados, como a criação de cópias forenses e a verificação de integridade através de funções de hash, de modo a assegurar a fiabilidade da prova (Casey, 2011).

A doutrina portuguesa tem sublinhado que a validade da prova digital depende da utilização de métodos reconhecidos e da intervenção de peritos qualificados, capazes de garantir que a análise respeita os padrões técnicos e jurídicos exigidos pelo processo penal (Marques Branco, 2021).

2.1.4. Código Processo Penal

O Código de Processo Penal estabelece o regime geral da prova e define as regras aplicáveis à recolha, preservação e apresentação de elementos probatórios (Portugal, 1987). No contexto da análise forense digital, assumem especial relevância as normas relativas à prova pericial, às buscas e apreensões e à interceção de comunicações.

A prova pericial é necessária sempre que a apreciação dos factos exige conhecimentos técnicos ou científicos, sendo essencial na informática forense, onde a interpretação dos dados requer competências especializadas. O relatório pericial deve documentar todas as operações realizadas, permitindo o controlo judicial e o exercício do contraditório (Veríssimo, 2023).

As buscas e apreensões dependem, em regra, de autorização judicial e devem ser realizadas de forma proporcional e devidamente documentada. A Lei do Cibercrime adapta estas regras ao ambiente informático, prevendo procedimentos específicos para a pesquisa e apreensão de dados, mantendo, contudo, a exigência de controlo judicial sempre que estejam em causa direitos fundamentais.

A jurisprudência tem afirmado que a apreensão de comunicações eletrónicas requer despacho do juiz de instrução, distinguindo-se entre interceção de comunicações em trânsito e acesso a mensagens armazenadas, regimes que obedecem a requisitos legais distintos. O regime de interceção de comunicações é restrito a determinados crimes e depende de autorização judicial prévia, incluindo regras rigorosas quanto à execução e conservação dos registos.

Embora o Código de Processo Penal não utilize expressamente o termo cadeia de custódia, as regras relativas à apreensão, guarda e documentação de objetos impõem a preservação da integridade da prova. Na análise forense digital, essa integridade é garantida através de técnicas como o cálculo de valores de hash e o registo de metadados, que permitem verificar que os dados não foram alterados desde a sua recolha (Casey, 2011).

Assim, o Código de Processo Penal fornece o enquadramento legal geral da prova, enquanto a Lei do Cibercrime estabelece mecanismos específicos adaptados ao ambiente digital. A conjugação entre normas jurídicas, procedimentos técnicos e controlo judicial é essencial para assegurar que a prova digital obtida em dispositivos móveis seja válida, fiável e admissível em tribunal.

2.2. Normas e Diretrizes Internacionais

A análise forense digital é orientada não apenas por legislação nacional, mas também por normas e diretrizes internacionais que estabelecem boas práticas para a recolha, preservação e análise de evidência digital. Estas orientações contribuem para a uniformização de procedimentos, promovendo maior rigor metodológico e reforçando a credibilidade da prova digital em contexto judicial. Entre os referenciais mais relevantes destacam-se as publicações do National Institute of Standards and Technology (NIST), as diretrizes da INTERPOL para primeiros intervenientes em evidência digital e as normas da International Organization for Standardization (ISO), que estabelecem princípios e procedimentos amplamente reconhecidos na comunidade científica e forense.

Nos pontos seguintes serão analisadas estas normas e orientações, evidenciado o seu contributo para a investigação forense digital em dispositivos móveis.

2.2.1. Publicações NIST

O NIST, organismo norte-americano de referência na definição de normas e boas práticas nos domínios da segurança da informação e da ciência forense digital, tem publicado um conjunto relevante de documentos orientadores para profissionais, académicos e instituições. Estas publicações assumem particular importância por fornecerem metodologias estruturadas, tecnicamente sólidas e internacionalmente reconhecidas, promovendo procedimentos rigorosos na recolha, preservação, análise e apresentação de prova digital.

Entre os documentos mais relevantes para a forense digital destacam-se a NIST SP 800-86: Guide to Integrating Forensic Techniques into Incident Response, dedicada à integração de técnicas forenses nos processos de resposta a incidentes; a NIST SP 800-72: Guidelines on PDA Forensics, centrada nos dispositivos PDA, precursores dos smartphones; a NIST SP 800-115: Technical Guide to Information Security Testing and Assessment, voltada para testes e auditorias de segurança; e, sobretudo, a NIST SP 800-101 Revision 1: Guidelines on Mobile Device Forensics, que constitui atualmente uma das principais referências internacionais para a análise forense de dispositivos móveis (National Institute of Standards and Technology, 2006; Ayers et al., 2014).

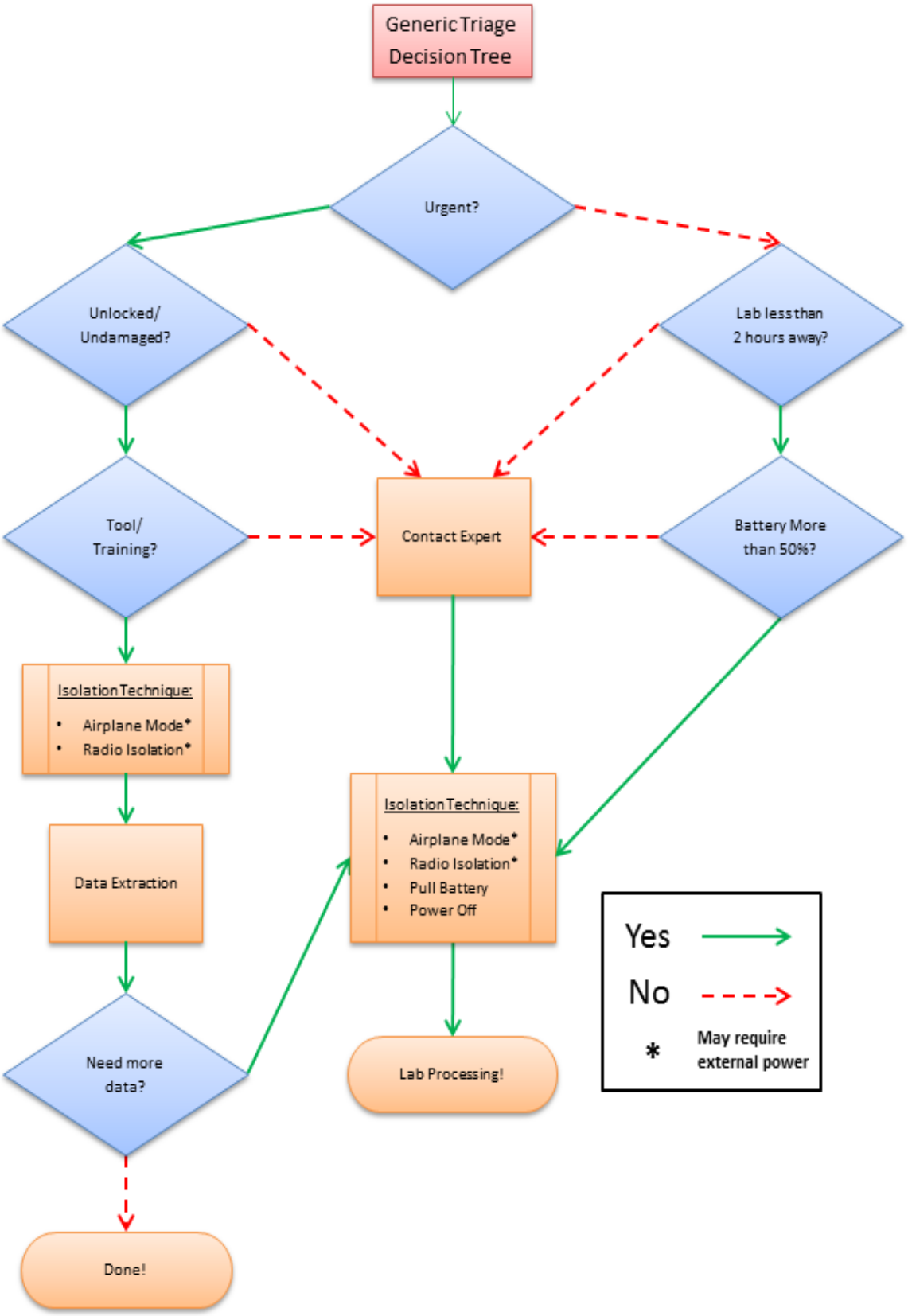
No que respeita à análise forense aplicada a dispositivos móveis, a NIST SP 800-101 Revision 1 ocupa lugar central. O documento surgiu como resposta à transformação tecnológica que converteu smartphones e tablets em repositórios de informação pessoal e profissional. Estes equipamentos concentram hoje comunicações, registos de localização, contas de correio eletrónico, conteúdos multimédia, aplicações bancárias, redes sociais e acesso a serviços em nuvem, tornando-se fontes privilegiadas de prova digital. Em simultâneo, essa evolução tecnológica aumentou a complexidade da sua análise forense, devido à diversidade de plataformas, ao ritmo acelerado de atualização dos sistemas e à crescente sofisticação dos mecanismos de segurança.

A publicação estrutura o processo forense em quatro grandes fases – apreensão, aquisição, análise e reporte – concebidas para assegurar não apenas a extração de dados relevantes, mas também a sua validade, integridade e admissibilidade em tribunal (Ayers et al., 2014). Estas fases não devem, contudo, ser entendidas como etapas rígidas e absolutamente lineares. Em contexto prático, podem ocorrer sobreposições, repetições e ajustamentos metodológicos em função das características concretas de cada caso, nomeadamente quando há necessidade de validar dados intermédios, repetir aquisições ou agir rapidamente perante informação volátil em risco de perda. Essa flexibilidade não fragiliza o processo; pelo contrário, reforça-o, porque permite adaptar a metodologia às circunstâncias da investigação sem comprometer o rigor técnico e jurídico.

A Figura 1 apresenta a triagem recomendada pela NIST SP 800-101 (Ayers et al., 2014). Esse fluxograma orienta o processo decisório nas fases iniciais da recolha de dispositivos, considerando fatores como a urgência do caso, o estado do equipamento, o nível de bateria e os recursos técnicos disponíveis. Em situações urgentes, a prioridade incide sobre a avaliação imediata do estado do dispositivo, a aplicação de técnicas de isolamento e, quando possível, a extração de dados. Em contextos menos urgentes, o modelo orienta o envio seguro do dispositivo para o laboratório, reduzindo o risco de perda, alteração ou contaminação dos dados e reforçando a fiabilidade da prova recolhida.

Deste modo, a Lei do Cibercrime constitui o principal instrumento jurídico na investigação forense digital, definindo simultaneamente o quadro penal e os procedimentos de recolha de prova em ambiente informático.

Figura 1: Procedimento geral proposto na NIST SP 800-101.



Fonte: NIST.

Cada uma das fases referidas é detalhada de seguida.

Fase 1: Apreensão

A apreensão constitui o ponto de partida do processo forense e assume importância decisiva para a validade da evidência digital. O seu objetivo é garantir que os dados existentes no dispositivo permanecem inalterados desde o momento da apreensão até à análise laboratorial, preservando a integridade, a autenticidade e a admissibilidade da prova.

No local da ocorrência, a primeira exigência consiste na documentação rigorosa do dispositivo e do contexto em que foi encontrado. Devem ser registadas as condições em que o equipamento se apresenta, nomeadamente se está ligado ou desligado, bloqueado ou desbloqueado, ligado à rede ou em modo offline, bem como o ambiente físico da apreensão. Esta documentação deve incluir fotografias, anotações detalhadas e identificação dos intervenientes presentes, de modo a fixar o estado inicial da evidência.

Um dos aspetos mais sensíveis desta fase é o isolamento do dispositivo, destinado a impedir alterações remotas aos dados, resultantes de sincronizações automáticas, atualizações, comunicações de rede ou ações deliberadas de terceiros. Para esse efeito, podem ser utilizadas bolsas de Faraday ou, quando operacionalmente viável, ativado o modo de voo. Em paralelo, deve ser assegurada a conservação física do equipamento, com recurso a invólucros adequados e embalagens seladas, protegendo-o contra danos mecânicos e ambientais.

O transporte até ao laboratório deve ocorrer em condições controladas e devidamente documentadas, de modo a manter a cadeia de custódia. Cada intervenção sobre o dispositivo deve ser registada, incluindo a identificação de quem apreendeu o equipamento, em que circunstâncias, que procedimentos foram adotados e quem teve acesso posterior à evidência. Em síntese, a apreensão constitui a base de todo o procedimento forense: sem uma recolha inicial rigorosa, a análise subsequente pode perder valor técnico e jurídico.

Fase 2: Aquisição

A aquisição representa uma das fases mais críticas da análise forense em dispositivos móveis, pois dela dependem a preservação do conteúdo digital e a possibilidade de replicação futura da análise. A NIST SP 800-101 organiza esta fase segundo uma classificação em cinco níveis, diferenciados pelo grau de complexidade técnica, intrusividade e profundidade de acesso à memória do equipamento (Ayers et al., 2014).

O primeiro nível corresponde à aquisição manual, em que o perito interage diretamente com o dispositivo e regista a informação visível no ecrã. Trata-se de um método simples e pouco intrusivo, útil em cenários urgentes ou na ausência de ferramentas especializadas, mas limitado à informação acessível visualmente e sujeito a erro humano (Ayers et al., 2014).

O segundo nível é a aquisição lógica, que permite extrair objetos de dados através do sistema operativo do dispositivo e das interfaces de comunicação disponíveis. Este método possibilita o acesso a mensagens, contactos, registos de chamadas, emails, ficheiros multimédia e dados de aplicações, sendo amplamente suportado por ferramentas forenses e apresentando a vantagem de ser relativamente rápido e não intrusivo. Contudo, raramente permite recuperar dados apagados ou aceder a áreas protegidas da memória.

O terceiro nível corresponde à aquisição física, que produz uma cópia bit a bit da memória do dispositivo, permitindo aceder a dados ativos, apagados ou fragmentados. Entre as técnicas possíveis incluem-se o recurso a interfaces de depuração JTAG e a utilização de bootloaders modificados (Joint Test Action Group, 2013). Embora este método seja mais completo, exige equipamento especializado, maior conhecimento técnico e comporta riscos acrescidos para o equipamento (Ayers et al., 2014).

O quarto nível, designado chip-off, consiste na remoção física do chip de memória para leitura externa, sendo reservado para situações em que o dispositivo está danificado ou em que os métodos anteriores falharam. É uma técnica altamente invasiva e potencialmente destrutiva, que requer condições laboratoriais adequadas e elevada especialização (Ayers et al., 2014).

O quinto e último nível é o micro-read, técnica extremamente especializada que consiste na leitura direta das células de memória através de microscopia eletrónica. Dada a sua complexidade, custo e morosidade, constitui uma solução de último recurso, aplicável apenas em casos excecionais.

Para além da memória interna do dispositivo, a aquisição deve abranger outras fontes relevantes de prova, como cartões SIM/UICC, cartões de memória removíveis e dados armazenados em cloud. Os cartões SIM/UICC podem conter identificadores como o IMSI e o ICCID, bem como mensagens, contactos e outros registos relevantes, sendo analisados com leitores especializados (MSAB, 2025).

Os cartões SD ou microSD devem ser tratados como suportes removíveis e sujeitos a clonagem forense, com verificação de integridade por meio de hashes. Já os dados em cloud assumem importância crescente, dado que muitos sistemas e aplicações realizam cópias automáticas para serviços remotos. A sua recolha amplia o alcance da investigação, mas exige cuidados acrescidos de ordem técnica e jurídica, nomeadamente no que respeita à obtenção de credenciais ou autorizações judiciais (Ayers et al., 2014).

A aquisição de dados em *Cloud* tornou-se parte das investigações forenses, pois dispositivos móveis podem criar cópias de segurança em serviços como iCloud, Google Drive ou OneDrive. A informação pode estar armazenada fora do equipamento. A recolha desses dados requer credenciais do utilizador ou ordens judiciais para acesso aos conteúdos. Ferramentas forenses incluem módulos de extração em *Cloud*, permitindo sincronizar e descarregar dados de contas online. A aquisição aumenta o alcance da investigação e exige controlo da cadeia de custódia e cumprimento do enquadramento jurídico (Ayers et al., 2014).

Fase 3: Análise

A fase de análise é aquela em que os dados adquiridos são processados, interpretados e correlacionados, com vista à produção de informação dotada de valor probatório. Se nas fases anteriores se privilegia a preservação da evidência, aqui a ênfase recai sobre a sua interpretação contextual e técnica, permitindo responder a questões concretas da investigação (Ayers et al., 2014).

O tratamento inicial da evidência inclui a organização e filtragem dos dados, a identificação de estruturas de ficheiros, a extração de bases de dados internas, a indexação de documentos e a recuperação de informação oculta, fragmentada ou eliminada. Técnicas de parsing permitem reconstruir conteúdos de aplicações móveis, tais como mensagens, históricos de navegação e registos de localização, mesmo quando dispersos por múltiplos ficheiros ou diretórios.

A análise pressupõe também a correlação dos dados com hipóteses investigatórias. Entre as operações mais relevantes incluem-se a associação entre chamadas, mensagens e contactos, a reconstrução de percursos com base em dados de GPS ou torres de telecomunicações, a identificação de comunicações em redes sociais e a deteção de programas maliciosos ou técnicas de ocultação de atividade. Em casos complexos, é frequente recorrer à validação cruzada com diferentes ferramentas, para confirmar a consistência e fiabilidade dos resultados.

Entre os principais desafios desta fase destaca-se a encriptação, cada vez mais presente nos dispositivos modernos. PIN, passwords, padrões de desbloqueio e mecanismos biométricos podem limitar o acesso à informação, obrigando ao recurso a técnicas específicas, sempre em conformidade com o enquadramento legal. Também os formatos proprietários e os mecanismos de compressão exigem ferramentas forenses atualizadas e adequadas.

Os dispositivos móveis oferecem uma grande diversidade de fontes de evidência, incluindo registos de chamadas, mensagens SMS e MMS, correio eletrónico, histórico de navegação, dados de geolocalização, fotografias e vídeos com metadados embutidos, aplicações de mensagens instantâneas e redes sociais. A dimensão temporal da evidência é igualmente decisiva: a correlação entre timestamps, registos de chamadas e eventos de GPS permite reconstruir cronologias de atividade essenciais para a prova dos factos.

As ferramentas utilizadas nesta fase incluem soluções comerciais e plataformas de código aberto, cuja escolha deve atender à fiabilidade, capacidade de validação e documentação do processo. O essencial é que a análise seja repetível, tecnicamente sustentada e adequadamente registada, de forma a garantir a admissibilidade legal da prova (Sutikno, 2024; Ferreira, 2020). Em síntese, esta fase transforma a evidência digital em conhecimento útil, articulando sofisticação técnica com capacidade interpretativa do perito.

Fase 4: Reporte

A fase final consiste na elaboração do relatório pericial, documento técnico em que os resultados da análise devem ser apresentados de forma estruturada, clara, objetiva e auditável. O relatório não se limita à enumeração dos dados extraídos; deve descrever pormenorizadamente os métodos aplicados, as ferramentas utilizadas, as versões de software, os valores de integridade e as operações realizadas, permitindo que terceiros compreendam, avaliem e, se necessário, reproduzam o procedimento (Ayers et al., 2014).

Um relatório forense robusto deve incluir, em primeiro lugar, a identificação da evidência analisada, com descrição do dispositivo, suportes associados, características técnicas e estado em que foi apreendido. Deve igualmente explicitar as metodologias adotadas, justificando a escolha de determinadas técnicas de preservação, aquisição, exame e análise, bem como indicar as ferramentas utilizadas em cada etapa e as respetivas limitações conhecidas.

Os resultados devem ser apresentados de forma sistematizada, acompanhados de elementos de suporte como capturas de ecrã, logs e registos de hashes. Devem também ser identificadas as limitações encontradas, incluindo dados inacessíveis devido a encriptação, incompatibilidades técnicas ou ausência de credenciais de acesso a serviços remotos. A documentação da cadeia de custódia é igualmente indispensável, assegurando a rastreabilidade completa do processo e a identificação de todos os intervenientes que tiveram contacto com a evidência.

Por fim, o relatório deve culminar em conclusões objetivas, diretamente relacionadas com as questões formuladas pela autoridade judiciária ou com os objetivos da investigação. A inclusão de anexos técnicos, como relatórios automáticos, cronologias ou listas detalhadas de hashes, reforça a transparência e a auditabilidade do processo, permitindo uma apreciação crítica por especialistas e pelo tribunal.

Outros Aspetos

Para além da estrutura metodológica, o NIST chama a atenção para vários aspetos técnicos que podem condicionar a eficácia da análise forense em dispositivos móveis. Um deles é a distinção entre memória volátil e não volátil. A memória volátil pode conter dados temporários particularmente relevantes, como credenciais ou chaves de sessão, mas perde o seu conteúdo quando o dispositivo é desligado. Já a memória não volátil armazena dados persistentes e pode, devido a mecanismos internos de gestão, conservar fragmentos ou múltiplas versões de ficheiros suscetíveis de recuperação (Ayers et al., 2014).

Outro aspeto relevante respeita aos cartões SIM/UICC, cuja análise autónoma pode revelar dados não acessíveis através do terminal, como identificadores de rede e certos registos de comunicações. O NIST sublinha também a importância dos CDR mantidos pelas operadoras, que complementam a análise realizada ao dispositivo ao fornecerem informação sobre localização aproximada, duração das chamadas, volume de tráfego e interações entre utilizadores.

Finalmente, a publicação aborda o problema dos dispositivos protegidos por bloqueios ou encriptação. Embora descreva abordagens técnicas para ultrapassar tais barreiras, o documento alerta para os riscos significativos de perda ou alteração da evidência, recomendando que essas técnicas sejam empregues apenas por peritos altamente especializados e em estrita conformidade com as exigências legais.

Em conclusão, a NIST SP 800-101 estabelece um quadro metodológico de referência que conjuga rigor técnico com conformidade legal, promovendo práticas orientadas para a eficácia da extração de dados e para a sua

aceitabilidade em tribunal. Mais do que um manual prescritivo, constitui um guia de boas práticas fundamental para a normalização internacional da análise forense digital em dispositivos móveis e para o desenvolvimento de capacidades institucionais nesta área.

2.2.2. Diretrizes INTERPOL

A INTERPOL, enquanto organização policial internacional, tem como missão promover a cooperação entre diferentes jurisdições no combate ao crime transnacional. No domínio da cibercriminalidade, essa missão traduziu-se na definição de orientações técnicas e operacionais destinadas a apoiar os primeiros intervenientes no local — agentes policiais, investigadores ou peritos que contactam inicialmente com incidentes envolvendo dispositivos digitais. Estas orientações procuram harmonizar procedimentos, reduzir o risco de adulteração da evidência e assegurar que os métodos de recolha permanecem compatíveis com a realidade tecnológica contemporânea (INTERPOL Innovation Centre, 2021).

As orientações da INTERPOL sintetizam aquilo que a organização entende como melhores práticas forenses internacionais e assumem especial relevância no contexto da apreensão inicial de dispositivos digitais, incluindo smartphones e tablets. Tal como sucede com outros referenciais internacionais, nomeadamente os documentos do NIST, estas diretrizes procuram assegurar que a atuação dos primeiros intervenientes seja rápida, eficaz e juridicamente sustentada. Contudo, ao contrário do modelo do NIST, mais abrangente e estruturado em quatro fases, as orientações da INTERPOL concentram-se sobretudo na fase inicial da intervenção, privilegiando a preparação da apreensão e a própria apreensão, com especial atenção às exigências operacionais do trabalho de campo.

O documento mais relevante neste contexto é o Guidelines for Digital Forensics First Responders: Best Practices for Search and Seizure of Electronic and Digital Evidence, por se destinar especificamente às equipas responsáveis pela apreensão e tratamento inicial de dispositivos digitais. O ponto de partida destas orientações é claro: a evidência digital, pela sua volatilidade e suscetibilidade de alteração ou destruição, deve ser tratada com elevado rigor metodológico, de forma a preservar a sua integridade, autenticidade e admissibilidade legal. Por isso, a INTERPOL recomenda que toda a intervenção seja cuidadosamente planeada, documentada e executada segundo procedimentos padronizados (INTERPOL Innovation Centre, 2021).

Fase 1: Preparação da Apreensão

A preparação da apreensão constitui o alicerce de qualquer operação forense em ambiente digital. Segundo a INTERPOL, uma intervenção mal preparada pode comprometer de forma irreversível a recolha da prova, conduzindo à perda de dados voláteis, à contaminação da evidência ou mesmo à sua rejeição em tribunal por incumprimento de requisitos legais. A preparação deve, por isso, ser entendida como um processo sistemático que integra dimensões jurídicas, técnicas, logísticas e humanas.

O primeiro passo consiste na definição clara dos objetivos e do âmbito da operação. A equipa deve compreender a natureza do crime em investigação, antecipar os tipos de dispositivos que poderá encontrar e identificar os dados cuja preservação deverá ser prioritária. Esta delimitação orienta a seleção das ferramentas, a composição da equipa e as prioridades operacionais no terreno.

A constituição da equipa de intervenção deve igualmente ser planeada com rigor. Para além dos primeiros intervenientes, podem ser necessários peritos em forense digital, técnicos especializados em redes ou servidores, agentes de segurança para o isolamento da cena e representantes legais que garantam a conformidade da operação com as normas aplicáveis. A definição prévia de funções e responsabilidades reduz o risco de falhas de comunicação, sobreposição de tarefas ou perda de informação crítica.

A preparação jurídica assume também um papel central. Antes da intervenção, devem ser obtidos e verificados os mandados de busca e apreensão ou outras autorizações legais relevantes, incluindo a sua validade temporal e territorial. Em determinadas situações, pode ainda ser necessário preparar pedidos destinados ao acesso a dados armazenados em servidores remotos ou serviços de nuvem, o que pode implicar mecanismos de

cooperação internacional. Sem esta base legal, a prova recolhida pode tornar-se inadmissível, independentemente da sua relevância material.

No plano técnico, a preparação exige a verificação rigorosa dos kits de apreensão digital. Estes devem incluir, entre outros materiais, sacos de Faraday para impedir comunicações sem fios, bloqueadores de escrita que permitam o acesso a suportes digitais sem alteração dos dados originais, duplicadores forenses, software de aquisição para criação de imagens bit a bit, câmaras fotográficas para registo da cena, etiquetas invioláveis, blocos de notas, fontes de energia portáteis e cabos compatíveis com diferentes equipamentos. Devem ainda estar disponíveis materiais de acondicionamento, como sacos antiestáticos e recipientes resistentes a impactos ou variações de temperatura.

Acresce a necessidade de uma avaliação prévia dos riscos associados à operação. Devem ser considerados não apenas riscos físicos, como condições perigosas do local, mas também riscos digitais, incluindo a possibilidade de eliminação remota de dados, sincronização automática com serviços em nuvem ou ativação de mecanismos de encriptação após desligamento do equipamento. Antecipar estes cenários permite à equipa preparar decisões críticas, nomeadamente sobre a conveniência de uma aquisição em vivo ou da apreensão imediata do dispositivo.

Por fim, a preparação envolve a coordenação entre todos os elementos da equipa. Antes da execução, todos devem conhecer o plano da operação, a sequência de entrada no local, os procedimentos de isolamento da cena, os responsáveis por cada tarefa e as medidas de contingência a adotar em caso de resistência, falha técnica ou descoberta imprevista. Esta coordenação reduz a margem de erro e aumenta a eficácia e robustez da recolha de prova digital.

Fase 2: Apreensão

A fase de apreensão corresponde ao momento em que a operação entra em execução e os primeiros intervenientes passam a interagir diretamente com a cena e com os dispositivos digitais. Trata-se de uma etapa particularmente sensível, porque as decisões tomadas no local podem determinar o sucesso ou fracasso da recolha e preservação da evidência. A INTERPOL sublinha que esta fase deve ser conduzida com disciplina, atenção ao detalhe e estrito respeito pelos princípios da integridade, autenticidade e legalidade da prova (INTERPOL Innovation Centre, 2021).

Ao chegar ao local, a prioridade consiste no controlo e isolamento da cena. É essencial impedir o acesso de pessoas não autorizadas aos dispositivos, evitando manipulações, apagamentos ou transmissões remotas de dados. Em seguida, deve ser efetuada uma avaliação rápida do espaço, com identificação de todos os equipamentos digitais relevantes, incluindo computadores, smartphones, tablets, servidores, sistemas de videovigilância, consolas ou dispositivos IoT. Antes de qualquer manipulação, deve ser realizada documentação fotográfica e descritiva do estado em que os equipamentos foram encontrados, preservando o contexto original da cena.

A manipulação dos dispositivos é um dos momentos mais delicados da operação. Os equipamentos podem estar desligados, ligados ou em modo de suspensão, e cada uma destas situações exige decisões técnicas próprias. Se o dispositivo estiver desligado, a recomendação é, em regra, não o ligar, pois isso pode desencadear alterações automáticas, rotinas de encriptação ou perda de vestígios em memória volátil. Quando o dispositivo se encontra ligado, deve ponderar-se cuidadosamente a conveniência de o manter ativo, de forma a preservar dados transitórios, como memória RAM, sessões abertas ou ligações de rede. Essa decisão, porém, comporta riscos, incluindo a possibilidade de acessos remotos não autorizados ou ativação de mecanismos de destruição de dados. Por isso, qualquer opção tomada deve ser rigorosamente documentada, incluindo a fundamentação técnica e jurídica subjacente.

Nos equipamentos em suspensão, a complexidade é ainda maior, uma vez que o retomar da atividade pode desencadear sincronizações, atualizações ou encriptação automática. Nestes casos, a decisão sobre o

procedimento adequado deve ser reservada a profissionais qualificados e orientada por protocolos previamente definidos.

Outro elemento central desta fase é o registo em tempo real de todas as ações realizadas. Cada intervenção sobre um dispositivo deve ser documentada, indicando o agente responsável, a hora da atuação e os meios utilizados. Este registo contínuo é essencial para a cadeia de custódia, permitindo demonstrar, em momento posterior, que a evidência permaneceu íntegra e juridicamente válida.

A apreensão em contexto digital deve ainda incluir a recolha de informação complementar sobre o ambiente tecnológico envolvente. Elementos como redes Wi-Fi disponíveis, ligações Bluetooth ativas, cabos conectados e periféricos em uso podem fornecer dados relevantes sobre a utilização dos dispositivos e sobre as interações entre equipamentos ou utilizadores.

Fase 3: Preservação

A preservação consiste na adoção de medidas destinadas a garantir que a evidência recolhida se mantém íntegra e apta a ser analisada posteriormente. Uma das práticas centrais nesta fase é a criação de cópias forenses completas, através de imagens bit a bit da memória, acompanhadas de mecanismos de verificação de integridade, como resumos criptográficos.

Este procedimento permite demonstrar que a cópia corresponde fielmente ao original, assegurando a sua preservação para futuras análises e reforçando a sua aceitação em tribunal. No caso específico dos dispositivos móveis, recomenda-se a sua colocação imediata em modo de voo e o respetivo acondicionamento em sacos de Faraday. Simultaneamente, devem ser extraídos e preservados de forma autónoma os cartões SIM e os cartões de memória, por poderem conter dados relevantes que não estejam disponíveis no dispositivo principal.

Os cartões SIM podem armazenar elementos importantes, como o IMSI, o ICCID e determinados códigos de acesso, enquanto os cartões de memória podem conter fotografias, vídeos, bases de dados de aplicações ou outros ficheiros relevantes para a investigação. A sua análise deve ser realizada separadamente e sempre acompanhada de documentação adequada.

A INTERPOL chama também a atenção para a relevância das ligações de rede associadas aos dispositivos móveis. O registo de redes Wi-Fi conhecidas e de conexões Bluetooth pode fornecer informação útil sobre os locais frequentados pelo utilizador e as interações estabelecidas com outros dispositivos. Além disso, muitos smartphones estão sincronizados com serviços de nuvem, como Google Drive ou iCloud, o que significa que a preservação da prova não se pode limitar ao equipamento físico. Em muitos casos, será necessário recorrer a pedidos legais complementares dirigidos a fornecedores de serviços para obter acesso aos dados armazenados remotamente.

Outros Aspetos

As diretrizes da INTERPOL assumem especial importância por promoverem uma linguagem comum e uma metodologia partilhada entre diferentes países, facilitando a cooperação internacional entre autoridades policiais e aumentando a probabilidade de aceitação da prova digital em processos transnacionais. A sua utilidade é particularmente evidente em investigações que envolvem múltiplas jurisdições e exigem compatibilização de procedimentos operacionais.

Contudo, estas orientações não têm caráter vinculativo e devem ser sempre enquadradas nas exigências legais de cada ordenamento jurídico. Não substituem, por isso, normas técnicas nacionais ou regionais, como as do NIST nos Estados Unidos ou outras recomendações europeias, mas funcionam como referencial complementar particularmente útil em operações com dimensão internacional.

Em síntese, as diretrizes da INTERPOL representam um contributo relevante para a harmonização internacional da prática forense digital, sobretudo no que respeita à atuação dos primeiros intervenientes em operações de

busca e apreensão de dispositivos digitais. No caso dos dispositivos móveis, a sua importância é ainda maior, dada a centralidade destes equipamentos na vida quotidiana e o seu crescente valor enquanto fontes de evidência digital.

2.2.3. Normas ISO

A norma ISO/IEC 27037:2012, elaborada conjuntamente pela International Organization for Standardization (ISO) e pela International Electrotechnical Commission (IEC), centra-se na gestão da evidência digital e constitui um dos principais referenciais internacionais neste domínio. Publicada num contexto de crescente dependência das tecnologias da informação e de proliferação de incidentes com relevância probatória, esta norma estabelece orientações para a identificação, recolha, aquisição e preservação de evidência digital, com o objetivo de garantir a sua integridade, autenticidade e fiabilidade para utilização em processos judiciais ou disciplinares (International Organization for Standardization, 2012).

O seu âmbito de aplicação é amplo, abrangendo uma grande diversidade de dispositivos e suportes digitais, incluindo computadores pessoais, discos rígidos, dispositivos móveis, cartões de memória, sistemas de navegação, câmaras digitais, sistemas de videovigilância e infraestruturas de rede. A norma dirige-se quer aos primeiros intervenientes, quer aos peritos responsáveis pelo tratamento da evidência, impondo que o manuseamento dos vestígios digitais seja efetuado de forma sistemática, imparcial e conforme à legislação aplicável em cada jurisdição.

A ISO/IEC 27037:2012 assenta em três princípios gerais fundamentais: relevância, integridade e suficiência. A relevância reporta-se à capacidade da evidência para contribuir de forma significativa para provar ou refutar factos em investigação. A integridade exige que os dados correspondam efetivamente ao estado em que foram encontrados, o que implica a utilização de mecanismos de validação, como funções de verificação criptográfica. Por fim, a suficiência refere-se à necessidade de recolher dados em quantidade e qualidade bastantes para permitir uma análise completa e robusta. Estes princípios são ainda reforçados por exigências de auditabilidade, repetibilidade e reprodutibilidade, assegurando que os procedimentos adotados podem ser avaliados e, quando necessário, replicados por outros peritos de forma independente. A norma enfatiza igualmente a importância da justificação das decisões tomadas, exigindo que, cada ação ou método aplicado seja, tecnicamente fundamentado e defensável em sede judicial ou disciplinar.

A estrutura metodológica proposta pela norma organiza-se em quatro fases: identificação, recolha, aquisição e preservação. Estas fases estabelecem um encadeamento lógico destinado a assegurar o tratamento adequado da evidência desde o primeiro contacto com os suportes digitais até ao seu armazenamento seguro.

Fase 1: Identificação

A fase de identificação consiste na procura, reconhecimento e documentação dos dispositivos ou suportes suscetíveis de conter evidência digital. Esta etapa abrange tanto dados voláteis, como a informação presente em memória RAM ou em processos ativos, como dados não voláteis, armazenados em discos rígidos, cartões de memória ou outros suportes persistentes. O objetivo principal é reconhecer, de forma tão exaustiva quanto possível, todas as potenciais fontes de evidência e documentar o seu estado inicial, evitando omissões que possam comprometer a investigação posterior (International Organization for Standardization, 2012).

Fase 2: Recolha

A recolha corresponde à remoção física dos dispositivos e ao seu transporte para ambientes controlados, devendo ser efetuada de modo a preservar o estado original dos sistemas. Esta fase não se limita aos equipamentos principais, exigindo também atenção a elementos complementares que possam ser relevantes, como periféricos, suportes auxiliares, anotações manuscritas com credenciais de acesso ou outros objetos associados. A norma sublinha que a recolha deve ser planeada e executada com rigor, de forma a evitar alterações acidentais, perdas de informação ou contaminação da evidência.

Fase 3: Aquisição

A aquisição consiste na criação de cópias forenses da informação, preferencialmente por meio de imagens bit a bit dos suportes digitais. Estas cópias devem ser validadas por funções de verificação, assegurando que correspondem fielmente ao conteúdo original. A norma destaca a necessidade de documentar detalhadamente esta fase, incluindo as ferramentas utilizadas, as versões de software, as condições técnicas do procedimento e quaisquer limitações ou alterações inevitáveis, como a existência de setores defeituosos ou a impossibilidade de desligar determinados sistemas críticos. Esta exigência de documentação reforça a transparência do procedimento e a credibilidade dos resultados obtidos (International Organization for Standardization, 2012).

Fase 4: Preservação

A fase de preservação visa proteger a evidência digital contra alteração, degradação ou destruição. Para tal, a norma recomenda o armazenamento seguro em instalações adequadas, bem como a utilização de embalagens antiestáticas, etiquetas invioláveis e condições ambientais controladas, nomeadamente quanto à temperatura, humidade, campos magnéticos e exposição à luz. A preservação não deve ser entendida apenas como armazenamento físico, mas como um conjunto de medidas destinadas a manter a integridade da evidência ao longo de todo o seu ciclo de vida, desde a recolha até à eventual apresentação em tribunal.

Outros Aspetos

A norma atribui especial relevância à cadeia de custódia, entendida como o registo cronológico de todos os movimentos, acessos e intervenções sobre a evidência desde a sua recolha até ao termo do seu ciclo de vida. Este registo é essencial para demonstrar que a prova permaneceu íntegra, devidamente controlada e acessível apenas a pessoas autorizadas. A correta manutenção da cadeia de custódia constitui, assim, uma condição decisiva para a admissibilidade e credibilidade da prova digital.

Em síntese, a ISO/IEC 27037:2012 oferece um enquadramento metodológico robusto para a gestão de evidência digital, permitindo uniformizar procedimentos a nível internacional e facilitar a cooperação transfronteiriça em matéria de cibercrime. Embora não substitua a legislação nacional, funciona como um guia de boas práticas que reforça a confiança no processo de investigação digital e no valor probatório dos vestígios recolhidos. Para além disso, influencia diretamente a formação dos profissionais, ao estabelecer requisitos de competência e ao ajudar a padronizar funções como a do primeiro interveniente forense, do especialista em aquisição, do analista de evidência e do responsável pela validação de métodos.

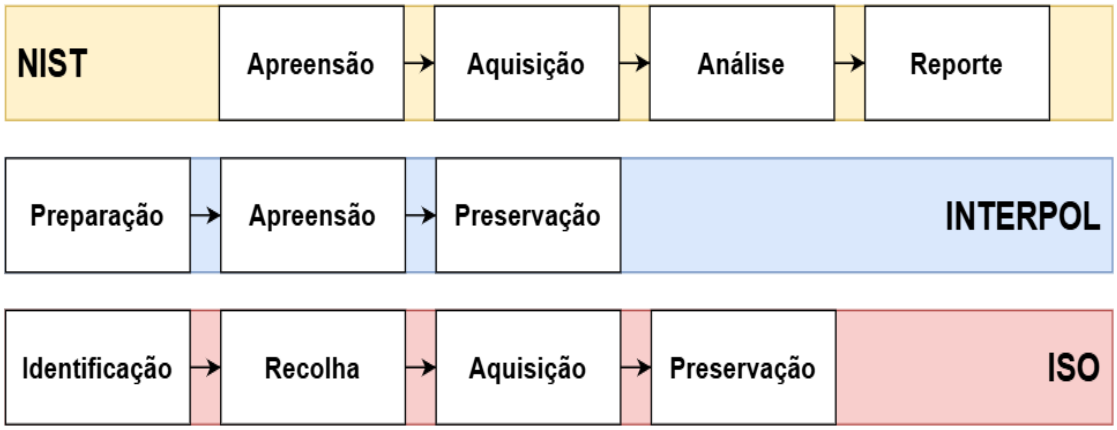
A diversidade de abordagens presentes nestes referenciais internacionais justifica uma análise comparativa das respetivas metodologias, de modo a identificar convergências, diferenças e contributos relevantes para a definição de um procedimento estruturado de análise forense digital. Essa comparação é apresentada na secção seguinte.

2.3. Análise Comparativa

A comparação entre os diferentes referenciais internacionais permite identificar semelhanças metodológicas e diferenças estruturais relevantes para a definição de procedimentos forenses consistentes.

A análise comparativa (ver Figura 2) entre a ISO/IEC 27037:2012, o guia da INTERPOL e a NIST SP 800-101 Revision 1 evidencia diferenças na forma como cada referencial estrutura o processo de análise forense digital, mas também revela pontos de convergência que demonstram a sua complementaridade. A figura mencionada no texto original apresenta, sob a forma de diagrama, a correspondência entre as fases definidas nos três modelos, permitindo visualizar as semelhanças e diferenças na organização metodológica.

Figura 2: Procedimento geral proposto na NIST SP 800-101.



A NIST SP 800-101 Revision 1 adota um ciclo estruturado em quatro fases - apreensão, aquisição, análise e reporte - aproximando-se do modelo clássico da ciência forense. Este referencial distingue-se por incluir explicitamente as fases de análise e de elaboração do relatório, que assumem particular relevância em contexto judicial, uma vez que é nelas que se produzem os relatórios periciais utilizados em sede de julgamento. A inclusão destas etapas evidencia a preocupação do NIST não apenas com a recolha e preservação da evidência, mas também com a sua interpretação técnica e com a sua apresentação formal perante as autoridades judiciais (Ayers et al., 2014).

O guia da INTERPOL segue uma abordagem mais operacional, orientada sobretudo para a atuação de agentes policiais e primeiros intervenientes. A sua estrutura organiza-se em três fases principais: preparação, apreensão e preservação. Ao contrário do modelo do NIST, não inclui fases autónomas de análise e reporte, concentrando-se nos momentos iniciais da intervenção, isto é, na preparação da operação, na recolha dos dispositivos e na manutenção da cadeia de custódia. Esta opção reflete o objetivo do documento, que é fornecer orientações práticas para o trabalho de campo, garantindo que a evidência digital é recolhida e preservada de forma segura e juridicamente válida (INTERPOL Innovation Centre, 2021).

A ISO/IEC 27037:2012 apresenta uma estrutura metodológica próxima da adotada pela INTERPOL, embora com maior formalização técnica. O processo é dividido em quatro fases: identificação, recolha, aquisição e preservação. Tal como sucede com o guia da INTERPOL, este referencial não inclui fases específicas de análise e reporte, centrando-se na gestão correta da evidência até ao momento em que esta se encontra pronta para ser examinada. A norma tem como principal objetivo assegurar que a evidência digital é identificada, recolhida e preservada de forma adequada, permitindo que etapas posteriores, eventualmente definidas por outros referenciais ou pela legislação nacional, possam ser realizadas sem comprometer a sua integridade (International Organization for Standardization, 2012).

Apesar das diferenças de estrutura, nível de detalhe técnico e público-alvo, os três referenciais partilham um conjunto de princípios fundamentais que constituem a base da prática da análise forense digital. Em primeiro lugar, todos atribuem prioridade absoluta à integridade da evidência digital, reconhecendo que qualquer alteração introduzida durante o processo pode comprometer a sua validade e admissibilidade em tribunal. A preservação do estado original dos dados é, por isso, um requisito comum a todos os modelos.

Outro ponto de convergência é a exigência de uma cadeia de custódia rigorosa. As três normas insistem na necessidade de manter um registo cronológico completo de todas as intervenções realizadas sobre os dispositivos e dados, incluindo a identificação dos intervenientes, as operações efetuadas e as condições em que a evidência foi armazenada ou transferida. Este registo garante a rastreabilidade da prova e permite demonstrar, em sede judicial, que esta não foi adulterada.

Também é comum aos três referenciais a ênfase na documentação detalhada dos procedimentos. Desde a apreensão inicial até às fases posteriores do processo, todas as ações devem ser registadas de forma clara e completa, assegurando transparência, auditabilidade e possibilidade de repetição por outros peritos. Esta exigência está diretamente ligada ao princípio da reprodutibilidade, considerado essencial para a credibilidade da prova digital.

Outro elemento partilhado é a necessidade de que os profissionais envolvidos possuam competência técnica adequada. Tanto o NIST como a INTERPOL e a ISO sublinham que a manipulação de evidência digital deve ser realizada por pessoas qualificadas, capazes de aplicar métodos reconhecidos e de justificar tecnicamente as decisões tomadas durante o processo.

Por fim, todos os referenciais afirmam que a análise forense digital deve respeitar a legislação aplicável na jurisdição onde decorre a investigação. As normas técnicas não substituem o direito processual ou penal, mas funcionam como orientações complementares destinadas a garantir que a recolha e tratamento da prova ocorrem de forma compatível com as exigências legais.

Em síntese, a comparação entre a NIST SP 800-101, o guia da INTERPOL e a ISO/IEC 27037:2012 demonstra que, apesar das diferenças de abordagem, os três referenciais são complementares. A INTERPOL privilegia a atuação inicial no terreno, a ISO fornece um enquadramento metodológico para a gestão da evidência e o NIST apresenta um ciclo completo que inclui análise e reporte. Em conjunto, estes modelos contribuem para a uniformização internacional da prática forense digital e reforçam a fiabilidade e admissibilidade da prova em contexto judicial.

2.4. Desafios Técnicos e Éticos

A análise forense digital de dispositivos móveis compreende o conjunto de procedimentos técnicos e metodológicos destinados à identificação, recolha, preservação, extração, análise e apresentação de dados armazenados ou processados por equipamentos portáteis, como smartphones, tablets e outros dispositivos com capacidades de comunicação e processamento. A evolução tecnológica destes equipamentos, bem como a crescente integração com serviços em nuvem, tem aumentado significativamente a complexidade das investigações forenses, exigindo métodos cada vez mais especializados para garantir a preservação da evidência e a sua validade probatória (Casey, 2011; Arnes, 2018).

Os sistemas operativos móveis dominantes, Android e iOS, apresentam arquiteturas distintas, mecanismos de segurança próprios e diferentes formatos de armazenamento de dados. Esta diversidade obriga à seleção criteriosa dos métodos de aquisição, tendo em conta o modelo do dispositivo, a versão do sistema operativo e as configurações de segurança existentes. Para além destes sistemas, podem também ser alvo de análise forense outros equipamentos, como telemóveis convencionais, dispositivos portáteis de Internet das Coisas, relógios inteligentes ou terminais especializados, como equipamentos de pagamento móvel, que igualmente podem conter informação relevante para a investigação (Casey, 2001).

No caso de dispositivos Android, o processo de arranque ocorre em várias fases, desde o carregamento inicial do firmware até à execução do sistema operativo e dos serviços de utilizador. A obtenção de dados pode ser realizada por aquisição lógica, que extrai apenas informação acessível ao sistema operativo, ou por aquisição física, que consiste na cópia integral da memória interna. A aquisição física é preferível quando se pretende recuperar dados eliminados ou aceder a partições não visíveis ao sistema, mas pode exigir técnicas avançadas e equipamento especializado. Ferramentas forenses comerciais amplamente utilizadas permitem suportar centenas de modelos de dispositivos, oferecendo funcionalidades de desbloqueio, extração e descodificação de dados (Arnes, 2018).

Nos dispositivos Apple, que utilizam o sistema iOS, o processo de arranque inclui uma cadeia de arranque segura, na qual cada etapa é validada criptograficamente antes de ser executada. Este mecanismo dificulta a extração forense direta, obrigando frequentemente ao recurso a métodos alternativos, como a análise de cópias de segurança, acesso a serviços de sincronização remota ou exploração de vulnerabilidades conhecidas. Em

determinados casos, modos especiais de arranque podem permitir acesso ao sistema de ficheiros, embora sujeitos a limitações impostas por mecanismos de encriptação integral do armazenamento interno (Casey, 2011).

Os dados de interesse forense em dispositivos móveis são numerosos e diversificados. Entre os mais comuns encontram-se registos de chamadas, mensagens SMS e MMS, mensagens de aplicações de comunicação, histórico de navegação, dados de localização, fotografias e vídeos, credenciais de acesso, ficheiros de aplicações e artefactos do sistema operativo. Grande parte desta informação é armazenada em bases de dados internas, frequentemente em formato SQLite, que podem conter dados eliminados ainda não sobrescritos. A análise destes registos exige ferramentas capazes de interpretar estruturas de dados específicas de cada sistema e de cada aplicação (Casey, 2001).

A sincronização com serviços de armazenamento remoto introduz novas fontes de evidência, mas também desafios adicionais. Muitos dispositivos mantêm cópias automáticas de dados em serviços de nuvem, o que significa que informação relevante pode não estar presente no equipamento físico. O acesso a estes dados pode exigir credenciais válidas, autorização judicial ou cooperação internacional com os fornecedores de serviços, o que aumenta a complexidade do processo forense (Arnes, 2018).

A encriptação constitui atualmente um dos maiores obstáculos à análise forense de dispositivos móveis. Em versões recentes do Android, a encriptação do armazenamento é frequentemente ativada por defeito, exigindo a chave do utilizador para acesso aos dados. Nos dispositivos Apple, a proteção de dados associa as chaves criptográficas ao hardware e ao código de desbloqueio, dificultando significativamente a extração de informação. Nestes casos, a análise pode limitar-se a dados disponíveis em cópias de segurança ou a informação obtida antes do desligar do dispositivo, quando ainda se encontra em memória volátil (Casey, 2011).

Para além da encriptação, existem técnicas de anti-forense que visam dificultar a investigação. Entre estas incluem-se aplicações concebidas para apagar automaticamente dados sensíveis, utilização de áreas seguras protegidas, sistemas operativos modificados ou mecanismos destinados a impedir a aquisição de dados. A deteção destas alterações exige análise da integridade do sistema, verificação de valores de hash e comparação com imagens de referência conhecidas, de modo a confirmar que o dispositivo não foi alterado de forma a ocultar informação (Casey, 2001).

O desenvolvimento da Internet das Coisas introduziu novas fontes de evidência associadas aos dispositivos móveis. Relógios inteligentes, pulseiras de atividade, veículos conectados, equipamentos médicos e sistemas domésticos inteligentes podem armazenar dados sobre localização, atividade física, comunicações ou interações do utilizador. A análise destes dispositivos exige conhecimento específico dos protocolos utilizados e dos formatos de dados, muitas vezes proprietários, bem como ferramentas adaptadas à sua extração (Arnes, 2018).

A volatilidade dos dados e a rápida evolução tecnológica tornam indispensável a atualização constante das ferramentas e das técnicas utilizadas na análise forense digital. A formação contínua dos peritos, aliada à adoção de procedimentos normalizados, é essencial para garantir consistência, reprodutibilidade e fiabilidade dos resultados obtidos. A aplicação de normas internacionais contribui para uniformizar práticas e reforçar a credibilidade da prova digital em contexto judicial (International Organization for Standardization, 2012).

Em síntese, a análise forense de dispositivos móveis exige a aplicação de métodos técnicos adequados a cada plataforma, respeitando princípios de preservação, documentação e validação da evidência. Este tipo de investigação envolve desafios técnicos e éticos significativos, resultantes do carácter intrusivo das técnicas utilizadas, do volume de informação recolhida e da possibilidade de aceder a dados pessoais sensíveis. A crescente complexidade dos dispositivos e a sua integração em redes e serviços remotos reforçam a necessidade de assegurar que todas as operações respeitam os princípios de legalidade, proporcionalidade e proteção da privacidade (Casey, 2011; Arnes, 2018).

3. Discussão sobre o Atual Enquadramento e suas Lacunas

A comparação entre os diferentes referenciais internacionais permite identificar semelhanças metodológicas e diferenças estruturais relevantes para o desenvolvimento de procedimentos forenses

A metodologia adotada iniciou-se com a identificação e análise da legislação aplicável à análise forense digital no enquadramento jurídico nacional e europeu. Esta fase teve como objetivo determinar se existia, no ordenamento jurídico vigente, um procedimento formalmente definido para a recolha, preservação e análise de prova digital, em particular no contexto de dispositivos móveis. Após a análise dos diplomas legais relevantes, verificou-se que, embora exista regulamentação sobre obtenção de prova, proteção de dados e investigação criminal, não se encontra definido um procedimento técnico-operacional específico para a realização de análise forense digital, quer na legislação nacional, quer na legislação europeia.

Face a esta lacuna normativa, o estudo foi alargado à análise de orientações, diretrizes e normas técnicas produzidas por entidades internacionais reconhecidas, com o objetivo de identificar modelos de referência que pudessem contribuir para a normalização de procedimentos de investigação forense digital. Nesta fase foram analisados documentos técnicos amplamente utilizados na comunidade forense, nomeadamente a NIST SP 800-101, as diretrizes da INTERPOL para primeiros intervenientes e a norma ISO/IEC 27037, por constituírem referenciais internacionais relevantes na definição de boas práticas para a gestão de evidência digital.

A análise destes documentos permitiu verificar que, embora todos apresentem orientações estruturadas, cada um deles possui um âmbito e objetivos distintos. A NIST SP 800-101 apresenta um modelo completo que inclui apreensão, aquisição, análise e reporte, enquanto as diretrizes da INTERPOL se concentram sobretudo nas fases iniciais da intervenção, com especial enfoque na preparação e apreensão. Por sua vez, a ISO/IEC 27037 define um enquadramento metodológico para identificação, recolha, aquisição e preservação da evidência, privilegiando a gestão adequada dos vestígios digitais antes da fase de análise.

A comparação entre estes referenciais evidenciou que, apesar de partilharem princípios comuns, nenhum deles cobre de forma integral todas as etapas necessárias à realização de uma análise forense digital de dispositivos móveis no contexto jurídico considerado. Esta constatação justificou a necessidade de propor um procedimento próprio, que integre os contributos das normas analisadas e que seja compatível com as exigências legais aplicáveis.

Assim, com base na análise da legislação e na comparação das normas internacionais, foi elaborado o procedimento de análise forense digital apresentado na secção seguinte, procurando estabelecer uma metodologia estruturada, tecnicamente fundamentada e juridicamente conforme, aplicável à investigação forense em dispositivos móveis.

Assim, a inexistência de um procedimento claramente definido para a análise forense de dispositivos móveis justifica o desenvolvimento de um modelo estruturado que integre boas práticas internacionais e respeite o enquadramento jurídico aplicável.

4. Proposta de Procedimento para Análise Forense Digital a Dispositivos Móveis

Com base na análise da legislação aplicável e na comparação das normas internacionais anteriormente discutidas, foi desenvolvido um procedimento estruturado para a análise forense digital de dispositivos móveis. O modelo proposto integra contributos das orientações do NIST, das diretrizes da INTERPOL e da norma ISO/IEC 27037, procurando adaptar estas boas práticas ao contexto jurídico português.

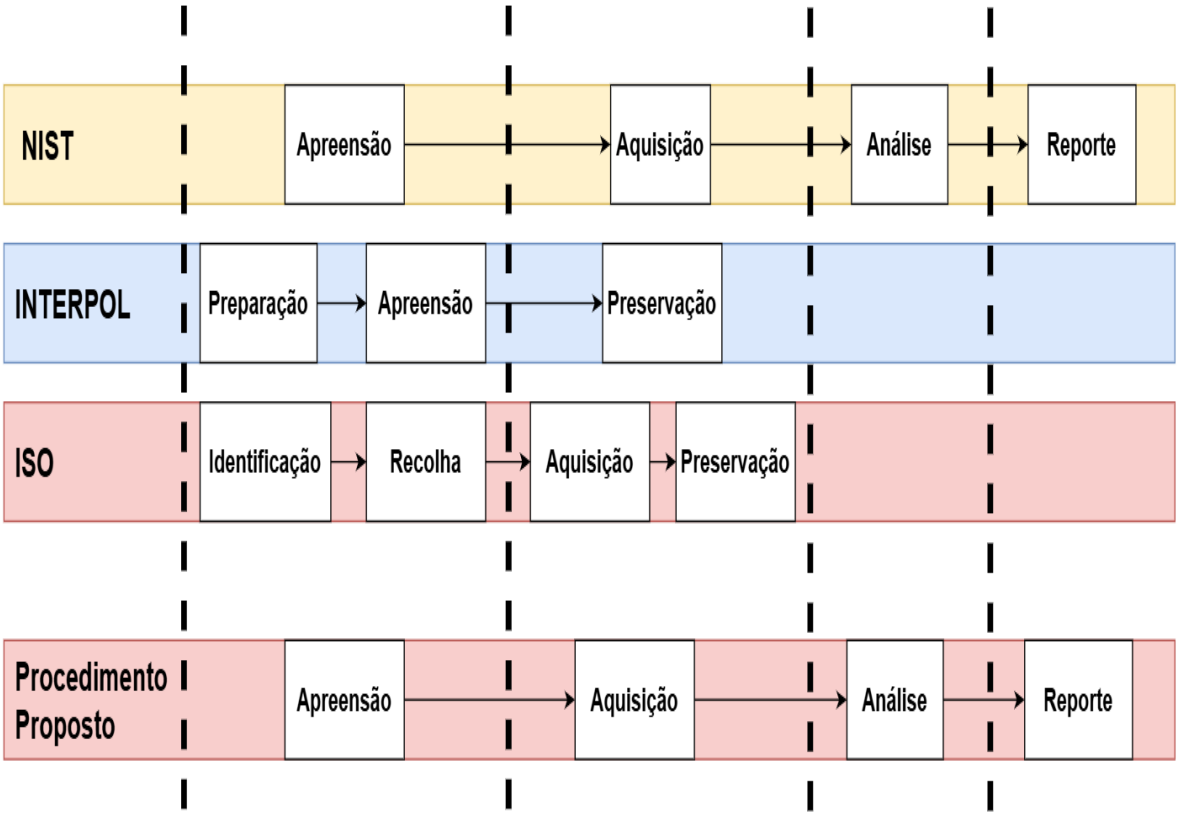
A definição de um procedimento estruturado e metodologicamente consistente revela-se fundamental para uniformizar a atuação dos diferentes intervenientes na análise forense digital. Em Portugal, embora os principais atores em processos de investigação criminal digital sejam habitualmente magistrados do Ministério Público e inspetores da Polícia Judiciária, podem igualmente intervir outros profissionais. Entre estes incluem-se peritos contratados por sociedades de advogados, especialistas ao serviço de empresas ou entidades lesadas, bem como

peritos que atuem no âmbito de protocolos com a Procuradoria-Geral da República. Neste contexto, a existência de um procedimento formalmente definido e devidamente documentado assume utilidade prática e relevância jurídica, contribuindo para maior consistência, transparência e credibilidade das investigações.

O procedimento aqui proposto resulta da integração de três referenciais de reconhecida autoridade internacional: a abrangência metodológica das orientações do NIST, a robustez normativa da ISO/IEC 27037:2012 e as boas práticas operacionais promovidas pela INTERPOL. A Figura 3 apresenta a correspondência entre o procedimento proposto e as fases previstas nas normas anteriormente analisadas.

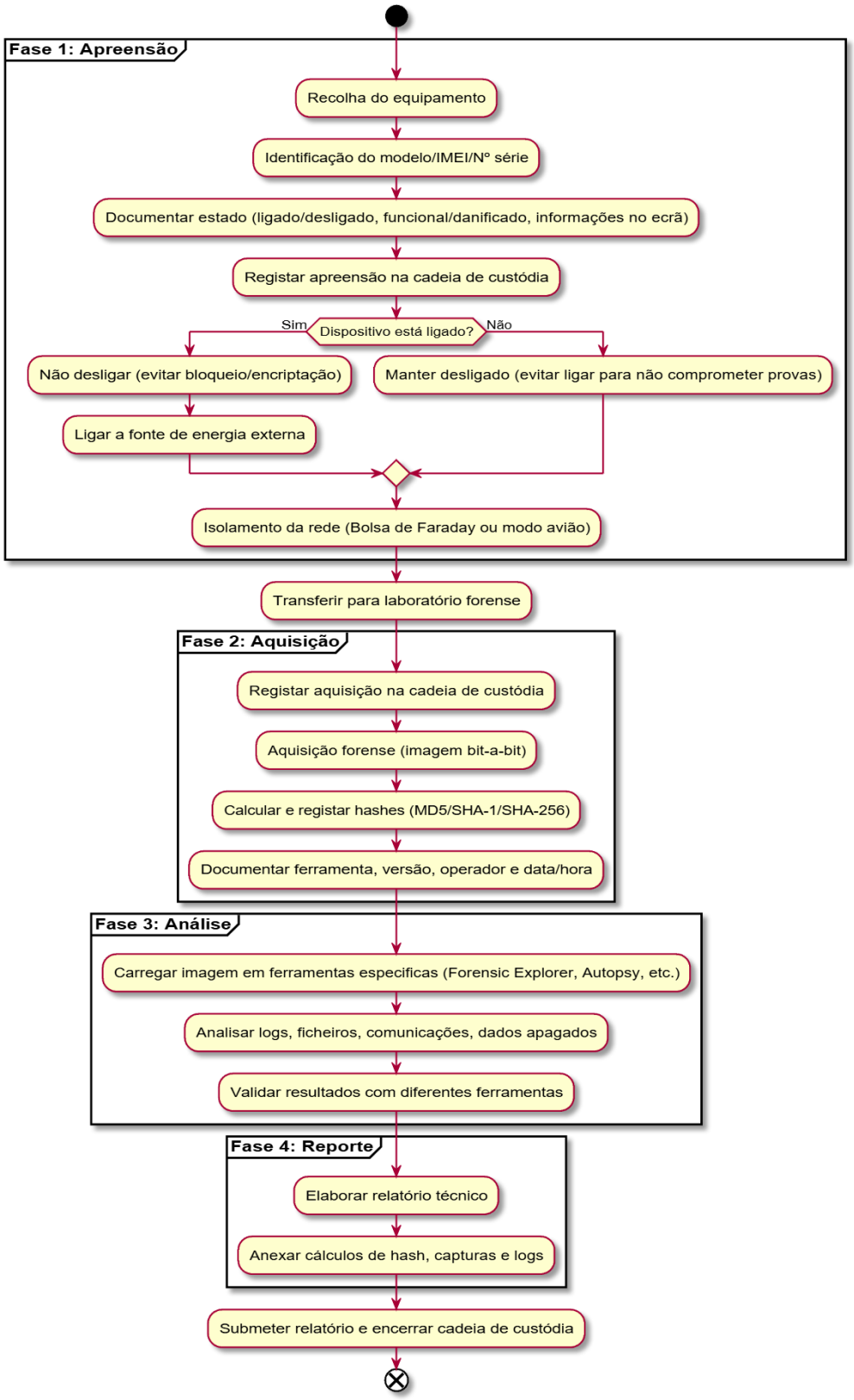
Da observação do diagrama verifica-se que apenas o modelo do NIST e o procedimento agora proposto incluem explicitamente as fases de análise e de reporte. Estas fases assumem particular relevância, pois é na análise que se avaliam as evidências e se formulam hipóteses sobre os factos investigados, e é no reporte que se elaboram os relatórios periciais que serão apreciados por magistrados e tribunais. As fases de apreensão e de aquisição são comuns a todos os referenciais, embora alguns atribuam maior importância à preparação da apreensão, como sucede nas orientações da INTERPOL, enquanto outros enfatizam a identificação dos dispositivos, como acontece na norma ISO.

Figura 3: Procedimento geral proposto na NIST SP 800-101.



O diagrama apresentado na Figura 4 organiza, de forma sequencial, as atividades associadas a cada fase, garantindo rastreabilidade, replicabilidade e rigor técnico. O procedimento estrutura-se em quatro fases principais: apreensão, aquisição, análise e reporte.

Figura 4: Procedimento proposto.



Fase 1: Apreensão

A primeira fase corresponde à apreensão do dispositivo, momento inicial em que o equipamento é retirado do seu contexto original e colocado sob custódia da autoridade investigadora. De acordo com a ISO/IEC 27037:2012, é indispensável proceder à correta identificação do equipamento, registando elementos como o fabricante, o modelo, o número de série e, no caso de dispositivos móveis, o código IMEI. Estes identificadores permitem estabelecer uma ligação inequívoca entre o dispositivo apreendido e o processo em investigação.

Em conformidade com as orientações da INTERPOL, o dispositivo deve ser imediatamente isolado de qualquer rede de comunicação, de modo a impedir manipulações remotas ou sincronizações automáticas que possam comprometer a integridade dos dados. Este isolamento pode ser realizado através da utilização de bolsas de Faraday ou pela ativação do modo de voo, sempre que tecnicamente possível.

Nesta fase deve ainda ser documentado o estado do equipamento, registando se se encontra ligado ou desligado, bloqueado ou desbloqueado, e se apresenta danos físicos. Recomenda-se a realização de registos fotográficos, complementados por notas descritivas, de forma a reforçar a credibilidade da cadeia probatória. A apreensão deve terminar com o registo formal na cadeia de custódia, mecanismo que assegura a rastreabilidade da prova desde a recolha até à sua eventual apresentação em tribunal.

O estado operacional do dispositivo condiciona os procedimentos seguintes. Se o equipamento se encontrar ligado, a ISO/IEC 27037 recomenda que não seja desligado, pois tal pode desencadear bloqueios ou encriptação automática. Nestas situações, em conformidade com o NIST, devem ser registadas as informações visíveis no ecrã, preferencialmente através de notas e fotografias. Se o dispositivo estiver desligado, deve manter-se nessa condição, uma vez que a sua inicialização pode alterar o sistema de ficheiros ou sobrescrever dados voláteis.

Quando o dispositivo se encontra protegido por palavra-passe ou outro mecanismo de segurança, podem ser utilizadas ferramentas forenses específicas que permitam o desbloqueio sem comprometer a integridade da evidência. Todas as ferramentas utilizadas, bem como as respetivas versões, devem ser registadas para posterior inclusão no relatório pericial.

Fase 2: Aquisição

A fase de aquisição inicia-se após o transporte seguro do dispositivo para o laboratório forense. Segundo a ISO/IEC 27037:2012, o objetivo principal desta fase é a criação de uma imagem forense, isto é, uma cópia bit a bit de todo o conteúdo do equipamento apreendido. Esta cópia inclui ficheiros ativos, dados eliminados e espaço não alocado, distinguindo-se de uma simples cópia de ficheiros por preservar integralmente o conteúdo do suporte.

Para garantir a autenticidade da imagem obtida, tanto a ISO/IEC 27037 como a NIST SP 800-101 recomendam o cálculo de resumos criptográficos antes e após a aquisição. Estes valores funcionam como assinaturas digitais que permitem verificar que a evidência não sofreu alterações. Funções antigas como MD5 ou SHA-1 deixaram de ser consideradas seguras, devendo ser utilizadas funções mais robustas, como SHA-256 ou SHA-512 (Xie, Feng, & Lai, 2013; Stevens et al., 2017).

As orientações da INTERPOL reforçam ainda a necessidade de documentar detalhadamente todo o processo, incluindo as ferramentas utilizadas, as configurações aplicadas e as condições técnicas da aquisição, de modo a permitir a verificação posterior por outros peritos.

Fase 3: Análise

Concluída a aquisição, inicia-se a fase de análise, que deve ser realizada exclusivamente sobre a cópia forense e nunca sobre o dispositivo original, conforme indicado na ISO/IEC 27037:2012. Nesta etapa, a imagem obtida é examinada através de ferramentas especializadas capazes de identificar e interpretar dados relevantes, como

registos de sistema, ficheiros eliminados, histórico de comunicações, dados de navegação, informação de geolocalização e metadados.

Entre as ferramentas frequentemente utilizadas encontram-se aplicações forenses comerciais e de código aberto, que permitem analisar diferentes formatos de dados e integrar resultados provenientes de várias fontes. A utilização de múltiplas ferramentas é recomendada pelo NIST, que enfatiza a importância da validação cruzada para reduzir a probabilidade de erro e aumentar a fiabilidade das conclusões (Ayers et al., 2014).

As orientações da INTERPOL sublinham igualmente que a análise deve ser objetiva, reprodutível e passível de auditoria externa. Por essa razão, todas as operações realizadas devem ser documentadas de forma detalhada, garantindo que o processo pode ser revisto e validado por terceiros.

Fase 4: Reporte

A última fase corresponde ao reporte, em que os resultados da investigação são consolidados num relatório técnico-científico. De acordo com a ISO/IEC 27037:2012, este relatório deve incluir a descrição detalhada dos procedimentos executados, a fundamentação das opções metodológicas, os resultados obtidos e as limitações encontradas durante a análise.

O relatório deve ser redigido de forma clara e compreensível, permitindo a sua leitura não apenas por peritos, mas também por magistrados, advogados e outros intervenientes processuais. Devem ser incluídos elementos de suporte, como valores de hash, capturas de ecrã, registos de operações e cronologias, de modo a demonstrar a integridade e autenticidade da evidência.

Recomenda-se igualmente que sejam indicadas as ferramentas utilizadas, incluindo versões e certificações, reforçando a credibilidade do trabalho realizado. O procedimento conclui-se com a formalização completa da cadeia de custódia, assegurando que toda a prova recolhida pode ser apresentada em tribunal de forma admissível, tecnicamente fundamentada e conforme os padrões internacionais de qualidade e legalidade.

6. Conclusão

O presente trabalho teve como objetivo propor um procedimento estruturado e adaptado à realidade portuguesa para a análise forense digital de dispositivos móveis. A partir da revisão da legislação nacional e europeia aplicável, bem como da análise de normas e orientações internacionais relevantes, nomeadamente a ISO/IEC 27037, as diretrizes da INTERPOL e o guia NIST SP 800-101, foi possível verificar a inexistência de um modelo padronizado especificamente aplicável ao contexto português. Esta lacuna pode originar inconsistências na recolha, preservação e análise da prova digital, com potenciais consequências na sua admissibilidade em tribunal.

Com base nesta constatação, foi desenvolvido um procedimento forense estruturado em quatro fases — apreensão, aquisição, análise e reporte — concebido de forma a articular as boas práticas internacionais com o enquadramento jurídico português e europeu. O procedimento proposto foi definido tendo em consideração, em particular, as exigências da Lei do Cibercrime, do Código de Processo Penal e do Regulamento Geral sobre a Proteção de Dados, assegurando que as operações técnicas realizadas no âmbito da análise forense digital respeitam os princípios de legalidade, proporcionalidade, integridade e proteção da privacidade.

A principal mais-valia do trabalho reside na conjugação entre a análise teórica, jurídica e normativa e a definição de um procedimento técnico aplicável à prática forense, permitindo aproximar as recomendações internacionais das necessidades específicas do ordenamento jurídico português. Este contributo pretende servir de referência para magistrados, órgãos de polícia criminal e peritos envolvidos em investigações que incluam evidência digital proveniente de dispositivos móveis, promovendo maior uniformidade de atuação e maior segurança jurídica na utilização da prova digital.

Numa perspetiva de trabalho futuro, considera-se relevante aprofundar e validar o procedimento proposto através da sua aplicação em contextos reais de investigação, permitindo avaliar a sua eficácia e identificar eventuais melhorias. Poderá igualmente ser explorada a integração do procedimento com sistemas de gestão de prova digital, de forma a automatizar o registo das operações e reforçar os mecanismos de controlo e rastreabilidade.

Adicionalmente, a utilização de tecnologias baseadas em blockchain constitui uma linha de desenvolvimento promissora, na medida em que pode contribuir para reforçar a imutabilidade, a transparência e a fiabilidade da cadeia de custódia. A aplicação destas soluções poderá aumentar o grau de confiança na prova digital apresentada em tribunal e favorecer a harmonização de procedimentos em investigações que envolvam múltiplas entidades ou diferentes jurisdições.

Referências

Arnes, A. (2018). *Digital forensics*. Wiley.

Assembleia da República (Portugal). (2009). *Lei n.º 109/2009, de 15 de setembro: Aprova a Lei do Cibercrime*. *Diário da República, Série I*(180).

Casey, E. (2001). *Handbook of computer crime investigation: Forensic tools and technology*. Academic Press.

Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers, and the internet* (3.ª ed.). Academic Press.

Cohen, F. (2012). Digital forensics. In H. Tipton & M. Krause (Eds.), *Information security management handbook* (6.ª ed.). Auerbach Publications. https://doi.org/10.1201/b11819-107

Conselho da União Europeia. (2001). *Convenção sobre o cibercrime (Budapeste, 23 de novembro de 2001)*. *Jornal Oficial da União Europeia*.

Council of Europe. (2001). *Convention on Cybercrime (ETS No. 185)*.

Cruz-Cunha, M. M., & Mateus-Coelho, N. R. (2020). *Handbook of research on cyber crime and information privacy*. IGI Global.

Diário da República. (2023). *Código Penal português (com as alterações até 2023)*.

European Union. (2016, April 27). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation)*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

Gilliland, A. J. (2016). Setting the stage. In M. Baca (Ed.), *Introduction to metadata*. Getty Research Institute. https://www.getty.edu/publications/intrometadata/setting-the-stage/

International Organization for Standardization. (2012). *ISO/IEC 27037:2012 – Guidelines for identification, collection, acquisition and preservation of digital evidence*.

International Organization for Standardization. (2017). *ISO 23081-1:2017 – Information and documentation – Records management processes – Metadata for records – Part 1: Principles*.

Kiran, S., Sanjana, J., & Reddy, N. J. (2019, March). Mobile phone addiction: Symptoms, impacts and causes—A review. In *International Conference on Trends in Industrial Value Engineering and Business and Social Innovation (ICTIVBSI)* (pp. 81–86).

Kist, D. J. (2019). *Prova digital no processo penal*. JH Mizuno.

Lei n.º 32/2008, de 17 de julho. (2008). *Diário da República*.

Limberger, T., Santanna, G. da S., & Giannakos, D. B. da S. (2023). Internet das coisas (IoT) e os direitos à privacidade e à proteção de dados do cidadão. *Revista Brasileira de Políticas Públicas*. https://doi.org/10.5102/rbpp.v13i3.8536

National Institute of Justice. (2008). *Electronic crime scene investigation: A guide for first responders* (2.ª ed.). U.S. Department of Justice.

National Institute of Standards and Technology. (2006). *Guide to integrating forensic techniques into incident response (Special Publication 800-86)*.

Portugal. (2019). *Lei n.º 58/2019, de 8 de agosto: Assegura a execução do RGPD na ordem jurídica nacional*. https://dre.pt/dre/detalhe/lei/58-2019-123815466

Queirós Colaço, M. F. dos S. (2023). *Buscas informáticas e subsequente apreensão de dados informáticos como métodos de obtenção de prova digital em processo penal* [Dissertação de mestrado, Universidade Católica Portuguesa].

Ramalho, D. S. (2013). The use of malware as a means of obtaining evidence in criminal proceedings. *Journal of Competition and Regulation, 4*(16), 195–243.

Ramos, A. D. (2014). *A prova digital em processo penal: O correio eletrónico* (2.ª ed.). Chiado Books.

República Portuguesa. (1987, fevereiro 17). *Código de processo penal (Decreto-Lei n.º 78/87)*. https://diariodarepublica.pt/dr/legislacao-consolidada/decreto-lei/1987-34570075

Santos, L. F. C. (2024). *Dynamic analysis techniques for Android applications* [Dissertação de mestrado, Polytechnic Institute of Leiria]. https://iconline.ipleiria.pt/bitstream/10400.8/9768/1/Te%CC%81cnicas%20de%20ana%CC%81lise%20dina%CC%82mica%20a%20aplicac%CC%A7o%CC%83es%20Android_cf.pdf

Stevens, M., Bursztein, E., Karpman, P., Albertini, A., & Markov, Y. (2017). The first collision for full SHA-1. In *Advances in Cryptology – CRYPTO 2017*.

Venâncio, P. D. (2020). Regime geral dos atos eletrónicos – Um regime esquecido. *Revista Electrónica de Direito*.

Venâncio, P. D. (2023). *Lei do cibercrime: Anotada e comentada*. Editora D'Ideias.

Xie, T., Feng, D., & Lai, X. (2013). Fast collision attack on MD5. *Journal of Cryptographic Engineering*.

Xu, X. (2019). *Impacts of mobile usage and experience in contemporary society*. IGI Global.

Declaração Ética

Conflito de Interesse: Nada a declarar. **Financiamento:** Nada a declarar. **Revisão por Pares:** Dupla-cega.

Sextortion ou *Cibersextortion*; delimitação do termo

Sextortion or Cybersextortion; delimitation of the term

10.29073/j2.v8i1.1118

Recebido: 04 de março de 2026.
Aprovado: 01 de abril 2026.
Publicado: 04 de abril de 2026.

Autor/a: Paulo Lourenço, ESTG-IPP, Portugal, paulo.enes.lourenco@hotmail.com.

Resumo

Em Direito, e em Direito Penal em particular, os termos, designações e conceitos devem ser de tal forma específicos que só por si já sejam capazes de afastar interpretações dúbias. Desta forma este artigo tem como objetivo refletir sobre a utilização do termo *Cibersextortion* em detrimento do termo *Sextortion* de forma a tornar mais clara a utilização de cada um deles na identificação do fenómeno que se pretenda analisar.

Palavras-Chave: Cibercrime; *Cibersextortion*; Crime; *Sextortion*.

Abstract

In Law, and in Criminal Law in particular, terms, designations, and concepts must be so specific that they alone are capable of avoiding ambiguous interpretations. Therefore, this article aims to reflect on the use of the term Cybersextortion instead of Sextortion in order to clarify the use of each in identifying the phenomenon being analyzed.

Keywords: Crime; Cybercrime; Cybersextortion; Sextortion.

1. Introdução

Os termos utilizados para os crimes praticados com recurso a tecnologias de informação e comunicação (TIC) ou sobre estas, são precedidos do prefixo "*Ciber*". Logo à partida o termo cibercrime deriva da palavra crime, mas, por ser praticado no ciberespaço ou por meio das TIC, ganhou o prefixo "*Ciber*". Por isto, toda a doutrina diz que é cibercrime o crime praticado através das TIC ou contra estas. No entanto, todas as condutas criminais praticadas sem recurso às TIC, são designadas como crime, sem o prefixo "*Ciber*".

Desta forma o vocábulo "*Cibersextortion*", faz mais sentido do que "*Sextortion*", uma vez que, à letra, esta última se refere apenas à extorsão sexual. Podendo ser praticada sem recurso às TIC e, dessa forma, induzir o leitor em erro. Já o termo *Cibersextortion*, não deixa margem para dúvidas. O prefixo "*Ciber*" coloca imediatamente esta prática no ciberespaço.

2. Metodologia

O presente estudo adota uma abordagem qualitativa, de natureza jurídico-dogmática, assente na análise crítica da doutrina nacional e internacional relevantes, bem como do enquadramento normativo aplicável ao fenómeno em estudo. Recorre-se, adicionalmente, a contributos da criminologia e dos estudos sobre cibercrime, com o objetivo de integrar diferentes perspetivas analíticas na delimitação conceptual proposta.

A metodologia utilizada baseia-se, assim, em três eixos fundamentais: (i) análise conceptual dos termos *Sextortion* e *Cibersextortion* na literatura científica; (ii) enquadramento jurídico-penal das condutas subjacentes à luz do ordenamento jurídico português; e (iii) problematização das implicações práticas decorrentes da adoção de diferentes opções terminológicas.

Não se trata, portanto, de um estudo empírico, mas antes de uma reflexão teórico-sistemática orientada para a clarificação conceptual e para a sua relevância na aplicação do Direito Penal.

3. Cibersextortion / Sextortion

Para Wolak e Finkelhor, o *Sextortion* é definido como fundamentalmente a ameaça de expor uma imagem sexual, real ou falsa, de modo a coagir a vítima a realizar algo ou por outros motivos, como vingança ou humilhação.

No contexto específico de envolvimento de menores, definem *Sextortion* como a ameaças de exposição pública para forçar a entrega de fotografias adicionais, à prática de atos sexuais ou outros favores. A essência reside na ameaça, independentemente de a exposição da imagem chegar a ocorrer (Wolak & Finkelhor, 2016).

Wittes e Popelin, por sua vez, descrevem *Sextortion* como uma forma de chantagem ou extorsão realizada através de uma rede informática, onde o item ou serviço exigido é a participação em um ato sexual. Caracterizam o crime como um "assalto remoto", destacando que a conectividade global permite que um agressor ameace sexualmente alguém sem estar no mesmo país. Distinguem ainda o *Sextortion* de esquemas que visem apenas dinheiro, colocando a "coação remota de sexo" como o elemento inovador deste crime (Wittes et al., 2016).

Para Liggett, Sextortion é definido como a ameaça de distribuir imagens ou vídeos íntimos a menos que a vítima satisfaça uma exigência, focando-se no processo de obtenção do conteúdo, como *grooming*[1] ou *hacking*[2](Liggett, 2019). Posteriormente, O'Malley e Smith enquadram o "*Sextortion* financeiro" como uma forma de abuso sexual baseado em imagens (IBSA), onde o agressor ameaça a divulgação pública dos conteúdos a menos que a vítima pague um resgate (O'Malley & Smith, 2024).

Igualmente em 2024, o grupo de trabalho de Tzani, classifica o *Sextortion* como um tipo de IBSA e violência sexual facilitada pela tecnologia (TFSV). Segundo os autores, o *Sextortion* ocorre quando um perpetrador ameaça distribuir material sexualmente explicito da vítima para a coagir a cumprir exigências como partilha de mais imagens, a prática de atos sexuais ou pagamentos financeiros (Tzani et al., 2024).

Desta forma, como já defendido em 2025[3], o *Cibersextortion* é tido como o ato de constranger, coagir ou ameaçar de expor publicamente imagens, vídeos ou mensagens que visem devassar a vida sexual das pessoas, através de meios de comunicação social, *Internet* ou outras formas de divulgação pública, para obter contrapartidas ilegítimas (Lourenço, 2025). Ao contrário do que acontece com crimes praticados sem recurso às TIC ou onde estas são visadas, esta prática utiliza "meios de comunicação social ou *Internet*".

Mesmo que se considere que "outros formas de divulgação pública" se refira a meios físico, flyers, panfletos ou cartazes, este elemento objetivo pode ser preenchido por, por exemplo, recurso às redes sociais. Onde até pode significar um impacto maior tanto no poder coercivo como nas consequências psicológicas nas vítimas deste tipo de ações (Wall, 2024). Observou-se ainda que o *Cibersextortion* pode decorrer de variadas motivações como sejam, as motivações económicas, sexuais, pessoais ou integradas.

De forma simples, entendeu-se enquadrar nas motivações económicas aquelas em que o agente age visando a obtenção de dinheiro. Nas motivações sexuais, aquelas em que o agente age com o objetivo de obter, por qualquer forma, gratificação sexual.

---

[1] O aliciamento online, também designado por *grooming* em inglês, pode ser definido como um processo de manipulação, geralmente aplicado em cenários em que as vítimas são crianças e/ou jovens menores. Em circunstâncias onde a vítima é maior de idade utilizam-se outras terminologias como *catfishing*, *romance scam*, entre outras. https://www.internetsegura.pt/grooming - Acedido em 31-03-2026.

[2]Hacking é o termo utilizado para descrever uma reprogramação de um sistema, programa ou dispositivo, de maneira não prevista e não autorizada pelo seu proprietário ou administrador. Com esta reprogramação o atacante pode obter acesso não autorizado a recursos e/ou ferramentas, anteriormente indisponíveis. https://www.internetsegura.pt/Hacking - Acedido em 31-03-2026.

[3] Ver a dissertação de Mestrado "O Fenómeno do Sextortion – Perspetivas jurídica e Tecnológica" - disponível em: https://recipp.ipp.pt/entities/publication/03cfd41c-afe5-4c43-96d6-fe134c27d70b - acedido em 31-03-2026.

Quanto às motivações pessoais entendeu-se enquadrar aquelas em que ofensor e vítima se conhecem caso, por exemplo, da pornografia de vingança. Já as motivações integradas, enquadra aquelas que abarcam dois ou mais dos pontos anteriores ou daqueles com outros menos expressivos (Lourenço, 2025).

Apesar da diversidade de definições apresentadas, importa sublinhar que a maioria das abordagens analisadas não distingue de forma clara entre contextos digitais e não digitais, privilegiando antes a natureza da ameaça e a finalidade coerciva da conduta. Esta ausência de diferenciação revela uma limitação conceptual relevante quando se pretende transpor estas definições para o domínio jurídico-penal.

Com efeito, ao não autonomizar o elemento tecnológico, estas definições tendem a diluir especificidades próprias do ambiente digital, nomeadamente o efeito multiplicador da exposição pública, a persistência dos conteúdos e a dificuldade de controlo sobre a sua disseminação. Tais fatores não apenas agravam o impacto sobre a vítima, como também alteram significativamente o equilíbrio de poder entre o agente e a vítima.

Neste sentido, a distinção entre *Sextortion* e *Cibersextortion* não deve ser entendida como meramente terminológica, mas como uma diferenciação com relevância material, capaz de influenciara interpretação e aplicação das normas penais.

4. Delimitação dogmática do conceito

A delimitação dogmática do conceito de *Cibersextortion* exige a identificação dos elementos estruturais que o distinguem de figuras afins, nomeadamente da extorsão clássica, da coação e de formas de abuso sexual baseado em imagem.

Neste sentido é possível identificar três elementos essenciais: (i) a existência de um conteúdo de natureza sexual, real ou simulado; (ii) a ameaça de divulgação desse conteúdo como forma de pressão; e (iii) a finalidade de obtenção de uma vantagem ilegítima, que pode assumir natureza patrimonial, sexual ou outra.

O elemento distintivo central reside, contudo, na mediação tecnológica da conduta. Ao contrário da extorsão tradicional, em que a ameaça pode assumir múltiplas formas, no *Cibersextortion* a capacidade coerciva decorre, em larga medida, do potencial de difusão massiva e instantânea, proporcionado pelas tecnologias digitais.

Deste modo, o conceito afasta-se de uma mera adaptação terminológica, assumindo relevância dogmática autónoma, na medida em que a dimensão digital não constitui apenas um meio, mas um fator que reconfigura a própria natureza da ameaça ampliando exponencialmente os seus efeitos (Venâncio, 2023; Wall, 2024; Lourenço, 2025).

4.1. Enquadramento jurídico-penal

Do ponto de vista jurídico-penal, o *Cibersextortion* não corresponde, no ordenamento jurídico português, a um tipo legal autónomo, sendo antes enquadrado numa pluralidade de tipos penais já previstos, em função das circunstâncias concretas do caso (Lourenço, 2025). Entre os tipos penais potencialmente aplicáveis incluem-se, desde logo, os crimes de ameaça do artigo 153º, e de coação do artigo 154º, ambos do Código Penal (CP), sempre que a conduta vise constranger a vítima à adoção de determinado comportamento.

Em situações em que exista obtenção de vantagem patrimonial, poderá igualmente estar em causa o crime de extorsão do artigo 223º, do CP. Paralelamente, quando a conduta envolve o acesso ou obtenção ilícita de conteúdos íntimos, poderá verificar-se a prática de crimes previstos da Lei do Cibercrime, nomeadamente o acesso ilegítimo do artigo 6º.

Acresce ainda a eventual aplicação do crime da devassa da vida privada do artigo 193º do CP, particularmente nos casos em que ocorre efetiva divulgação dos conteúdos.

Esta dispersão normativa destaca a natureza fragmentada da resposta ao fenómeno, levantando questões relevantes ao nível do concurso de crimes, da delimitação da pena e da coerência do sistema jurídico-penal face a novas formas de criminalidade digital (Ramalho & Ramalho, 2023). Importa, portanto, salientar que esta

multiplicidade de enquadramentos legais levanta dificuldades ao nível do concurso de crimes, nomeadamente na distinção entre concurso efetivo e aparente, bem como na delimitação do tipo legal prevalente.

Acresce que a dispersão normativa pode gerar incerteza na prática judiciária, conduzindo a soluções divergentes em casos materialmente semelhantes. Tal realidade reforça a necessidade de uma interpretação sistemática e teleologicamente orientada, capaz de assegurar coerência na aplicação do Direito Penal como defendido pela doutrina.

4.2. Cibercrime

Como já referido, o conceito de cibercrime encontra-se associado à prática de ilícitos em ambiente digital. O desenvolvimento exponencial das tecnologias digitais, aliado à massificação da *Internet* enquanto tecnologia de informação e comunicação, tem produzido transformações estruturais profundas nas dinâmicas sociais contemporâneas (Wall, 2024). Estas inovações proporcionaram ganhos inequívocos ao nível da comunicação, do acesso à informação e da partilha de conteúdos (F. P. De Andrade et al., 2020).

Todavia, em paralelo, catalisaram o aparecimento de novas formas de criminalidade, frequentemente desmaterializadas, transnacionais e tecnologicamente sofisticadas (Ribeiro, 2015). Neste sentido, o cibercrime surge como um fenómeno jurídico-criminal dinâmico, cuja delimitação conceptual e enquadramento normativo se encontram em constante mutação, acompanhando a evolução das técnicas e dos meios utilizados no ciberespaço (Venâncio, 2023).

A definição unívoca de cibercrime tem sido dificultada pela heterogeneidade de fenómenos que se pretende abranger. Na doutrina portuguesa, esta diversidade tem sido sistematizada através da distinção entre cibercrime em sentido estrito e em sentido amplo. O conceito de cibercrime surge de forma abrangente para designar um conjunto de ilícitos praticados com recurso às TIC, englobando tanto crimes novos como crimes tradicionais adaptados ao ambiente digital (Verdelho et al., 2003). Cibercrime em sentido estrito, refere-se às condutas em que o elemento informático integra o próprio tipo legal ou constitui o bem jurídico protegido, como sucede com os ilícitos previstos na Lei nº 109/2009, de 15 de setembro.

Já os cibercrimes em sentido amplo, são aqueles que abrangem todas as condutas ilícitas em que as tecnologias digitais assumem um papel meramente instrumental, funcionando como meio para a prática de crimes tradicionais (Venâncio, 2023; Nunes, 2024). Este entendimento corresponde, no plano internacional, ao que frequentemente se designa como crimes facilitados por tecnologias digitais (Hedidi, 2023). Distinção realizada entre crimes ciberdependentes e crimes ciberpotenciados.

Os primeiros são aqueles cuja existência depende intrinsecamente do ambiente digital, como o *hacking*, os ataques de negação de serviço (*DoS*)[4] ou a disseminação de *malware*[5]. Os segundos correspondem a crimes tradicionais cuja execução é ampliada ou facilitada pelas tecnologias, como a fraude *online*, o *phishing*[6] ou o *Cibersextortion*(Leukfeldt&Holt, 2019).

[4]Um ataque de negação de serviço (DoS) inunda um servidor com tráfego, tornando um site ou recurso indisponível. Disponível em: https://www.fortinet.com/br/resources/cyberglossary/dos-vs-ddos - Acedido em 31-03-2026.

[5]*Malware* é um termo genérico para qualquer tipo de software malicioso concebido para prejudicar ou explorar qualquer dispositivo, serviço ou rede programável. Os cibercriminosos normalmente utilizam-no para extrair dados que podem ser utilizados nas vítimas para obter ganhos financeiros. Esses dados podem variar entre dados financeiros, registos de assistência médica, correio eletrónico e palavras-passe. Disponível em: https://www.mcafee.com/pt-pt/antivirus/malware.html - Acedido em 31-03-2026.

[6]O*phishing* deve o seu nome à palavra inglesa "fishing" que significa "pescar", uma vez que estes grupos lançam o anzol e fazem-se passar por entidades geralmente conhecidas e credíveis, para obter acesso a contas privadas.A prática consiste em utilizar métodos tecnológicos que levam o utilizador a revelar dados pessoais e/ou confidenciais. Este tipo de ataques é geralmente acompanhado por mensagens de SPAM, enviadas para vários utilizadores.Disponívem em: https://www.internetsegura.pt/Phishing - Acedido em: 31-03-2026.

Esta tipologia articula-se com a doutrina nacional de (Venâncio, 2023) e (Nunes, 2024),e reforça a ideia de que o cibercrime constitui um fenómeno plurifacetado, abrangendo tanto ilícitos tradicionais adaptados ao meio digital como novas formas e criminalidade emergentes (Hedidi, 2023).

Assim, importa sublinhar que o *Cibersextortion* constitui um exemplo paradigmático de interceção entre cibercrime em sentido amplo e em sentido estrito. Durante a sua execução, podem verificar-se simultaneamente condutas que se enquadram em crimes tradicionais, como ameaça artigo 153º ou a coação do artigo 154ºambos do Código Penal, mediados por tecnologias. E, ilícitos em que o elemento informático integra o tipo legal, como o acesso ilegítimo do artigo 6º da Lei 106/2009 de 15/09 (Lei do Cibercrime - LC) ou a devassa da vida privada por meios digitais artigo 193º do CP.

Esta sobreposição contribui para a complexidade do seu enquadramento jurídico e torna evidente a necessidade de respostas normativas e investigatórias mais articuladas (Venâncio, 2023).:

5. Natureza do Ciberespaço

O ciberespaço, é simultaneamente um espaço informacional e uma rede global interconectada, contribui para a diluição das fronteiras físicas, colocando desafios significativos ao direito penal tradicional. A dimensão transnacional destas condutas exige, por conseguinte, mecanismos eficazes de cooperação internacional e esforços de harmonização legislativa (Deodato, 2024).

Contudo, persiste uma considerável heterogeneidade entre ordenamentos jurídicos, quer ao nível da tipificação penal, quer no que respeita aos regimes de obtenção e admissibilidade da prova digital, refletindo dificuldades já assinaladas na doutrina em 2009 (M. C. Andrade, 2009) e que, apesar do tempo decorrido, ainda não foram mitigadas.

Esta fragmentação normativa torna-se particularmente evidente em fenómenos híbridos como o *Cibersextortion*. Trata-se de uma realidade criminológica complexa que pode integrar múltiplos tipos penais, consoante as circunstâncias do caso em concreto, incluindo crimes previstos no Código Penal, na Lei do Cibercrime e em legislação e penal extravagante. Por exemplo, a Lei de Proteção de Dados Pessoais (Lei nº58/2019) que executa o Regulamento Geral sobre a Proteção de Dados (RGPD) de 2016. Tal pluralidade de enquadramentos jurídicos evidencia a dificuldade de subsunção destas condutas a categorias tradicionais e reforça a necessidade de abordagens integradas (Hedidi, 2023).

Acresce que a ausência de consenso conceptual a nível internacional gera constrangimentos operacionais relevantes. Desde logo, dificulta a produção de estatísticas comparáveis e compromete mecanismos de cooperação judiciária, como o reconhecimento mútuo de decisões ou a extradição de criminosos. Esta problemática é assim agravada pela natureza transnacional do *Cibersextortion*, em que os agentes operam frequentemente a partir de jurisdições distintas das da vítima (O'Malley & Smith, 2024)..

6. Problematização jurídica

A distinção entre *Sextortion* e *Cibersextortion* produz consequências práticas relevantes no plano jurídico, que ultrapassam a mera precisão conceptual. Desde logo, ao nível da qualificação jurídica dos factos. A utilização do termo *Cibersextortion* permite evidenciar a presença de elementos típicos associados ao cibercrime, facilitando a identificação de normas aplicáveis, nomeadamente as constantes da Lei do Cibercrime.

Em contraste, a utilização indistinta do termo *Sextortion* pode conduzir a uma subsunção excessivamente genérica a tipos legais tradicionais, desvalorizando a especificidade dos meios digitais.

Por outro lado, a distinção assume particular relevância em sede de investigação criminal. A identificação precoce da dimensão digital da conduta permite a adoção de mecanismos específicos de recolha de prova, como a preservação de dados informáticos ou a cooperação com plataformas digitais, cuja eficácia depende frequentemente da celeridade da intervenção.

Acresce ainda o impacto ao nível da cooperação internacional. A qualificação de determinados comportamentos como cibercrime pode facilitar a ativação de instrumentos jurídicos específicos, como convenções internacionais ou mecanismos de assistência mútua, particularmente relevantes em contextos transnacionais.

Por fim, a clareza terminológica contribui para uma melhor produção de dados estatísticos e para a definição de políticas mais eficazes, permitindo uma resposta mais ajustada à realidade do fenómeno. Não obstante, importa reconhecer que a adoção de uma terminologia mais precisa não resolve, por si, as dificuldades estruturais associadas ao fenómeno.

A eficácia da reposta jurídico-penal dependerá sempre da capacidade da adaptação dos mecanismos de investigação, da formação especializada dos operadores judiciários e da cooperação entre entidades públicas e privadas. Ainda assim, a clarificação conceptual constitui um primeiro passo para construção de um enquadramento jurídico mais coerente e eficaz.

7. Conclusões

A análise desenvolvida ao longo do presente artigo permite sustentar que a utilização indistinta dos termos *Sextortion* e *Cibersextortion* não é meramente uma questão semântica, mas antes um problema com implicações dogmáticas, jurídicas e operacionais no âmbito do Direito Penal.

Desde logo, verificou-se que o termo *Sextortion*, tal como definido na literatura internacional, apresentam uma natureza ampla e ambígua, podendo abranger condutas praticadas tanto em ambiente digital como fora dele. Esta amplitude conceptual, embora útil em contextos sociológicos, revela-se insuficiente quando transposta para o domínio jurídico-penal, onde a precisão terminológica constitui um requisito essencial.

Por outro lado, o termo *Cibersextortion* demonstra maior adequação técnico-jurídica, na medida em que incorpora expressamente o elemento digital como componente essencial da conduta. O prefixo "ciber" não apenas delimita o espaço de atuação, como também permite enquadrar o fenómeno no âmbito mais amplo do cibercrime, facilitando a sua integração sistemática nas categorias já consolidadas pela doutrina e legislação. Adicionalmente, conclui-se que o *Cibersextortion* constitui um fenómeno híbrido, situado na interseção entre cibercrimes em sentido estrito e em sentido amplo.

Tal característica traduz-se na coexistência de múltiplos tipos legais aplicáveis, desde crimes tradicionais mediados por tecnologias, como ameaça ou coação, até ilícitos especificamente informáticos, como o acesso ilegítimo ou a devassa da vida privada por meios digitais. Esta sobreposição gera dificuldades de enquadramento jurídico e exige uma abordagem interpretativa integrada.

Verificou-se ainda que a natureza transnacional do ciberespaço agrava os desafios associados à investigação e repressão deste fenómeno, nomeadamente ao nível da cooperação internacional, da recolha de prova digital e da harmonização legislativa. A ausência de consenso terminológico contribui, neste contexto, para a fragmentação das respostas jurídicas e para a ineficácia de mecanismos de cooperação.

Por fim, considera-se que a adoção do termo *Cibersextortion* no discurso jurídico e académico constitui um contributo relevante para a clarificação conceptual do fenómeno, promovendo maior rigor dogmático e facilitando a sua operacionalização prática. Tal opção terminológica revela-se particularmente importante num contexto em que a evolução tecnológica continua a desafiar as categorias tradicionais do Direito Penal.

Referências

Andrade, M. C. (2009). *Bruscamente no verão passado: A reforma do Código de Processo Penal – Observações críticas sobre uma lei que podia e devia ter sido diferente*. Coimbra Editora.

De Andrade, F. P., Fonseca, I., Silva, J. A., De Abreu, J. C., Jerónimo, P., Venâncio, P. D., & Freitas, P. M. (2020). *Relatório Cibersegurança em Portugal: Ética & direito*. https://www.cncs.gov.pt/docs/relatorio-eticadireito2020-observatoriociberseguranca-cncs.pdf

Deodato, B. R. L. (2024). *A investigação criminal em ambiente digital e a utilização de malware como meio de obtenção de prova entre a ineficácia e a ilegalidade* [Master's thesis, Universidade de Coimbra]. https://hdl.handle.net/10316/118220

Hedidi, M. (2023). Perspective chapter: Sexual cybercrime – The transition from the virtual aggression to the physical aggression. IntechOpen. https://doi.org/10.5772/intechopen.108786

Leukfeldt, R., & Holt, T. J. (2019). *The human factor of cybercrime* (1st ed., Vol. 3). Routledge. https://doi.org/10.4324/9780429460593

Liggett, R. (2019). Exploring online sextortion. *Sexual Assault Report*, 22(11), 58–63. https://www.civicresearchinstitute.com/online/PDF/FIPV-1104-04-Sextortion.pdf

Lourenço, P. (2025). *O fenómeno do sextortion: Perspetivas jurídica e tecnológica* [Master's thesis, Escola Superior de Tecnologia e Gestão, Politécnico do Porto]. http://hdl.handle.net/10400.22/31195

Nunes, D. R. (2024). *Os crimes previstos na lei do cibercrime* (2nd ed.; Gestlegal, Ed.).

O'Malley, R. L., & Smith, K. (2024). Suicidal ideation among male victim-survivors of financial sextortion. *Victims and Offenders*, 1–22. https://doi.org/10.1080/15564886.2024.2379818

Ramalho, J., & Ramalho, S. (2023). Sextortion: Caracterização dogmática e delimitação da imputação criminal em Portugal (O. Sanguiné, Ed.). *Revista Eletrônica de Direito Penal e Política Criminal – REDPPC*. https://seer.ufrgs.br/index.php/redppc/issue/view/5019/1429

Ribeiro, M. da C. F. (2015). *Cibercrime e prova digital* [Master's thesis, Instituto Superior Bissaya Barreto]. http://hdl.handle.net/10400.26/28946

Tzani, C., Ioannou, M., Fletcher, R., & Williams, T. J. V. (2024). Psychological factors leading to sextortion: The role of personality, emotional factors and sexual needs in victimisation. *Computers in Human Behavior, 159*, 108323. https://doi.org/10.1016/j.chb.2024.108323

Venâncio, P. D. (2023). *Lei do cibercrime: Anotada e comentada*. Editora d'Ideias.

Verdelho, P., Bravo, R., Rocha, M. L., & Veiga, P. (2003). *Leis do cibercrime* (1st ed.). Centro Atlântico.

Wall, D. (2024). *Cibercrime: A transformação do crime na era da informação*.

Wittes, B., Poplin, C., Jurecic, Q., & Spera, C. (2016, May). *Sextortion: Cybersecurity, teenagers, and remote sexual assault 1*. The Brookings Institution, 1–47. https://www.brookings.edu/wp-content/uploads/2016/05/sextortion1-1.pdf

Wolak, J., & Finkelhor, D. (2016). *Sextortion: Findings from a survey of 1,631 victims*. https://respect.international/sextortion-findings-from-a-survey-of-1631-victims/

Declaração Ética

Conflito de Interesse: Nada a declarar. **Financiamento:** Nada a declarar. **Revisão por Pares:** Dupla-cega.

Cookies, privacy and data protection

Cookies, privacidade e proteção de dados

10.29073/j2.v8i1.1124

Recebido: 01 de fevereiro de 2026.
Aprovado: 25 de março de 2026.
Publicado: 04 de abril de 2026.

Autor/a: Sílvia Cardoso, ESTG-IPP, Portugal, silviacardosolg@gmail.com.

Abstract

This paper aims to analyze issues related to cookies, privacy, and data protection, providing a critical overview of relevant literature and regulatory frameworks. It examines the implications of cookie usage in the context of the General Data Protection Regulation (GDPR), highlights current challenges, and discusses emerging trends such as the decline of third-party cookies and the rise of alternative tracking technologies. The paper concludes by proposing measures that organizations should adopt to ensure compliance and enhance user privacy in an evolving digital landscape.

Keywords: Cookies; Data Protection; ePrivacy; GDPR; Privacy.

Resumo

Este artigo tem como objetivo analisar questões relacionadas a cookies, privacidade e proteção de dados, fornecendo uma visão crítica da literatura relevante e dos marcos regulatórios. Examina as implicações do uso de cookies no contexto do Regulamento Geral de Proteção de Dados (RGPD), destaca os desafios atuais e discute tendências emergentes, como o declínio dos cookies de terceiros e a ascensão de tecnologias alternativas de rastreamento. O artigo conclui propondo medidas que as organizações devem adotar para garantir a conformidade e aprimorar a privacidade do usuário em um cenário digital em constante evolução.

Palavras-Chave: Cookies; Privacidade; Privacidade Eletrónica; Proteção de Dados; RGPD.

1. Introduction

Cookies, defined as small text files stored in a user's web browser when visiting a website, are a fundamental component of modern web technologies. They serve multiple purposes, including session management, personalization, and targeted advertising. However, due to their ability to collect and store significant amounts of user data, cookies raise substantial concerns regarding privacy and data protection.

With the enforcement of the General Data Protection Regulation (GDPR), stricter requirements were introduced regarding the processing of personal data, including data derived from cookies. The GDPR emphasizes transparency, accountability, and the need for explicit user consent(European Union, 2016). However, despite these requirements, many websites continue to implement inadequate consent mechanisms. As a result, the existing ePrivacy framework has been increasingly scrutinized, revealing regulatory gaps and the need for further legal harmonization.

In recent years, additional developments – such as stricter enforcement by data protection authorities and technological changes in tracking mechanisms – have significantly reshaped the landscape of online privacy. Notably, the progressive elimination of third-party cookies by major web browsers and the emergence of alternative tracking technologies have introduced new challenges and regulatory considerations.

Recent enforcement actions by European data protection authorities have reinforced the importance of valid consent, particularly in relation to misleading cookie banners and the use of manipulative design practices (CNIL,

2024). These developments highlight the need for continuous adaptation of both legal frameworks and organizational practices.

Furthermore, the rapid evolution of digital technologies and business models has made data protection an increasingly complex and dynamic field, requiring continuous adaptation of both legal and technical approaches.

2. Related Work

Several studies have explored the relationship between cookies and data protection, highlighting both legal and practical implications.

The study by Lima et al. (2023) compares cookie policies under the Brazilian LGPD and the European GDPR. It concludes that user consent mechanisms are often ineffective, as users are frequently compelled to accept terms to access online services. Furthermore, it emphasizes that the GDPR provides a more detailed and restrictive framework than other regulations.

Jayakumar (2021) investigates user attitudes toward cookie consent banners in the European Union. It highlights that factors such as design, trust, and perceived risk significantly influence user behavior. Importantly, it anticipates the decline of third-party cookies and suggests the emergence of more complex tracking technologies, reinforcing the need for enhanced regulatory frameworks.

Another study by Alharbi et al. (2023), evaluates compliance and usability of cookie interfaces. The findings reveal widespread use of manipulative design practices (dark patterns), with many websites failing to provide adequate privacy information or meaningful consent options.

Similarly, Cui (2021) presents empirical evidence showing that, despite regulatory requirements, many websites still fail to provide effective user control. Even when users attempt to reject cookies, tracking mechanisms often persist.

More recent studies reinforce these findings. Nouwens et al. (2025) highlight that a significant number of websites remain non-compliant with GDPR requirements, particularly due to the absence of clear rejection options. Additionally, Grossman et al. (2025) demonstrate that many cookie banners use manipulative design techniques to influence user behavior, undermining the validity of consent.

3. Challenges and Opportunities

3.1. Challenges

The use of cookies and similar tracking technologies raises several critical challenges.

Cookies enable extensive tracking and profiling of users across multiple websites, allowing organizations to build detailed behavioral profiles. This practice raises serious privacy concerns and may constitute an intrusion into user's personal lives.

Furthermore, cookies facilitate the collection and storage of large volumes of personal data, increasing the risk of unauthorized access and data breaches. The lack of transparency regarding how data is collected and used further exacerbates these concerns.

The protection of informational self-determination remains a critical challenge in the context of online tracking. Despite regulatory requirements, users often lack effective control over their data. Many websites implement interfaces that make it difficult to refuse cookies, frequently using manipulative design strategies known as dark patterns (CNIL, 2024; Grossman et al., 2025). These manipulative practices not only undermine user autonomy but also call into question the validity of consent under the GDPR framework (CNIL, 2024).

In addition, recent research indicates that tracking may persist even when users explicitly reject cookies, raising concerns about the effectiveness of consent mechanisms (Rasaii et al., 2025).

The ongoing evolution of tracking technologies also presents new regulatory challenges. As third-party cookies are progressively phased out, alternative techniques such as browser fingerprinting are becoming more prevalent, often operating outside traditional regulatory frameworks.

3.2. Opportunities

Despite these challenges, cookies and related technologies also present several benefits.

They enable personalized user experiences, improving usability and efficiency. Additionally, cookies support targeted advertising, allowing organizations to deliver more relevant content to users.

Cookies also play an important role in enhancing security, particularly in authentication processes and fraud detection. Moreover, the development of privacy-enhancing technologies, such as virtual private networks (VPNs) and ad blockers, provides users with greater control over their data.

Finally, evolving regulatory frameworks encourage organizations to adopt more transparent and user-centric data practices, contributing to improved privacy protection.

4. Recent Developments (Update)

In recent years, significant changes have reshaped the digital privacy landscape.

Data protection authorities have intensified enforcement actions, imposing substantial fines for non-compliance with cookie regulations (CNIL, 2025, 2026). These actions demonstrate a growing commitment to ensuring that organizations adhere to GDPR requirements. In practice, many widely used websites still implement non-compliant cookie banners, demonstrating a persistent gap between legal requirements and real-world implementation.

At the same time, major technology companies have begun phasing out third-party cookies, marking a significant shift in online tracking and advertising practices. This transition is leading to the emergence of alternative tracking technologies, which poses significant challenges for privacy protection.

In addition to the GDPR, the European Union has been working on the proposed ePrivacy Regulation, which is intended to replace the current ePrivacy Directive and provide more specific rules regarding electronic communications and the use of tracking technologies such as cookies.

The ePrivacy Regulation aims to strengthen user confidentiality, regulate the use of metadata, and ensure stricter conditions for storing and accessing information on user devices. In particular, it reinforces the requirement for prior user consent for non-essential cookies and seeks to address emerging tracking techniques that are not fully covered by existing legislation.

However, despite its relevance, the regulation has faced delays and has not yet been fully adopted, creating ongoing legal uncertainty in the field of online privacy (European Union, 2016). This delay highlights the difficulty of regulating rapidly evolving technologies, particularly in the context of digital advertising and data-driven business models.

5. Conclusions

Cookies remain a central component of the modern digital ecosystem, particularly in areas such as marketing and personalization. However, their use continues to raise important concerns regarding privacy and data protection.

While the GDPR has established a strong legal foundation, ongoing technological developments and evolving tracking practices require continuous regulatory adaptation. The increasing use of alternative tracking methods further complicates the landscape, highlighting the need for more robust and comprehensive solutions.

To address these challenges, organizations should adopt several key measures. These include ensuring transparency in data collection practices, limiting the use of third-party cookies, implementing strong security mechanisms, and providing users with clear and accessible control options.

Additionally, organizations must obtain explicit and informed consent, avoid manipulative interface designs, and define clear data retention policies. These measures are essential to ensure compliance with regulatory requirements and to protect users' fundamental rights.

Achieving a balance between technological innovation and privacy protection is crucial. As the digital environment continues to evolve, both legal frameworks and organizational practices must adapt to ensure that user privacy is effectively safeguarded. Ultimately, safeguarding user privacy in the digital age is not only a legal obligation but a fundamental requirement for maintaining trust in modern data-driven ecosystems.

Despite the existence of robust legal frameworks, there is a persistent gap between regulation and practice, as many organizations continue to implement non-compliant tracking mechanisms. This suggests that enforcement alone may not be sufficient, requiring a combination of technological solutions, user awareness, and stricter accountability mechanisms.

References

Alharbi, J. A., Albesher, A. S., & Wahsheh, H. A. (2023). An empirical analysis of e-governments' cookie interfaces in 50 countries. *Sustainability, 15*(2), 1231. https://www.mdpi.com/2071-1050/15/2/1231

Commission Nationale de l'Informatique et des Libertés (CNIL). (2024). *Dark patterns in cookie banners: CNIL issues formal notice to website publishers*. https://www.cnil.fr/en/dark-patterns-cookie-banners-cnil-issues-formal-notice-website-publishers

Commission Nationale de l'Informatique et des Libertés (CNIL). (2025). *Cookie regulation: CNIL continuing action plan and sanctions*. https://www.cnil.fr/en/cookie-regulation-cnil-continuing-action-plan-initiated-2019-and-has-imposed-two-fines-shein-and

Commission Nationale de l'Informatique et des Libertés (CNIL). (2026). *Sanctions and corrective measures: CNIL's actions in 2025*. https://www.cnil.fr/en/sanctions-and-corrective-measures-cnils-actions-2025

Cui, Y. (2021). *Measure cookie setting behavior of web pages showing cookie privacy warnings* (Master's thesis, University of Edinburgh). https://groups.inf.ed.ac.uk/tulips/projects/20-21/cui.pdf

European Union. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation)*. https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A02016R0679-20160504

Grossman, R., Smith, M., Borcea, C., & Chen, Y. (2025). Using salient object detection to identify manipulative cookie banners that circumvent GDPR. https://arxiv.org/pdf/2510.26967

Jayakumar, L. N. (2021). Cookies 'n' consent: An empirical study on the factors influencing website users' attitudes towards cookie consent in the EU. *DBS Business Review*. https://dbsbusinessreview.ie/index.php/journal/article/view/72

Lima, C. R. C., Silva, I. F. S., Silva, R. D., & Carr, C. N. (2023). Cookies and their close relationship with data protection policy. *Brazilian Journal of Development*. https://ojs.brazilianjournals.com.br/ojs/index.php/BRJD/article/view/56231/41313

Nouwens, M., Kristensen, J. B., Maalt, K., & Bagge, R. (2025). A cross-country analysis of GDPR cookie banners and compliance: Flexible methods for scraping them.

Rasaii, A., Dao, H., Feldmann, A., Javid, M., Gasser, O., & Gosain, D. (2025). Intractable cookie crumbs: Unveiling the nexus of stateful banner interaction and tracking cookies. https://www.researchgate.net/publication/395442240_Intractable_Cookie_Crumbs_Unveiling_the_Nexus_of_Stateful_Banner_Interaction_and_Tracking_Cookies

Declaração Ética

Conflito de Interesse: Nada a declarar. **Financiamento:** Nada a declarar. **Revisão por Pares:** Dupla-cega.

A mitigação de riscos à privacidade e vieses no pré-processamento de dados num processo de triagem de currículos baseado em modelos de I.A. generativa

Mitigating privacy risks and algorithmic biases in data pre-processing within generative AI-based curriculum screening processes

10.29073/j2.v8i1.1107

Recebido: 20 de fevereiro de 2026.
Aprovado: 21 de março de 2026.
Publicado: 04 de abril de 2026.

Autor/a 1: Ana Dara Fernandes, ESTG-IPP, Portugal, 8240099@estg.ipp.pt.
Autor/a 2: Marco Filipe Gomes, ESTG-IPP, Portugal, mfg@estg.ipp.pt.
Autor/a 3 (Correspondente): Sérgio Miguel Tomás, ESTG-IPP, Portugal, smt@estg.ipp.pt.

Resumo

Este artigo analisa o uso de I.A. generativa em sistemas de triagem automatizada de currículos, articulando perspetivas jurídicas e computacionais, ao estudar um conjunto de 758 currículos associados a um processo de recrutamento na Federação Polaca de Futsal.

O objetivo centrou-se em criar uma cadeia de pré-processamento de dados que mitigasse os riscos associados à privacidade e vieses (bias) dos dados de entrada a modelos de I.A. A experiência realizada permitiu desenvolver procedimentos de extração automática, anonimização manual e de normalização dos dados em bruto que mitigassem vieses inerentes. Os programas desenvolvidos foram executados localmente, alinhando-se com os princípios do RGPD e com as obrigações do regulamento AI Act para sistemas de alto risco.

Os resultados indicam uma redução do risco associado aos vieses e reforça a importância de uma abordagem de mitigação de riscos no pré-processamento dos dados antes de os submeter a modelos de I.A. generativa.

Palavras-Chave: Inteligência Artificial Generativa; Recrutamento; Recursos Humanos; RGDP; Triagem de Currículo.

Abstract

This article examines the use of generative AI in automated résumé-screening systems, combining legal and computational perspectives through the analysis of a dataset of 758 résumés associated with a recruitment process conducted by the Polish Futsal Federation. The objective was to design a data pre-processing pipeline capable of mitigating privacy risks and biases present in the input data used by AI models.

The experiment enabled the development of procedures for automatic data extraction, manual anonymization, and normalization of raw data in order to reduce inherent biases. All programs were executed locally, ensuring alignment with GDPR principles and with the obligations established by the AI Act for high-risk systems.

The results indicate a reduction in bias-related risks and reinforce the importance of adopting a risk-mitigation approach during data pre-processing before submitting information to generative AI models.

Keywords: GDPR; Generative Artificial Intelligence; Human Resources; Recruitment; Résumé Screening.

1. Introdução

A Inteligência Artificial (I.A.) tornou-se um elemento central na transformação da área de recursos humanos (RH), permitindo automatizar e otimizar funções como o recrutamento, a integração, a formação e a avaliação

de desempenho (Dasaklis et al., 2025). Entre estas funções, o recrutamento e a seleção assumem um papel particularmente relevante, uma vez que influenciam diretamente o desempenho global das organizações.

A triagem de currículos constitui a primeira fase eliminatória do processo de recrutamento, na qual os profissionais de RH analisam e filtram candidaturas para identificar perfis alinhados com os requisitos da função e com a cultura organizacional (Costa, 2024; Barreto et al., 2023).

O facto de o recrutamento e a triagem de currículos serem funções transversais a organizações de diferentes setores, geografias e dimensões reforça a relevância científica e social deste domínio. Pequenas alterações nos critérios de seleção ou nos dados utilizados podem afetar grandes volumes de candidatos, reproduzindo práticas discriminatórias em larga escala (Rana, 2021).

Apesar dos avanços tecnológicos da I.A., a automatização da triagem de currículos apresenta riscos significativos para reproduzir e amplificar padrões de discriminação. Apesar dos avanços tecnológicos da I.A., a automatização da triagem de currículos apresenta riscos significativos de reprodução e amplificação de enviesamentos.

Estudos demonstram que sistemas treinados com dados históricos podem reproduzir padrões de discriminação de género, idade e outras características demográficas, dado que estes sistemas são "alimentados" por conjunto de dados contendo vieses inerentes (e.g., um conjunto de dados que não representa a realidade de forma equilibrada ou neutra, fazendo com que certas características, grupos ou padrões apareçam mais ou menos importantes do que realmente são). Por exemplo, mulheres mais velhas ou com filhos apresentam menor probabilidade de avançar para etapas subsequentes, mesmo quando possuem qualificações equivalentes (Derous & Decoster, 2017; González et al., 2019). Similarmente, currículos de candidatos mais velhos recebem menos respostas positivas do que os de candidatos mais jovens, evidenciando discriminação etária (Derous & Decoster, 2017).

No ordenamento jurídico português, o artigo 24.º do Código do Trabalho, reforçado pela Lei n.º 13/2023 (Agenda do Trabalho Digno), consagra o princípio da igualdade e da não discriminação no acesso ao emprego e nas condições de trabalho. Este regime articula-se com o RGPD, em particular com o artigo 22.º relativo a decisões automatizadas, e com o Regulamento Europeu de Inteligência Artificial (AI Act), que classifica os sistemas de I.A. utilizados em contexto laboral como sistemas de alto risco, impondo obrigações reforçadas de transparência, segurança, supervisão humana e mitigação de riscos de discriminação.

Este trabalho destaca, assim, a mitigação do risco de enviesamento das decisões promovidas por modelos de I.A. como um campo de investigação importante e considera a fase de pré processamento de currículos em sistemas de triagem automatizada com I.A. generativa como uma fase importante para a mitigação dos riscos associados à reprodução da discriminação e à privacidade dos dados.

Este enquadramento jurídico-normativo condiciona o desenho da solução técnica adotada, nomeadamente as opções de execução local, anonimização e normalização dos dados, em conformidade com o RGPD e o AI Act. Importa distinguir decisões automatizadas, nos termos do artigo 22.º do RGPD, de sistemas de apoio à decisão. No presente estudo, a triagem configura uma decisão automatizada, por resultar do processamento autónomo do sistema, convocando as garantias aplicáveis a decisões exclusivamente automatizadas com impacto significativo.

Alinhadas com o objetivo do artigo, duas perguntas de investigação foram formuladas: a primeira, é possível, no contexto de um processo de triagem de currículos, desenvolver procedimentos que possam mitigar os riscos associados ao processamento de conjuntos de dados contendo vieses? e a segunda, até que ponto a eliminação de vieses e a mitigação de riscos à privacidade podem reduzir indicadores diretos e indiretos a atributos sensíveis nos currículos num conjunto de dados desbalanceado (em que certas categorias, grupos ou valores estão representados de forma muito desigual)?

Embora um conjunto de estudos recentes, destacados na revisão da literatura deste artigo, explore as potencialidades e oportunidades da utilização de sistemas de inteligência artificial nos processos de recrutamento, em particular na fase de triagem, a maioria dessas abordagens não se centra nos riscos associados à submissão de conjuntos de dados desbalanceados e estruturalmente enviesados a modelos de inteligência artificial generativa (por exemplo, ChatGPT).

É neste contexto que o presente trabalho enfatiza uma experiência conduzida com 758 currículos reais, submetidos no âmbito de um processo de candidatura a um cargo na administração da Federação Polaca de Futsal. Todos os programas desenvolvidos foram executados localmente, num ambiente controlado, sem recurso a infraestruturas externas, com o objetivo de responder às questões de investigação que orientaram este estudo. A experiência permitiu analisar, de forma controlada, como os procedimentos adotados influenciam a mitigação de riscos num processo de triagem automatizada. A execução local garantiu a confidencialidade, integridade e auditabilidade dos dados, reforçando a segurança e a conformidade com os princípios do RGPD e do AI Act.

2. Revisão da Literatura

O recrutamento e seleção envolve ações estruturadas para atrair candidatos qualificados (Loureiro, 2023), sendo a triagem de currículos crucial para determinar quem avança, influenciando a equidade e eficácia da seleção (Costa, 2024). Tradicionalmente realizada manualmente ou com regras fixas, o aumento do número de candidaturas gerou gargalos operacionais (Barreto et al., 2023), tornando a automação e a I.A. ferramentas estratégicas para gerir grandes volumes de dados, triagem de currículos, avaliação de competências e entrevistas (Lo et al., 2025; Blumen & Cepellos, 2023; Dargnies et al., 2022; Moreira, 2022).

A I.A. generativa destaca-se por compreender linguagem natural, sintetizar informações e extrair conhecimento de grandes volumes de dados, permitindo decisões mais eficientes (Dasakliset al., 2025) e triagem automatizada flexível capaz de identificar competências implícitas (Lo et al., 2025). Apesar de ganhos em eficiência e redução de custos (Chen, 2023; Marcelino, 2023), estes sistemas reproduzem vieses que podem comprometer princípios de equidade e não discriminação (Chen, 2023; Moreira, 2022; Anzenberg et al., 2025). Estudos mostram que mulheres mais velhas e candidatos com nomes estrangeiros têm menor probabilidade de avançar, e que a idade funciona como proxy de outros atributos (González et al., 2019; Wen et al., 2025). Sivakaminathan & Musi (2025) evidenciam que o ChatGPT reforça enviesamentos de género presentes em anúncios de emprego, privilegiando traços associados a linguagem masculina, enquanto a falta de transparência gera frustração entre candidatos (Armstrong et al., 2024).

Dada a influência direta das decisões automatizadas, a utilização de I.A. no recrutamento exige enquadramento jurídico e ético rigoroso, com mecanismos de segurança, transparência e responsabilização. Em Portugal, o Código do Trabalho garante não discriminação e igualdade, aplicáveis a decisões algorítmicas, prevendo inversão do ónus da prova (Falcão & Tomás, 2025, pp. 102-109; Machado & Magalhães, s.d.), enquanto o artigo 22.º do RGPD limita decisões exclusivamente automatizadas, exigindo salvaguardas como supervisão humana (Peixe, 2025).

O AI Act regula sistemas de alto risco, reforçando gestão de risco, qualidade de dados, transparência e supervisão, articulando-se com RGPD nos princípios de minimização de dados, proteção desde a conceção e segurança do tratamento (artigos 5.º, 25.º e 32.º).

A anonimização assume papel central na mitigação de riscos de privacidade, e o artigo 10.º permite tratamento de dados sensíveis para mitigar enviesamentos, condicionado a pré-processamento rigoroso e auditoria (Awadet al., 2023; van Bekkum, 2025). O caso da Amazon (2018) ilustra estes riscos, com enviesamento de género que levou à suspensão do sistema (Rodriguez, 2023; Viana & Macedo, 2024; Ataíde, 2025).

A literatura evidencia limitações na aplicação da I.A. generativa na triagem de currículos, nomeadamente no que concerne à reprodução de enviesamentos e a falta de transparência e privacidade. Em resposta, o capítulo seguinte apresenta a metodologia utilizada neste estudo, baseada num pré-processamento estruturado e

sequencial, inspirado em equidade composicional (Biswas&Rajan, 2021), permitindo analisar sistematicamente o impacto de cada intervenção na mitigação dos riscos mencionados anteriormente na fase de pré-processamento dos dados de um sistema de triagem automatizada.

3. Redução de Vieses e Proteção de Privacidade no Pré-Processamento de Currículos para Sistemas de I.A. de Alto Risco

A presente experiência parte do pressuposto de que, em sistemas de triagem automatizada baseados em modelos de linguagem de grande dimensão, a gestão dos dados e o pré-processamento são determinantes centrais do comportamento algorítmico, frequentemente mais relevantes do que a própria arquitetura do modelo. A literatura indica que estes modelos tendem a reproduzir enviesamentos linguísticos e estruturais existentes, sobretudo em domínios marcados por desigualdades de género e idade.

A experiência baseou-se num conjunto de 758 currículos reais relativos a um processo de candidatura à administração da Federação Polaca de Futsal, disponibilizados no âmbito de uma colaboração científica com a Universidade de Bielsko-Biala.

Os dados apresentavam elevada heterogeneidade estrutural e linguística (currículos no formato digital em diferentes formatos (e.g., PDF, DOCX) e em diferentes línguas (Polaco e Inglês) e existindo uma distribuição demográfica e profissional desigual (83% dos candidatos eram do género masculino e 72% tinham sido jogadores ou treinadores) configurando um risco algorítmico relevante.

Neste contexto, adotou-se uma abordagem de Ação-Investigação, integrando a neutralização de enviesamentos e a proteção da privacidade desde a fase de pré-processamento, concebida como um instrumento de governação de dados em sistemas de I.A. de alto risco.

As seções seguintes descrevem detalhadamente a cadeia de pré-processamento desenvolvida, as etapas envolvidas, os riscos mitigados e a sua articulação com os requisitos legais aplicáveis, incluindo o RGPD e o AI Act.

3.1. Metodologia Aplicada e Etapas do Pré-Processamento

A investigação adotou uma abordagem de Ação-Investigação, na qual cada intervenção técnica no pré-processamento foi acompanhada por observação sistemática e reflexão crítica sobre os seus efeitos no comportamento do modelo de linguagem. Esta metodologia permitiu iterar e ajustar a cadeia de pré-processamento com base em evidência empírica, integrando simultaneamente requisitos técnicos, éticos e jurídicos.

O objetivo central foi mitigar a reprodução de enviesamentos presentes nos dados, assegurando, em paralelo, a integridade, utilidade e confidencialidade da informação no sistema automatizado de triagem.

O pré-processamento foi estruturado em cinco etapas principais. A primeira consistiu na extração automática do conteúdo textual dos currículos com scripts em Python capazes de lidar com múltiplos formatos e línguas, garantindo uniformidade, rastreabilidade e mitigação de vieses estruturais.

A segunda etapa envolveu a anonimização manual, justificada pela elevada densidade contextual dos documentos. A título ilustrativo, antes do pré-processamento, cerca de 82% dos currículos continham identificadores diretos (nomes completos, endereços de email ou contactos telefónicos), percentagem que foi reduzida para 0% após a anonimização.

Foram igualmente removidos identificadores indiretos, como referências a instituições, cargos específicos e eventos profissionais, com a eliminação fictícia de aproximadamente 1950 entidades nomeadas, distribuídas por categorias como instituições de ensino (41%), clubes ou organizações desportivas (33%) e cargos ou funções específicas (26%).

Estas intervenções protegeram a privacidade e neutralizaram fontes explícitas de enviesamento associadas à identificação individual, em conformidade com o RGPD. Seguiu-se a terceira etapa em que consistiu na normalização estrutural, segmentando os currículos em secções homogéneas (formação académica, experiência profissional, competências e certificações).

Após esta etapa, 100% dos currículos passaram a obedecer a uma estrutura comum, eliminando variações narrativas que, em cenários não controlados, podem favorecer estilos discursivos associados a determinados grupos sociais.

Esta normalização permitiu ainda identificar, de forma controlada, indicadores indiretos de atributos sensíveis, como referências temporais suscetíveis de inferir idade, sem os expor diretamente ao modelo. A quarta etapa centrou-se na mitigação de enviesamentos linguísticos. De forma ilustrativa, referências explícitas a atributos sensíveis (e.g., género, estado civil) foram reduzidas de cerca de 18% dos currículos para 0%, enquanto variáveis substitutas com potencial discriminatório foram neutralizadas e padronizadas em aproximadamente 64% dos casos identificados.

A quinta etapa consistiu na execução local de toda a cadeia de pré-processamento, sem recurso a infraestruturas externas em linha com boas práticas de engenharia de software. O resultado foi um conjunto de currículos anonimizados, normalizados e com parcialidade mitigada, adequado à avaliação por modelos de I.A. generativa e à comparação com decisões humanas. Isto permitiu separar claramente enviesamento nos dados (desigualdade demográfica e profissional) do enviesamento no output do modelo, preparando os dados para avaliação ética de sistemas de I.A. generativa.

Todas as intervenções foram alinhadas com os princípios do RGPD e do AI Act, incluindo minimização de dados, proteção desde a conceção, segurança do tratamento, qualidade dos dados, gestão de riscos, supervisão humana e transparência. Assim, o pré-processamento assumiu-se como instrumento de governação de dados, assegurando uma triagem automatizada ética, transparente e juridicamente compatível.

3.2. Resultados Obtidos

O conjunto de currículos foi submetido à cadeia de pré-processamento (feito através de uma sequência de execução de programas em Python desenvolvidos para o efeito) e resultou num conjunto de dados anonimizados, normalizados e com parcialidade mitigada. Importa notar que, apesar destas medidas, a anonimização não é absoluta, aproximando-se conceptualmente de pseudonimização, subsistindo um risco residual de reidentificação em cenários de cruzamento com fontes externas, o qual foi considerado aceitável no contexto controlado do estudo. A análise das etapas de pré-processamento ajudou a compreender os passos para a mitigação de riscos e enviesamentos (ver a Tabela 1).

Em particular, para salientar o que foi realizado na experiência, destacam-se alguns dos procedimentos concretizados: a extração automática assegurou integridade e uniformidade dos dados, mitigando o viés estrutural associado a diferentes formatos e extensões de documentos.

Por outro lado, a anonimização manual reduziu o risco de re-identificação e viés de prestígio; a normalização garantiu que a informação relevante fosse avaliada de forma consistente; e a execução local garantiu confidencialidade e integridade dos dados sensíveis, em conformidade com o RGPD e o AI Act. Os resultados indicaram uma redução da influência de fatores irrelevantes ou potencialmente discriminatórios, aumentando a equidade e a auditabilidade das decisões automatizadas.

De forma sintetizada, a relação entre decisões de pré-processamento, enviesamentos mitigados e enquadramento regulatório encontra-se apresentada na Tabela 1.

Tabela 1: Decisões de pré-processamento, enviesamentos e regulamentação

Decisão técnica	Enviesamento ou risco mitigado	Fundamentação regulatória

Extração automática padronizada	Viés estrutural	Art. 25.º RGPD; Art. 10.º AI Act
Anonimização manual	Risco de re-identificação e viés de prestígio	Art. 5.º, 25.º, 32.º RGPD; Art. 10.º, 14.º AI Act
Normalização estrutural	Viés narrativo	Art. 10.º, 13.º AI Act
Mitigação de enviesamentos linguísticos	Viés de género, etário e geracional	Art. 9.º AI Act
Execução local da cadeia de pré-processamento	Risco de confidencialidade	Art. 32.º RGPD; Art. 9.º AI Act

Esta abordagem permitiu estabelecer um enquadramento para a governação de dados, integrando mitigação de parcialidade, proteção da privacidade e conformidade regulatória, assegurando uma triagem automatizada ética, transparente e auditável.

3.3. Discussão e Limitações Técnicas

A experiência desenvolvida demonstra que uma cadeia de pré-processamento contendo procedimentos de mitigação de riscos, como a anonimização manual, a normalização estrutural e a mitigação de enviesamentos linguísticos, contribui de forma para a redução dos vieses de dados e dos riscos à privacidade, permitindo que modelos de linguagem de grande dimensão (I.A. generativa) operem de forma mais equitativa e auditável.

À luz dos indicadores quantitativos apresentados, é possível afirmar que o pré-processamento contribuiu de forma significativa para a redução de vieses nos dados, em particular no que respeita a viés de identificação pessoal, viés estrutural e viés linguístico, com reduções observáveis entre 75% e 100%, consoante a categoria analisada. Em contrapartida, o viés de representatividade demográfica e profissional manteve-se, refletindo a composição original da amostra e sendo tratado como um risco conhecido e controlado, e não como um artefacto introduzido pelo sistema.

Esta separação permitiu distinguir claramente enviesamento nos dados de enviesamento no output do modelo, reforçando a validade metodológica e a interpretabilidade dos resultados. Estes resultados alinham-se com a necessidade de mitigar os riscos estudos dado que os modelos generativos como o ChatGPT podem amplificar enviesamentos de género na triagem de currículos quando expostos a descrições de funções com linguagem "orientada ao género" (Sivakaminathan & Musi, 2025).

Apesar destes resultados, a investigação apresenta limitações metodológicas. A distribuição demográfica desigual do conjunto de dados limitou a avaliação do impacto das intervenções em grupos minoritários. Adicionalmente, a anonimização manual e a neutralização de variáveis substitutas exigem elevado esforço humano e conhecimento contextual, dificultando a sua replicação em conjuntos de dados de grande escala.

Por fim, a execução local da cadeia de pré-processamento, embora assegure elevados níveis de confidencialidade e segurança, restringe a escalabilidade e a integração em arquiteturas distribuídas.

3.4. Resposta às Perguntas de Investigação

Em resposta à primeira pergunta de investigação, que questiona se é possível desenvolver procedimentos que mitiguem os riscos associados ao processamento de conjuntos de dados contendo vieses, a experiência demonstrou que procedimentos sistemáticos de pré-processamento são eficazes nesse sentido.

A combinação de extração automática do conteúdo textual (utilizando bibliotecas Python como PyPDF2, python-docx e Textract), anonimização manual e automatizada (com técnicas de Reconhecimento de Entidades Nomeadas, via spaCy), normalização estrutural (segmentação semântica em secções de formação, experiência e competências, apoiada em regras heurísticas e classificadores simples) e neutralização de enviesamentos

linguísticos e estruturais (com a remoção de referências a género, idade e proxies implícitos) mostrou-se capaz de reduzir a influência de atributos sensíveis e padrões discriminatórios.

A execução local em ambiente controlado garantiu rastreabilidade, integridade e conformidade com o RGPD e o AI Act, evidenciando que tais procedimentos constituem instrumentos relevantes de governação de dados em sistemas de triagem automatizada de alto risco.

Relativamente à segunda pergunta de investigação, que incide sobre até que ponto a eliminação de vieses e a mitigação de riscos à privacidade reduzem indicadores diretos e indiretos de atributos sensíveis em conjuntos de dados desbalanceados, a análise revelou que o pré-processamento diminuiu significativamente a presença de identificadores diretos (nomes, contactos, referências institucionais) e de representantes de atributos sensíveis (como extensões de carreira ou expressões linguísticas codificadas por género ou idade).

Apesar do desbalanceamento acentuado por género e faixa etária, estas intervenções tornaram os dados mais neutros e consistentes, reduzindo a probabilidade de reprodução de discriminação implícita. Embora não elimine totalmente os efeitos do desbalanceamento, o pré-processamento forneceu uma base mais segura para a aplicação de modelos de I.A. generativa e para comparações com avaliações humanas, demonstrando que a mitigação de enviesamentos e a proteção de privacidade a montante são cruciais para reduzir riscos éticos, legais e técnicos em sistemas de triagem automatizada.

4. Conclusão

A investigação realizada centrou-se no estudo da fase inicial de tratamento dos dados para sistemas de triagem automatizada, em que a ausência de pré-processamento rigoroso pode perpetuar desigualdades históricas de género, idade e origem, produzindo decisões enviesadas e, por conseguinte, juridicamente inválidas. Por isso, este estudo integrou uma cadeia de pré-processamento de dados contendo procedimentos de mitigação de riscos, constituindo uma resposta técnico-jurídica concreta à necessidade de integrar os requisitos do RGPD e do AI Act.

Este trabalho representa, assim, o primeiro passo de um estudo mais amplo, que visa não apenas fundamentar técnica e juridicamente a fase de preparação dos dados, mas também avaliar empiricamente os efeitos dessa preparação sobre o desempenho e a equidade dos modelos de I.A. generativa aplicados à triagem de currículos. A continuidade do estudo incidirá sobre a avaliação empírica do impacto do pré-processamento, através de uma comparação sistemática entre os conjuntos de dados brutos e tratados.

Como perspetiva de trabalho futuro, pretende-se ampliar a generalização desta metodologia a conjuntos de dados mais vastos e diversificados, incorporando currículos de diferentes contextos geográficos, setores profissionais e níveis de qualificação, de forma a testar a robustez da abordagem em condições variadas e analisar o desempenho de modelos de I.A. generativa considerando conjunto de dados pré-processados e não pré-processados no contexto de processos de triagem automatizada.

Referências

Anzenberg, E., Samajpati, A., Chandrasekar, S., & Kacholia, V. (2025). Evaluating the promise and pitfalls of LLMs in hiring decisions [Preprint]. *arXiv*. https://doi.org/10.48550/arXiv.2507.02087

Armstrong, L., Liu, A., MacNeil, S., & Metaxa, D. (2024). The silicon ceiling: Auditing GPT's race and gender biases in hiring [Preprint]. *arXiv*. https://doi.org/10.48550/arXiv.2405.04412

Ataíde, M. C. (2025). A discriminação algorítmica na seleção de trabalhadores: O caso Amazon. *Cadernos Jurídicos da Faculdade de Direito de Sorocaba, 5*(1), 33–58. https://cadernosjuridicos.fadi.br/cadernosjuridicos/article/view/125

Awad, E., Balafoutas, L., Chen, L., Ip, E., & Vecci, J. (2023). Artificial intelligence and debiasing in hiring: Impact on applicant quality and gender diversity [Preprint]. *SSRN*. https://doi.org/10.2139/ssrn.4626059

Barreto, J. C., Stefano, E., Freitag, A. E. B., Santana, W. A., & Picoli, M. A. (2023). Currículo inclusivo: Uma proposta para a equidade e efetividade nos processos de recrutamento. *Revista de Gestão e Secretariado, 14*(5), 7586–7607. https://doi.org/10.7769/gesec.v14i5.2139

Biswas, S., & Rajan, H. (2021). Fair preprocessing: Towards understanding compositional fairness of data transformers in machine learning pipeline [Preprint]. *arXiv*. https://doi.org/10.48550/arXiv.2106.06054

Blumen, D., & Cepellos, V. M. (2023). Dimensões do uso de tecnologia e inteligência artificial (IA) em recrutamento e seleção (R&S): Benefícios, tendências e resistências. *Cadernos EBAPE, 21*(2), 1–16. https://doi.org/10.1590/1679-395120220080

Chen, Z. (2023). Ethics and discrimination in artificial intelligence-enabled recruitment practices. *Humanities & Social Sciences Communications, 10*, Article 567. https://doi.org/10.1057/s41599-023-02079-x

Costa, V. S. A. (2024). *A utilização de inteligência artificial na triagem de currículos e tomada de decisão em processos seletivos* [Trabalho de conclusão de curso, Universidade Estadual de Goiás]. Repositório Institucional. https://repositorio.ueg.br/jspui/handle/riueg/6213

Coutinho, C. P., Sousa, A., Dias, A., Bessa, F., Ferreira, M. J., & Vieira, S. (2009). Investigação-ação: Metodologia preferencial nas práticas educativas. *Psicologia, Educação e Cultura, 12*(2), 455–479. https://hdl.handle.net/1822/10148

Dargnies, M. P., Hakimov, R., & Kübler, D. (2022). Aversion to hiring algorithms: Transparency, gender profiling, and self-confidence [Preprint]. *SSRN*. https://doi.org/10.2139/ssrn.4238275

Dasaklis, T. K., Giannopoulos, P. G., Koutras, D., Malamas, V., & Chountalas, P. T. (2025). Large language models in human resource management: A systematic literature review of applications, open issues, and future research directions. *Decision Support Systems*. Advance online publication. https://doi.org/10.2139/ssrn.5314976

Derous, E., & Decoster, J. (2017). Implicit age cues in résumés: Subtle effects on hiring discrimination. *Frontiers in Psychology, 8*, Article 1321. https://doi.org/10.3389/fpsyg.2017.01321

Falcão, D., & Tomás, S. T. (2025). *Lições de direito do trabalho: Relação individual de trabalho* (15.ª ed.). Almedina.

González, J., Cortina, C., & Rodríguez, J. (2019). The role of gender stereotypes in hiring: A field experiment. *European Sociological Review, 35*(2), 187–204. https://doi.org/10.1093/esr/jcy055

Lei n.º 13/2023, de 3 de abril. Altera o Código do Trabalho e legislação conexa no âmbito da agenda do trabalho digno. *Diário da República, 1.ª série, n.º 66*. https://diariodarepublica.pt/dr/detalhe/lei/13-2023-211340863

Lei n.º 58/2019, de 8 de agosto. Assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 (Regulamento Geral sobre a Proteção de Dados). *Diário da República, 1.ª série, n.º 151*. https://diariodarepublica.pt/dr/detalhe/lei/58-2019-123815982

Lei n.º 7/2009, de 12 de fevereiro. Aprova a revisão do Código do Trabalho. *Diário da República, 1.ª série, n.º 30*. https://www.unl.pt/sites/default/files/codigo_do_trabalho.pdf

Lo, F. P.-W., Qiu, J., Wang, Z., Yu, H., Chen, Y., Zhang, G., & Lo, B. (2025). AI hiring with LLMs: A context-aware and explainable multi-agent framework for resume screening [Preprint]. *arXiv*. https://doi.org/10.48550/arXiv.2504.02870

Lukács, B. (2023). GDPR-compliant AI-based automated decision-making in the world of work. *Computer Law & Security Review, 49*, Article 105789. https://doi.org/10.1016/j.clsr.2023.105789

Machado, S. S., & Magalhães, M. M. (n.d.). O uso responsável dos algoritmos no mundo do trabalho em Portugal. In *Direitos sociais: Diálogos transdisciplinares* (Vol. II, pp. 385–391). IberojurSciencePress. https://doi.org/10.62140/SMMM3852024

Marcelino, N. R. (2023). *Inteligência artificial aplicada aos processos de recrutamento e seleção em Portugal* [Dissertação de mestrado, Instituto Politécnico de Setúbal]. Repositório Comum. http://hdl.handle.net/10400.26/58467

Moreira, T. C. (2022). *Direito no trabalho na era digital*. Almedina.

Page, M. J., Moher, D., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., … McKenzie, J. E. (2021). PRISMA 2020 explanation and elaboration: Updated guidance and exemplars for reporting systematic reviews. *BMJ, 372*, Article n160. https://doi.org/10.1136/bmj.n160

Peixe, J. (2025). Decisões automatizadas, inteligência artificial e proteção de dados: Riscos e desafios no contexto português e europeu. *Vida Judiciária*. https://www.vidajudiciaria.com

Rana, C. I. P. (2021). *Gestão de talentos e processos de recrutamento: Vantagens e desafios* [Dissertação de mestrado, ISCTE – Instituto Universitário de Lisboa]. Repositório ISCTE-IUL. https://repositorio.iscte-iul.pt/bitstream/10071/24227/1/master_catarina_pereira_rana.pdf

Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 (Regulamento Geral sobre a Proteção de Dados). *Jornal Oficial da União Europeia, L 119*, 1–88. https://eur-lex.europa.eu/eli/reg/2016/679/oj

Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024 (Regulamento sobre Inteligência Artificial). *Jornal Oficial da União Europeia, L.* https://eur-lex.europa.eu/eli/reg/2024/1689/oj

Rodriguez, V. (2023). Ethical implications of AI-based algorithms in recruiting processes: A study of civil rights violations under Title VII and the Americans with Disabilities Act [Graduate project, Boise State University]. *ScholarWorks @ Boise State University*. https://scholarworks.boisestate.edu/cgi/viewcontent.cgi?article=1006&context=cyber_gradproj

Sequeira, F. V. (2022). O algoritmo no tecido empresarial: Das vicissitudes de contratação ao despedimento de trabalhadores – uma arma nociva que necessita de ser desarmada? In *Anuário da Proteção de Dados 2022* (pp. 70–126). Faculdade de Direito da Universidade Nova de Lisboa. https://protecaodedadosue.cedis.fd.unl.pt/wp-content/uploads/2022/12/3.-Frederico-Sequeira.pdf

Sivakaminathan, S. S., & Musi, E. (2025). ChatGPT is a gender bias echo-chamber in HR recruitment: An NLP analysis and framework to uncover the language roots of bias. *AI & Society*. Advance online publication. https://doi.org/10.1007/s00146-025-02564-8

van Bekkum, M. de M. (2025). Using sensitive data to de-bias AI systems: Article 10(5) of the AI Act. *Computer Law & Security Review, 56*, Article 106115. https://doi.org/10.1016/j.clsr.2025.106115

Wen, A., Patil, T., Saxena, A., Fu, Y., O'Brien, S., & Zhu, K. (2025). FAIRE: Assessing racial and gender bias in AI-driven resume evaluations [Preprint]. *arXiv*. https://doi.org/10.48550/arXiv.2504.01420

Xavier, J. P., & Ferreira, D. O. (2025). Inteligência artificial e direitos fundamentais da seleção em Portugal. In *Livro de atas* (pp. 371–395). https://doi.org/10.62140/JXDF3712025

Declaração Ética

Conflito de Interesse: Nada a declarar. **Financiamento:** Nada a declarar. **Revisão por Pares:** Dupla-cega.

Análise comparativa de sistemas de IA para suporte à decisão judicial: Aplicabilidade no Tribunal de Justiça da União Europeia

Comparative analysis of AI systems for judicial decision support: Applicability in the Court of Justice of the European Union

10.29073/j2.v8i1.1111

Recebido: 27 de fevereiro de 2026.
Aprovado: 31 de março de 2026.
Publicado: 04 de abril de 2026.

Autor/a: Cristiana Monteiro Pereira, ESTG-IPP, Portugal, cristianap01@hotmail.com.

Resumo

O presente artigo incide sobre o papel da Inteligência Artificial, doravante IA, no contexto da justiça, com especial foco no Tribunal de Justiça da União Europeia adiante TJUE.

Parte-se da evolução da IA e da sua crescente aplicação em sistemas judiciais, analisando-se diversos exemplos internacionais de utilização desta tecnologia, nomeadamente em funções de triagem processual, análise documental, apoio à decisão e previsão de resultados.

Procede-se, igualmente, à análise do conceito de justiça preditiva, evidenciando-se o seu potencial. No que respeita ao TJUE, o artigo destaca o aumento do volume processual, a duração média dos processos e o elevado número de pendências, sublinhando a relevância do princípio da celeridade processual no contexto europeu.

Conclui-se que a IA poderá constituir um instrumento relevante para a modernização da justiça, sobretudo em áreas como a pesquisa jurídica, análise de jurisprudência, tradução, anonimização e apoio à decisão. A sua integração, desde que realizada de forma responsável e em conformidade com os princípios fundamentais do direito, poderá contribuir para uma maior eficiência e celeridade dos processos judiciais.

Palavras-Chave: Celeridade; Inteligência Artificial; Tribunal de Justiça da União Europeia.

Abstract

This article focuses on the role of Artificial Intelligence, hereinafter AI, in the context of justice, with a special focus on the Court of Justice of the European Union (CJEU).

It begins with the evolution of AI and its increasing application in judicial systems, analyzing several international examples of the use of this technology, namely in procedural triage, document analysis, decision support, and outcome prediction.

The concept of predictive justice is also analyzed, highlighting its potential. With regard to the CJEU, the article highlights the increase in the volume of cases, the average duration of proceedings, and the high number of pending cases, underlining the relevance of the principle of procedural speed in the European context.

It concludes that AI could be a relevant instrument for the modernization of justice, especially in areas such as legal research, case law analysis, translation, anonymization, and decision support. Its integration, provided it is carried out responsibly and in accordance with fundamental legal principles, can contribute to greater efficiency and speed in judicial proceedings.

Keywords: Artificial Intelligence; Court of Justice of the European Union; Speed.

1. Introdução

Este tema surgiu no âmbito de uma breve pesquisa realizada no início daquele que foi o processo de escrita da dissertação do Mestrado em Práticas Jurídico-Digitais, cujo objetivo é entender a forma como a Inteligência Artificial pode ser útil na área jurídica. Neste sentido, este artigo apresenta-se como sendo um breve fragmento daquilo que foi abordado na referida dissertação.

O crescimento exponencial do uso das tecnologias de IA reflete-se na consecutiva transformação de diversos setores, como é o caso do setor Jurídico, trazendo não só novas oportunidades como também desafios, sobretudo a nível ético e legal.

A aplicação de sistemas de IA no suporte à decisão judicial pode transformar e agilizar a forma como os tribunais lidam com casos complexos, aumentando por consequência, a precisão das decisões e reduzindo a carga de trabalho dos juízes. Neste caso em concreto, a aplicação no TJUE de sistemas de IA pode traduzir-se num avanço tecnológico significativo.

A análise dos sistemas já existentes, bem como das suas funcionalidades e limitações, permite avaliar o potencial desta tecnologia no apoio à atividade jurídica. Paralelamente, a compreensão do funcionamento do Tribunal de Justiça da União Europeia, aliada à análise do seu volume processual e dos desafios associados à celeridade dos processos, revela-se fundamental para identificar as áreas em que a IA poderá desempenhar um papel mais relevante.

2. Enquadramento

Na década de 50 do século passado, a IA foi definida como uma ciência ou uma engenharia capaz de gerar uma máquina que desempenha funções semelhantes às humanas. Esta definição sofreu alterações ao longo do tempo, sendo atualmente (2024) a Inteligência Artificial é definida como um sistema capaz de se adaptar a alterações, adquirir conhecimentos e aplicar os mesmos a cenários desconhecidos (Cunha, 2022).

No presente século (XXI), a Inteligência Artificial é considerada uma área vasta da ciência da computação que tem como principal função a máquina funcionar como se de facto tivesse inteligência, isto é como tal um conceito abrangente e que engloba as tecnologias que se baseiam em algoritmos.

2.1. Sistemas de Inteligência Artificial utilizados nos Tribunais

Um dos grandes temas de estudo desta pesquisa são os sistemas de IA já existentes e usados por vários tribunais, por exemplo europeus, norte-americanos ou brasileiros (por exemplo). O estudo destes sistemas é de extrema importância, uma vez que nem todos têm a mesma funcionalidade e finalidade. É possível verificar que já há países que utilizam inteligência artificial nos seus sistemas judiciais através do "*Centre de Ressources sur la Cyberjustice et L'Intelligence Artificielle*" da Comissão Europeia Para a Eficiência da Justiça.

Podemos observar a nível estatístico, que existem 160 sistemas de IA a ser utilizados no âmbito da justiça, e estes dividem-se em: suporte à decisão; triagem, atribuição e automatização do fluxo de trabalho; pesquisa de documentos; serviços de informação e assistência; anonimização e pseudonimização; registos, transcrição e tradução; resolução automatizada de litígios e previsão de resultados de litígios.

De reparar também que a grande parte dos sistemas de IA são públicos (144 ferramentas), 9 ferramentas são privadas e 7 são ainda apenas projetos de pesquisa ou projetos desenvolvidos em universidades. Além disso, três ferramentas são utilizadas em Portugal: a primeira é de triagem, atribuição e automatização do fluxo de trabalho e de pesquisa de documentos, a segunda é de serviços de informação e assistência que está disponível através do site Justiça.Gov.PT com o nome de "Guia prático da Justiça" e a última é de anonimização e pseudonimização e de pesquisa de documentos disponível no site govtech.

A nível internacional um dos exemplos mais conhecidos é o sistema COMPAS (*Correctional Offender Management Profiling For Alternative Sanctions*), utilizado nos Estados Unidos da América, que tem como

funcionalidade prever o risco de reincidência, fazendo com que os juízes apliquem penas mais "severas" (Lobo, 2020).

Outro exemplo de sistema de IA,é o projetoVitór(IA)que começou a serdesenvolvido no Brasil em 2017, numa parceria entre o Supremo Tribunal Federal e a Universidade de Brasília. Este tem como principal funcionalidade auxiliar o estudo de recursos extraordinários em especial, a classificação de temas de repercussão geral (Pagel, 2024, pág. 22) através de *machine learning*. (Federal,2023) (Filho & Junquilho, 2018).

Já em 2021, o Supremo Tribunal Federal concluiu que o "Victor" desempenhava quatro tarefas principais, a saber: a conversão de imagens em textos no processo digital ou eletrónico; separação do começo e do fim de um documento (peça processual, decisão, etc); separação e classificação das peças processuais mais utilizadas nas atividades do STF e a identificação dos temas de repercussão geral de maior incidência (que são 27 no total) (Supremo Tribunal Federal, 2021).

Noque diz respeito ao plano Europeu existe o exemplo da Alemanha que já introduziu no seu sistema judiciário dois projetos de IA denominados de OLGA (Ober Landes GertsAsistent) e FRAUKE (Frankfurter Judgment Configurator, Electronic), uma das funções do primeiro sistema é analisar decisões de primeira instância, já o segundo sistema foi introduzido no Tribunal Distrital de Frankfurt e tem como função extrair automaticamente dos documentos dados relevantes dos casos, como por exemplo: aeroportos de partida e destino ou qual é distância do voo, agilizando assim a análise de dados dos processos (Mielke,2023).

Por sua vez, a França tentou implementar em 2017, um software denominado de PREDICTICE, que tinha como objetivo tentar reduzir a variedade excessiva de decisões em nome da igualdade dos cidadãos perante a lei, no entanto este não foi bem-sucedido (Rebecchi et al., 2019, p.122 e 123).

Este sistema foi utilizado durante três meses, em dois tribunais de recurso denominados de Rennes e Douai, não tendo obtido resultados promissores, dado que a experiência nada acrescentou ao estudo sobre o papel da IA na tomada de decisão. Uma das razões para o fracasso deste software deveu-se ao facto de ao analisar as decisões dos juízes que foram utilizadas como "*data fuel*",o mesmo confundiu-se entre o conjunto de ocorrências e as causalidades tendo sido obtidos resultados absurdos(Sampaio et al., 2019, p. 10) (CEPEJ, 2018, p. 14).

Ainda na França, houve uma tentativa de desenvolver um algoritmo denominado de DataJust, que tinha como objetivo extrair e explorar de forma automática os dados contidos nas decisões judiciais relativos a indemnizações por danos físicos. Mais especificamente, pretendia-se identificar os montantes solicitados e oferecidos pelas partes, as avaliações propostas no âmbito dos procedimentos de resolução extrajudicial e os montantes que eram atribuídos às vítimas pelos tribunais. Este sistema foi desenvolvido ao longo de dois anos, todavia, à semelhança do PREDICTICE, também não teve grande sucesso, dado que o banco de dados deste algoritmo foi considerado incompleto e tendencioso, o projeto foi então abandonado (Benoit, 2022).

Importa ainda fazer referência ao caso de Inglaterra que já utiliza modelos de IA na justiça para diversas funções como por exemplo a plataforma *HM Online Courts & Tribunals Services* (HMCTS), que é utilizada para facilitar e agilizar o acesso à justiça, servindo inclusive para resolução de pequenos litígios, onde a IA intervém na análise de documentos e auxílio de mediação, contribuindo para uma melhor gestão processual (Grove, 2018).

2.2. A Justiça Preditiva

A Justiça Preditiva é considerada um software baseado em inteligência artificial que tem como principal funcionalidade antever e prever uma dada decisão judicial, baseando-se para o efeito na jurisprudência e em dados que lhe são introduzidos. Analisando estes dados o sistema de IA é capaz de desenvolver recomendações e até mesmo decisões para casos futuros (Cunha, 2022, p.68).

Uma das definições dadas à justiça preditiva é a capacidade que as máquinas têm de converter a linguagem natural em lei aplicável, com a finalidade de tratar os processos judiciais, e colocá-la no contexto baseado nas

suas características (o lugar, a personalidade dos juízes, advogados etc) a fim de antecipar a probabilidade da decisão (Garapon, 2018).

Já *Loïc Cadiet* refere que, citado por *Nouri* et al. (2024), que a justiça preditiva consiste num conjunto de ferramentas desenvolvidas a partir da análise de uma vasta quantidade de dados judiciais que sugerem, especialmente através de cálculos de probabilidade, como um dado caso se irá desenvolver (p.121).

Um dos claros exemplos de sucesso da utilização deste tipo de software é o estudo realizado por investigadores da *University College of London*, Universidade de *Sheffield* e da Universidade da Pensilvânia. Este estudo foi realizado com base em dados de 584 casos, do Tribunal Europeu de Direitos Humanos (TEDH), que violavam três artigos da Convenção Europeia dos Direitos do Homem (Convenção Europeia dos Direitos do Homem, 1950), em concreto: o artigo 3º (Proibição da Tortura), artigo 6º (Direito a um Processo Equitativo) e artigo 8º (Direito ao respeito pela vida privada e familiar) (Macedo, 2020, p.26).

O software fez a análise dos casos utilizando a *machine learning algorithm* e formulou a sua própria decisão, sendo considerado o primeiro a prever os resultados de um tribunal internacional, tendo sido obtida uma precisão de 79% (Trials, 2016).

Este é um dos estudos que fundamenta a importância de continuar a investir na evolução deste tipo de sistemas de IA, para que no futuro a mesma se torne uma ferramenta indispensável à celeridade dos processos jurídicos.

3. O Tribunal de Justiça da União Europeia

O Tribunal de Justiça da União Europeia é o órgão máximo da justiça da União Europeia, foi criado em 1952, localizado no Luxemburgo e tem como principal função velar para que a legislação da União Europeia seja interpretada e aplicada de forma igual em todos os 27 Estados Membros, bem como garantir que as instituições dos mesmos respeitam o direito europeu.

É composto por duas jurisdições: o Tribunal de Justiça e o Tribunal Geral (art.º 19 do Tratado da União Europeia e art.º 251º a 281º do Tratado Sobre o Funcionamento da União Europeia). O primeiro é composto por um juiz de cada país da UE e onze advogados-gerais tal como consta no artigo 19º, nº 2, 1ª parte do TUE, este trata concretamente dos "pedidos de decisões a título prejudicial provenientes das jurisdições nacionais, bem como de certas ações de anulação e de recursos" (art.º 19º, nº 3 do TUE). Este funciona da seguinte forma, após a designação de um juiz relator e um advogado-geral os processos são tratados em duas fases: a escrita e a oral (art.º 259º, 3º parágrafo do TFUE e art.º 20º do Estatuto do Tribunal de Justiça da União Europeia).

Por outro lado, o Tribunal Geral (art.º 254º a 257º do TFUE) é composto por dois juízes de cada país da UE tal como consta do artigo 19º, nº2, 2ª parte do TUE e tem como função prenunciar-se sobre os recursos de anulação interpostos por particulares, empresas e em determinados casos, governos dos Estados-Membros. Ora isto quer dizer que o Tribunal Geral trata essencialmente de matérias relacionadas com o direito de concorrência, auxílios estatais, comércio, agricultura e marcas registadas. Este funciona de forma semelhante ao Tribunal de Justiça salvo que na maioria das vezes os processos são entregues a três juízes e não há intervenção dos advogados-gerais.

Apesar da competência do TJUE em várias matérias, os processos mais comuns são: interpretação de legislação, aplicação de legislação, anulação de atos legislativos europeus, tem a obrigação de ação e aplicação de sanções às instituições europeias (União Europeia, “Tribunal de Justiça Da União Europeia”).

3.1. Estatísticas do TJUE e o Princípio da Celeridade dos Processos

Para compreender o modo como a Inteligência Artificial seria útil no TJUE, é essencial analisar, em primeiro lugar, o volume de processos que tramitam neste Tribunal.

Estatisticamente, em 2024 deram entrada no TJUE 920 processos, um aumento de 12% relativamente a 2023, verificou-se igualmente um aumento no número de recursos de decisões do Tribunal Geral, sendo que, em 2024,

o número de recursos, incluindo os relativos a medidas provisórias e pedidos de intervenção, atingiu 277 processos, superando novamente o número do ano anterior.

No que respeita aos processos findos, em 2024 o TJUE encerrou, um total de 863 processos, maioritariamente relativos a reenvios prejudiciais e recursos de decisões do Tribunal Geral, o que representa um aumento de 10% face a 2023.

Contudo, o aumento da afluência processual tem tido como consequência o prolongamento da duração média dos processos, que em 2024 atingiu 17,7 meses o que se traduz em aproximadamente um ano e meio, valor superior ao registado em 2023. Paralelamente, o número de processos pendentes continua a ser elevado, situando-se em 1206 processos, sendo este o número mais alto de sempre registado no TJUE.

Este cenário evidencia a necessidade de "dar voz"ao princípio da celeridade processual, sendo que, neste caso, a Inteligência Artificial se apresenta como uma possível solução, não no sentido de substituir o ser humano, mas sim, no sentido de auxiliar as funções do Tribunal de Justiça da União Europeia.

O princípio da celeridade processual assume, portanto, um papel central, estando consagrado tanto no ordenamento jurídico português como no europeu. No plano nacional, encontra-se previsto no artigo 6.º, n.º 1 do Código de Processo Civil, impondo ao juiz o dever de providenciar pelo andamento célere do processo, bem como no artigo 32.º, n.º 2 da Constituição da República Portuguesa, que garante ao arguido o direito a ser julgado no mais curto prazo compatível com as garantias de defesa, e ainda no artigo 20.º, n.º 4 da Constituição, que consagra o direito a uma decisão em prazo razoável mediante processo equitativo.

Ao nível europeu, este princípio encontra-se igualmente consagrado no artigo 41.º, n.º 1 da Carta dos Direitos Fundamentais da União Europeia, sob a epígrafe "Direito a uma boa administração", que estabelece que todas as pessoas têm direito a que os seus assuntos sejam tratados de forma imparcial, equitativa e dentro de um prazo razoável. Por sua vez, o artigo 6.º da Convenção Europeia dos Direitos do Homem, sob a epígrafe "Direito a um processo equitativo", prevê que qualquer pessoa tem direito a que a sua causa seja examinada de forma equitativa e pública, num prazo razoável, por um tribunal independente e imparcial.

A relevância deste princípio torna-se particularmente evidente quando se constata que os processos no TJUE, em determinadas situações, ultrapassam aquilo que pode ser considerado um prazo razoável.

Segundo Joaquim Pires de Lima1, a verificação da violação do direito a uma decisão em prazo razoável depende da análise de quatro fatores fundamentais: a complexidade da causa, a conduta das autoridades, a conduta do queixoso e a finalidade do processo.

A complexidade da causa está diretamente relacionada com o tempo necessário à realização das diligências processuais no caso concreto, podendo ser aferida tanto pela duração global do processo como pela existência de períodos de inatividade ou de tramitação irregular.

Por sua vez, a conduta das autoridades prende-se com a eventual inércia do tribunal ou de outras entidades envolvidas, sendo o Estado responsável por situações de desorganização ou insuficiência de meios. Contudo, importa, sublinhar que a simples violação de prazos legais não é, por si só, suficiente para concluir pela violação do direito a uma decisão em prazo razoável, exceto quando esses prazos são manifestamente ultrapassados.

Um exemplo desta problemática é o que se encontra plasmado no acórdão do Tribunal Geral (Terceira Secção Alargada), no processo n.º T-577/14, em que as sociedades *Gascogne Sack Deutschland GmbH* e *Gascogne* intentaram uma ação contra a União Europeia, alegando danos decorrentes da duração excessiva dos processos (5 anos e 9 meses). O Tribunal condenou a União Europeia ao pagamento de uma indemnização de 47.064,33€

[1] Direito à Justiça em Prazo Razoável, 1990

a título de danos materiais, bem como 5.000,00€ a cada uma das sociedades a título de danos morais, em consequência da violação do prazo razoável de julgamento nos processos T-72/06 e T-79/06.

Relativamente à conduta do queixoso, esta também deve ser considerada na avaliação da eventual violação do direito, não sendo legítimo imputar-lhe a responsabilidade por atrasos decorrentes do exercício dos seus direitos processuais. Como refere Pires de Lima, muitas vezes não são os requerimentos das partes que provocam a demora, mas sim servem de pretexto para a inércia do tribunal.

Por fim, a finalidade do processo constitui igualmente um critério relevante, sobretudo em situações em que a decisão tardia compromete a utilidade do próprio processo. Como salienta Joaquim Pires de Lima, existem casos em que os tribunais demoram cerca de dois meses a decidir providências destinadas a evitar danos irreparáveis em prazos muito mais longos, tornando a decisão, na prática, inútil.

Apesar destas orientações, a definição concreta de "prazo razoável" continua a depender das circunstâncias do caso. Ainda assim, a jurisprudência do Tribunal de Justiça fornece alguns parâmetros, como o consagrado no acórdão de 13 de dezembro de 2018, no processo n.º C-150/17 P[2], cujo parágrafo 76 considera que um prazo de dois anos e seis meses pode ser tido como razoável.

Neste contexto, a crescente pressão sobre o TJUE e a necessidade de garantir decisões em tempo útil tornam evidente o potencial da Inteligência Artificial como instrumento de apoio à eficiência judicial, contribuindo para a concretização efetiva do princípio da celeridade processual.

3.2. Áreas Onde a Inteligência Artificial Seria Útil

Em face do exposto supra, importa agora perceber em que áreas a IA seria útil e contribuiria para a celeridade dos processos.

Primeiramente é necessário ter em consideração, as características específicas dos processos que tramitam no TJUE como: de facto muitos dos processos envolverem diversas línguas dos Estados-Membros; complexidade legal elevada, dado que há processos que envolvem diversos ordenamentos jurídicos, regulamentos, diretivas, jurisprudência etc. e o elevado volume de processos que correm termos no TJUE.

Neste sentido, podemos considerar que as áreas onde a IA seria de facto útil são: a pesquisa jurídica e análise de jurisprudência, resumo de processos e documentação, transcrição, tradução e anonimização e suporte à decisão.

Relativamente à pesquisa jurídica e análise de jurisprudência, a IA seria útil para identificar precedentes, extrair decisões relevantes em casos semelhantes, classificar acórdãos segundo temas jurídicos, bem como analisar jurisprudência e leis dos diferentes ordenamentos jurídicos europeus, contribuindo, assim, para acelerar a investigação, reduzindo o esforço humano.

Quanto ao resumo de processos e documentação que já existem sistemas de IA com estas funcionalidades a nível europeu (sistema FRAUKE). Estes, como o próprio nome diz, permitem resumir longas peças processuais, e extrair dos documentos informações de forma cronológica e relevantes, o que permitiria e facilitaria a compreensão dos pontos principais do processo, isto no caso dos resumos, e pouparia tempo aos juízes e advogados na análise de documentos extensos melhorando a eficiência da justiça.

Relativamente à transcrição, tradução e anonimização a IA seria útil para a transcrição de áudios nas audiências, tradução de documentos de e para várias línguas da UE, anonimizar decisões ou documentos para publicação ou bases de dados públicas. Isto permitiria poupar tempo, assegurar o cumprimento dos preceitos de anonimização de dados do RGPD e garantir maior acessibilidade à justiça.

Por último, o suporte à decisão pode ser visto como "a IA substituta dos juízes", no entanto a ideia que se pretende passar não é a da substituição dos juízes, advogados ou escrivãos, mas sim a de apoio à justiça e

[2] Tribunal de Justiça da União Europeia, *ACÓRDÃO DO TRIBUNAL de JUSTIÇA (Primeira Secção). Proc. C-150/17 P*

cumprindo o princípio da celeridade dos processos. No fundo se repararmos todas as áreas abordadas até agora podem encaixar-se no suporte à decisão, seja a transcrição, tradução e anonimização, seja a pesquisa e análise de jurisprudência ou o resumo de processos e documentação, todos contribuem para o suporte à decisão, não no sentido de decidirem ou influenciarem o juiz, mas sim no sentido de agilizar os processos que correm termos no TJUE.

Neste âmbito a IA seria ainda útil para dar sugestões de estrutura de acórdãos, verificação automática de citações e notificações, permitindo assim que juízes e advogados foquem a sua atenção no que é realmente crucial e mais complexo no processo.

6. Conclusão

Em conclusão, a evolução de sistemas de Inteligência Artificial (IA) reflete uma mudança significativa na forma como as "máquinas" podem ser concebidas para imitar e até aprimorar capacidades humanas. A definição de IA sofreu alterações desde a década de 1950 tendo evoluído para um conceito mais dinâmico e adaptativo, englobando sistemas que são capazes de aprender, ajustar-se e aplicar conhecimentos a situações inéditas.

A aplicação deste tipo de sistemas nos tribunais, tem vindo a aumentar exemplos disso são os sistemas COMPAS, Vitór (IA), OLGA, FRAUKE e DataJust, que ilustram as diversas formas para as quais a tecnologia tem sido utilizada, seja com a finalidade de otimizar a gestão processual ou auxiliar a tomada de decisões.

No entanto, o destaque deste artigo é o Tribunal de Justiça da União Europeia e a forma como a IA poderá revolucionar o seu funcionamento. O crescente volume de processos que tramitam no TJUE releva que, cada vez mais, se torna difícil “dar voz” ao princípio da celeridade dos processos, deste modo a IA apresenta-se como uma possível solução.

Assim, a integração da IA no âmbito do TJUE deverá ser orientada por critérios de rigor, transparência e conformidade jurídica, de modo a garantir que a inovação tecnológica se traduza numa efetiva melhoria da qualidade da justiça, sem comprometer os princípios fundamentais que a regem.

Referências

Benoit, M. (2022, January 17). The Ministry of Economy abandons the development of DataJust, the algorithm that should help calculate compensation for personal injury - ActuIA. *ActuIA*. https://www.actuia.com/english/the-ministry-of-economy-abandons-the-development-of-datajust-the-algorithm-that-should-help-calculate-compensation-for-personal-injury/

CEPEJ. (2025). *Resource Centre Cyberjustice and AI*. Tableau. https://public.tableau.com/app/profile/cepej/viz/ResourceCentreCyberjusticeandAIFR/AI%20TOOLSINITIATIVESREPORT

Cunha, G. B. R. D. (2022). *A inteligência artificial no exercício da função judicial: de juiz humano a juiz robot?* [Tese, Universidade do Minho].

ESTATUTO DO TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. (n.d.). *Versão consolidada*. https://curia.europa.eu/jcms/upload/docs/application/pdf/2016-08/tra-doc-pt-div-c-0000-2016-201606984-05_00.pdf

Filho, M. S. M., & Junquilho, T. A. (2018). Projeto Victor: Perspectivas de aplicação da inteligência artificial ao direito. *Revista de Direitos e Garantias Fundamentais, 19*(3), 218–237. https://doi.org/10.18759/rdgf.v19i3.1587

Garapon, A., & Lassegue, J. (2018). *Justice digital: Revolution graphique et rupture anthropologique*.

Grove, R. (2018, September). AI, machine learning and the administration of justice in England and Wales: Prospects, opportunities, challenges. https://rm.coe.int/ai-machine-learning-and-the-administration-of-justice-

in-england-and-w/16808e4d87
https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c

Justice, European Commission for the Efficiency of (CEPEJ). (2018, December 3–4). *European ethical charter on the use of artificial intelligence in judicial systems and their environment* (p. 14).

Lobo, F. R. (2020). *A utilização de sistemas preditivos de inteligência artificial na justiça* [Universidade Lusíada-Norte, Porto].

Macedo, R. M. (2020). *Inteligência artificial: Justiça digital e tribunais*. 1º Curso de Pós-graduação em Direitos Humanos e Tribunais.

Mielke, D. B. (2023, November 28). Künstliche Intelligenz in der Justiz: Sechs Einsatzbereiche am Beispiel von aktuellen Pilotprojekten. *Legal-Tech.de*. https://legal-tech.de/kuenstliche-intelligenz-in-der-justiz-pilotprojekte/#_ftn3

Nouri, Z., Salah, W. B., & Alomeran, N. (2024). Artificial intelligence and administrative justice: An analysis of predictive justice in France. In *Hasanuddin Law Review* (pp. 119–143).

Pires de Lima, J. (1990, November 30). Considerações acerca do direito à justiça em prazo razoável. https://portal.oa.pt/upl/%7Bd704c67c-deb6-4bc5-b858-7852d48ba894%7D.pdf

Rebecchi, M. C., et al. (2019). *THEMIS Annual Journal 2019, 1*(1). https://ejtn.eu/wp-content/uploads/2023/02/TAJ-2019.pdf

Reis, J. C. G., Espírito Santo, P., & Melão, N. (2020). *Impact of artificial intelligence research on politics of the European Union member states: The case study of Portugal*. Edições Universitárias Lusófonas.

Rocha, M. L., & Pereira, R. S. (2020). *Inteligência artificial & direito*. Almedina.

Sampaio, E. A., Seixas, J. J., & Gomes, P. J. (2019, July 2–4). Artificial intelligence and the judicial ruling (p. 10). https://portal.ejtn.eu/PageFiles/17916/TEAM%20PORTUGAL%20I%20TH%202019%20D.pdf

TF amplia emprego de inteligência artificial. (2023). *Supremo Tribunal Federal*. https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=508710&ori=1

Tribunal de Justiça da União Europeia. (2011, November 16). Acórdão do Tribunal (Quarta Câmara), Proc. T 79/06. https://curia.europa.eu/juris/document/document.jsf?text=&docid=114442&pageIndex=0&doclang=FR&mode=lst&dir=&occ=first&part=1&cid=1084031

Tribunal de Justiça da União Europeia. (2011, November 16). Acórdão do Tribunal (Quarta Câmara), Proc. T 72/06. https://curia.europa.eu/juris/document/document.jsf?text=&docid=114408&pageIndex=0&doclang=FR&mode=lst&dir=&occ=first&part=1&cid=1084031

Tribunal de Justiça da União Europeia. (2017, January 10). Acórdão do Tribunal Geral (Terceira Secção Alargada), Proc. T 577/14. https://curia.europa.eu/juris/document/document.jsf?text=&docid=186675&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=1084031

Tribunal de Justiça da União Europeia. (2018, December 13). Acórdão do Tribunal de Justiça (Primeira Secção), Proc. C 150/17 P. https://curia.europa.eu/juris/document/document.jsf?text=&docid=208962&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=19417047

Tribunal de Justiça da União Europeia. (2018, December). Acórdão do Tribunal de Justiça (Primeira Secção).

Tribunal de Justiça da União Europeia. (2025, March). *Estatísticas Judiciárias do Tribunal de Justiça*.

UCL. (2018, November 15). AI predicts outcomes of human rights trials. *UCL News*. https://www.ucl.ac.uk/news/2016/oct/ai-predicts-outcomes-human-rights-trials

Declaração Ética

Conflito de Interesse: Nada a declarar. **Financiamento:** Nada a declarar. **Revisão por Pares:** Dupla-cega.

Jornal Jurídico